



UNIL | Université de Lausanne

Unicentre

CH-1015 Lausanne

<http://serval.unil.ch>

Year : 2023

SERIOUS GAMING AS CRIME PREVENTION? The Effectiveness of a Serious Game and the Role of Personality Traits in reducing the proneness towards Social Engineering fraud

Muhly Fabian

Muhly Fabian, 2023, SERIOUS GAMING AS CRIME PREVENTION? The Effectiveness of a Serious Game and the Role of Personality Traits in reducing the proneness towards Social Engineering fraud

Originally published at : Thesis, University of Lausanne

Posted at the University of Lausanne Open Archive <http://serval.unil.ch>

Document URN : urn:nbn:ch:serval-BIB_A7ACAD9F01135

Droits d'auteur

L'Université de Lausanne attire expressément l'attention des utilisateurs sur le fait que tous les documents publiés dans l'Archive SERVAL sont protégés par le droit d'auteur, conformément à la loi fédérale sur le droit d'auteur et les droits voisins (LDA). A ce titre, il est indispensable d'obtenir le consentement préalable de l'auteur et/ou de l'éditeur avant toute utilisation d'une oeuvre ou d'une partie d'une oeuvre ne relevant pas d'une utilisation à des fins personnelles au sens de la LDA (art. 19, al. 1 lettre a). A défaut, tout contrevenant s'expose aux sanctions prévues par cette loi. Nous déclinons toute responsabilité en la matière.

Copyright

The University of Lausanne expressly draws the attention of users to the fact that all documents published in the SERVAL Archive are protected by copyright in accordance with federal law on copyright and similar rights (LDA). Accordingly it is indispensable to obtain prior consent from the author and/or publisher before any use of a work or part of a work for purposes other than personal use within the meaning of LDA (art. 19, para. 1 letter a). Failure to do so will expose offenders to the sanctions laid down by this law. We accept no liability in this respect.

UNIVERSITÉ DE LAUSANNE
FACULTÉ DE DROIT, DES SCIENCES CRIMINELLES ET D'ADMINISTRATION PUBLIQUE
ÉCOLE DES SCIENCES CRIMINELLES

SERIOUS GAMING AS CRIME PREVENTION?
**The Effectiveness of a Serious Game and the Role of Personality Traits in reducing the
proneness towards Social Engineering fraud**

THÈSE DE DOCTORAT

Présentée à la

Faculté de droit, des sciences criminelles et d'administration publique
de l'Université de Lausanne

pour l'obtention du grade de

Docteur en Criminologie

Par

Fabian Muhly

Directeur de thèse
Prof. Dr. Stefano Caneppele

Jury

Prof. Dr. Christophe Champod : Président
Prof. Dre Marianne Junger (Université de Twente, Pays-Bas) : Experte externe
Major Martin Burke (Armée Suisse): Expert externe
Prof. Dr Olivier Ribaux (Université de Lausanne) : Expert interne

LAUSANNE
2023

IMPRIMATUR

A l'issue de la soutenance de thèse, le Jury autorise l'impression de la thèse de Monsieur Fabian Muhly, candidat au doctorat en droit en criminologie et sécurité, intitulée :

**« Serious gaming as crime prevention ?
The effectiveness of a serious game and the role of personality traits
in reducing the proneness towards social engineering fraud »**



Professeur Christophe Champod
Président du jury

Lausanne, le 1^{er} juin 2023



UNIL | Université de Lausanne

Unicentre
CH-1015 Lausanne
<http://serval.unil.ch>

Year: 2023

SERIOUS GAMING AS CRIME PREVENTION?

The Effectiveness of a Serious Game and the Role of Personality Traits in reducing the proneness towards Social Engineering fraud

Fabian Muhly

Fabian Muhly, 2023, SERIOUS GAMING AS CRIME PREVENTION?

The Effectiveness of a Serious Game and the Role of Personality Traits in reducing the proneness towards Social Engineering fraud

Originally published at: Thesis, University of Lausanne

Posted at the University of Lausanne Open Archive <http://serval.unil.ch>

Document URN :

Droits d'auteur

L'Université de Lausanne attire expressément l'attention des utilisateurs sur le fait que tous les documents publiés dans l'Archive SERVAL sont protégés par le droit d'auteur, conformément à la loi fédérale sur le droit d'auteur et les droits voisins (LDA). A ce titre, il est indispensable d'obtenir le consentement préalable de l'auteur et/ou de l'éditeur avant toute utilisation d'une oeuvre ou d'une partie d'une oeuvre ne relevant pas d'une utilisation à des fins personnelles au sens de la LDA (art. 19, al. 1 lettre a). A défaut, tout contrevenant s'expose aux sanctions prévues par cette loi. Nous déclinons toute responsabilité en la matière.

Copyright

The University of Lausanne expressly draws the attention of users to the fact that all documents published in the SERVAL Archive are protected by copyright in accordance with federal law on copyright and similar rights (LDA). Accordingly it is indispensable to obtain prior consent from the author and/or publisher before any use of a work or part of a work for purposes other than personal use within the meaning of LDA (art. 19, para. 1 letter a). Failure to do so will expose offenders to the sanctions laid down by this law. We accept no liability in this respect.

Executive Summary

Social Engineering is a threat for the security of information to individuals and companies alike. Deceptive criminals with malicious intentions manipulate people all around the world for their financial gain or for the sake of the information itself. Social engineering threats show themselves for example in phishing attacks, phone call scams or even interpersonal physical attacks. Effective universal preventive strategies against those criminal acts are still desirable. What all the different types of attack have in common is its manipulation of human psychology to trick people into trusting a trickster with confidence.

The aim of this thesis was to investigate the role of personality traits and the effectiveness of an interactive serious game as security training concerning the proneness of people in falling prey to a social engineering attack. A discussion and derivation of psychological influencing factors was presented for the further application in the research. In a qualitative study with a sample size of 97 professionals, a serious game was researched for improvements concerning its content and proceeding. The derived serious game was then used as an intervention in a controlled quasi-randomized field experiment with 180 reserve soldiers of the Swiss Armed Forces. Phishing emails were used as test instruments, testing whether participants click a link in the email that would direct them to a designated landing page and secondly whether those who clicked also inputted the requested information on the landing page. Time pressure and Cialdini's authority and unity principles were applied. The result was that the Honesty-Humility dimension of the HEXACO personality inventory seems to be slightly predictive for falling prey to the pre-test and inputting information on the designated landing page. Moreover, Honesty-Humility is positively associated with less risky cybersecurity behaviour, whereas higher scores in Openness and Conscientiousness indicate more favourable attitudes towards cybersecurity and cybercrime. Emotionality shows a slight negative impact on a desired attitude towards cybersecurity. In the pre-test setting, 57.2% of study participants complied to the request of clicking the link in the email, whereas of those who clicked, 88.3% also disclosed information. In the post-test settings, results were significantly lower. For the first post-test the shares were 16.7% who fell for the scam and of those who fell for it 26.7% inputted information, whereas for the second post-test the numbers were 25.6% and 43.5%, respectively. However, the results showed that no effect for the intervention was observable in the data. Both study groups statistically significantly improved from pre- to post-tests. Experimental group participants did however not improve substantially more than the control group. Advanced statistical analysis showed that the sample size was too

small to measure significant effects for the serious game. A sample two to three times as large would have been necessary. The largest statistically significant effect was, however, measured for other variables. Past victimization and individual victimization expectation were found to be good predictors for the vulnerability to the phishing scams in this research. This is an essential finding of this dissertation. A routine activity approach for social engineering was derived in the course of the thesis, which is, to the best of my knowledge, the first of its kind.

It is concluded that certain personality traits help to better evaluate cybersecurity behaviour in an organization. Studies with larger sample sizes are needed to look on the effects of the serious game. An observed U-shaped relationship among one's own capability of spotting and resisting phishing scams and an eventual victimization is a key finding that is worth looking at in future studies. Approaches that put the spotlight on personality characteristics like self-confidence could be helpful in tackling human proneness to social engineering fraud. The findings of this dissertation help practitioners in the Swiss Armed Forces to better evaluate cybersecurity behaviour based on personality traits and self-reported victimization variables.

Résumé

L'ingénierie sociale constitue une menace pour la sécurité des informations, tant pour les particuliers que pour les entreprises. Des criminels motivés par des intentions malveillantes manipulent des personnes dans le monde entier pour en tirer un avantage financier ou pour dérober des informations. Les menaces d'ingénierie sociale se manifestent par exemple par des attaques de phishing, des escroqueries par téléphone ou même des attaques physiques. Des stratégies préventives universelles efficaces contre ces actes criminels sont toujours souhaitables. Le point commun de tous ces différents types d'attaques est la manipulation de la psychologie humaine pour inciter les gens à faire confiance à un agent malveillant.

L'objectif de cette thèse était d'étudier le rôle des traits de personnalité sur la prédisposition des sujets à devenir victimes d'une attaque d'ingénierie sociale, et l'efficacité d'un jeu sérieux interactif en tant que formation à la sécurité. Une discussion et une dérivation des facteurs d'influence psychologiques ont été présentées pour une application ultérieure dans la recherche. Dans une étude qualitative portant sur un échantillon de 97 professionnels, un jeu sérieux a fait l'objet d'une recherche visant à améliorer son contenu et son déroulement. Ce jeu a ensuite été utilisé comme intervention dans une expérience de terrain contrôlée quasi-randomisée avec 180 soldats de réserve des forces armées suisses. Des courriels d'hameçonnage ont été utilisés comme instruments de test pour vérifier si les participants cliquaient sur un lien dans le courriel qui les dirigeait vers une page de destination désignée, et dans un deuxième temps si ceux qui suivaient ce lien saisissaient également les informations demandées sur la page de destination. La pression du temps et les principes d'autorité et d'unité de Cialdini ont été appliqués. Les résultats obtenus indiquent que la dimension Honnêteté-Humilité de l'inventaire de personnalité HEXACO semble être légèrement prédictive de la possibilité de cliquer sur le pré-test et de saisir les informations sur la page de destination désignée. De plus, la dimension Honnêteté-Humilité est positivement associée à un comportement moins risqué en matière de cybersécurité, tandis que des scores plus élevés en Ouverture et Conscience indiquent des attitudes plus favorables à la cybersécurité et à la cybercriminalité. L'émotivité a un léger impact négatif sur l'attitude souhaitée à l'égard de la cybersécurité. Dans le cadre du pré-test, 57,2 % des participants à l'étude se sont conformés à la demande de cliquer sur le lien dans le courriel, tandis que parmi ceux qui ont cliqué, 88,3 % ont également divulgué des informations. Dans le cadre du post-test, les résultats étaient nettement inférieurs. Pour le premier post-test, 16,7 % des participants sont tombés dans le piège et 26,7 % d'entre eux ont fourni des informations, tandis que pour le second post-test, les chiffres étaient respectivement

de 25,6 % et 43,5 %. Cependant, les résultats ont montré qu'aucun effet de la formation au moyen du jeu sérieux n'était observable dans les données. Les deux groupes d'étude se sont améliorés de manière statistiquement significative entre les pré et post-tests. Les participants du groupe expérimental ne se sont toutefois pas améliorés de manière substantielle par rapport au groupe de contrôle. Une analyse statistique avancée a montré que la taille de l'échantillon était trop petite pour mesurer des effets significatifs pour le jeu sérieux. Un échantillon deux à trois fois plus grand aurait été nécessaire. Un effet statistique plus important a toutefois été mesuré pour d'autres variables. La victimisation antérieure et les attentes individuelles en matière de victimisation se sont avérées être de bons prédicteurs de la vulnérabilité aux escroqueries par hameçonnage dans cette recherche. Il s'agit là d'une conclusion essentielle de cette thèse. Une approche d'activité de routine pour l'ingénierie sociale a été dérivée au cours de la thèse, qui est, à ma connaissance, la première de ce genre.

Il est observé que certains traits de personnalité aident à mieux évaluer le comportement en matière de cybersécurité dans une organisation. Des études avec des échantillons de plus grande taille sont nécessaires pour examiner les effets du jeu sérieux. L'observation d'une relation en forme de U entre la capacité d'une personne à repérer et à résister aux escroqueries par hameçonnage et une éventuelle victimisation est un résultat clé qui mérite d'être examiné dans de futures études. Les approches qui mettent l'accent sur les caractéristiques de la personnalité, comme la confiance en soi, pourraient être utiles pour lutter contre la tendance humaine à la fraude par ingénierie sociale. Les résultats de cette thèse aident les praticiens des Forces armées suisses à mieux évaluer le comportement en matière de cybersécurité en fonction des traits de personnalité et des variables de victimisation autodéclarées.

Acknowledgements

Finishing a project like a PhD thesis is satisfying and fills with pride. In my case this has been about three and a half years of work, hopes, doubts, motivation, ambition, setbacks and partial achievements. Prior to starting this journey, I was asked by my supervisor Prof. Stefano Caneppele in summer 2019 to create a risk management plan in order to better foresee and deter any obstacles throughout this journey as best as possible in advance. I remember quite well how thoughtfully I tried to include any potential risk that could hinder me from walking and finishing this path, as I ambitiously planned it to walk. What was perceived as a very complete risk management plan by my supervisor and myself was proofed wrong within the last three and a half years. Pandemics and wars with a potential of a nuclear conflict have not been on my list. The years 2019 – 2022 have put the world society in front of global challenges that have not been there in its extent since generations. Like any other sector, academia had to carry a heavy toll during the CoVid-19 pandemic too. Not only were the majority of curricula taught digitally, but many researchers, also like me, had to cope with setbacks of their research due to restricted access to study participants, funding opportunities or the like. Simultaneously, those three and a half years have been changing my life in various aspects. I started a new job, founded a company, became father of two wonderful daughters. It is therefore all the more important to thank those people that have made this research possible and supported me on my journey to its completion.

First, I would like to thank my supervisor Prof. Stefano Caneppele for his invaluable advice, his superb support and his immense knowledge. Stefano is one of the key persons that made this dissertation possible. His believe in me as a researcher, in my capabilities and in my development potential as criminologist were the starting point for this PhD journey that evolved to be a fascinating tour d'bonheur and the beginning of a professional career track I was desperately looking for prior to taking this direction. My gratitude extends to the jury members of my doctoral committee Prof. Marcelo Aebi, Prof. Marianne Junger, Prof. Olivier Ribaux and Martin Burke for their support, for their critical and reflective feedbacks and for their invaluable advice. Moreover, my gratitude extends to the School of Criminal Justice of the University of Lausanne.

Second, I would like to thank the Swiss Armed Forces for their support of my experimental research conducted with reserve soldiers. First and foremost, I would like to thank General Lieutenant Thomas Süssli for supporting my research request and for making available decisive manpower resources to convert my research idea into an effective field study within

the troop. In this regard, my gratitude extends to various persons of the respective brigade and battalion whom I, due to reasons of confidentiality, do not mention personally, but who would know when reading this acknowledgment. I thank them for their support during the preparation and effective execution of the field study. Without their continuous time and professional contribution, the study could not have been performed in its eventual outcome. I also like to give a special thanks to Brigadier General Hugo Roux, commander of the Military Academy (MILAK) at ETH Zürich, PD Dr. Marcus Keupp and Philipp Fischer for their support.

Finally, I want to express my sincerest gratitude to those persons that have shaped my journey of life during and beyond this PhD path on a personal basis. My thanks belong to Thomas Spichtig who was an important mentor and helped me to discover my interests and strengths so that I eventually came up with the ambition to pursue a PhD with my supervisor Stefano. Additionally, I would like to thank Philipp Leo. Philipp is not only a good friend and business partner, but he is also a knowledgeable, smart, and supporting mentor whom belongs a huge share of this research outcome. Without Philipp, the research at hand would not have taken place in its current form. Last but not least, I would like to thank my family. I thank my parents who always supported me in what I am pursuing and who shaped my ambitious and determined character. I thank my wife who supported me in this demanding task over the last three and a half years, who gave birth to our two wonderful daughters, who encouraged me to contact Stefano and ask him about the possibility of an external doctorate, who gave up additional income and wealth I would have earned in another job without doing this PhD and who loves me the way I am. Nathalie, I love you too. You are my sunshine in the rain, the vigour for my brain.

Wettswil, Switzerland

June 2023

TABLE OF CONTENT

1. Introduction	1
2. Definitions and Concepts	5
Victimisation and victimisation models	5
Personality traits	8
Fraud - A concise historical review	13
Social Engineering	17
Serious Gaming	33
Experimental Research Designs	35
3. Literature Review	37
3.1 Social Engineering & Fraud	39
3.2 Personality Traits & Fraud	41
3.3 Serious Gaming & Crime Prevention	44
3.4 Summary	45
4. Serious Gaming against Social Engineering as Operational Framework	47
Game Design	47
Improved Game Design	49
5. Research Questions and Hypotheses	51
6. Methodology	57
6.1 Research Design	57
6.2 Data & Data collection	60
Sample Recruiting and Characteristics	60
Pre-Experiment Survey	63
Intervention	66
Post-Serious Game Survey	68
Pre- and Post-Test	68
Variables.....	75
Confidentiality and Data Management	76
Dataset of Pre-Experiment Survey	78
Dataset of Test Stages	80
Dataset of Post Serious Game Survey	82
6.3 Analytical strategies	85
6.4 Methodological Limitations	89
7. Results	92

7.1	Personality Traits and SE Fraud Victimization	92
7.2	Personality Traits and Cyberfraud Victimization Behaviour and Attitudes.....	95
7.3	Serious Gaming for Social Engineering Resilience	102
	Cross-Sectional Analysis.....	102
	Longitudinal Analysis	103
	Difference-in-Differences Analysis	106
	Generalized Linear Mixed Effects	107
	Improvement from Pre-Test	107
7.4	General Classification Model	110
	Logistic Regression	110
	Decision Trees.....	112
	Random Forests.....	113
7.5	Power Analysis.....	115
7.6	«What-If» Analysis	116
7.7	Subjective Effects of Serious Gaming.....	120
7.8	Summary	121
8.	A Routine Activity Framework for Social Engineering.....	124
9.	Discussion.....	142
9.1	Research findings.....	142
9.2	Obstacles and limitations	146
9.3	Novelties and achievements	148
9.4	The Way Ahead	152
10.	Conclusion.....	153
11.	Reference List	157
12.	Annex.....	180
A.	A Serious Game for Social Engineering Awareness Creation (Published in: Journal of Cybersecurity Education, Research and Practice: Vol. 2022 : No. 1 , Article 4.)	180
B.	Serious Game Material	200
C.	Excerpt of Pre-experiment survey	220
D.	Ethical approval CER-UniL.....	246
E.	Flyer for participant recruitment	247
F.	Phishing Scenarios	249
H.	Pre- and Post Serious Game survey and Phishing results.....	259
1.	Pre-Serious Game Survey Results.....	259
1.1	Information Security Training and Importance.....	259

1.2	Victimisation	262
1.3	Risky Cybersecurity Behaviours (RCsB)	266
1.4	Attitudes Towards Cybersecurity and Cybercrime in Business (ATC-IB).....	276
2.	Phishing results	289
3.	Post Serious Game Survey Results	290

1. Introduction

More than three thousand years ago the fight for an unconquerable town has been won by tricking the adversary with a genius idea. After fighting for around ten years without successfully conquering the defending walls or beating the opponent's troops, it was an act of reciprocity and pleasantness that allowed the offender to intrude right into the interior of its enemy's premises with devastating consequences for the screwed enemy due to accepting the fraudulent gift.

Fraud is an old phenomenon and at least as old as Greek mythology like in the example above (Cendrowski & Petro, 2012). This story that has been passed on over centuries, written by Homer in his work *Ilias*, is also known as the history of the Trojan Horse. The Trojan Horse nowadays is rather commonly known as a mean method of infecting and exploiting computers, when for example cybercriminals send malicious mails. It is a means to conduct online fraud with the intention to acquire economic gains and it is commonly observed in online banking frauds (Mermod, 2012; Jansen & Leukfeldt, 2015). Although there is neither a joint agreement on, whether this story has been evolved in the way what is common knowledge nowadays, nor whether it is true at all, this story does provide some valuable insights into offender strategies for committing crimes that will lead us through this thesis. In general, there are two main points we can derive from the Trojan Horse example that are of importance in the course of this thesis. First, the human factor is an important component in setting-up effective strategies against fraud vulnerability. In a setting where security measures, and literally speaking, walls are intended to be set so high that you just cannot overcome them, offenders will look for other entry points like vulnerabilities in the human that are easier to overcome with a well-thought-out scamming scheme and that will increase the likelihood of their attack to be successful. In the Trojan Horse example this was obviously the case when the Greeks focused their attack on the Trojans' gentleness, pleasantness and for sure to some degree on their self-perceived invincibility. Nowadays, the most vulnerable link that can be exploited for frauds and in particular for frauds using online appliances is often stated to be the human factor as well (Nohlberg, 2009; Mahfuth et al., 2017; Sharma & Bashir, 2020; Wiley et al., 2020). Technological solutions have advanced and will further advance online security. Nevertheless, internet users can contribute to reduce their own vulnerability towards fraudulent online scams by acquiring a sustainable awareness about the fact that they themselves are often the primary attack vector for motivated offenders (Aldawood & Skinner, 2018; Armerding, 2018). Second, understanding the rationales behind the approach by which the human factor is exploited is a decisive component for the reduction

of individual vulnerability towards such fraud threats. The Trojans have been tricked to believe that the Greeks returned home, leaving them a farewell gift. Imagine a hypothetical situation, where this farewell gift was not attractive enough to be accepted or where the Trojans were simply more suspicious towards the supposed gift. Thus, demonstrating a different more risk aware behaviour and attitude towards the situation. The story might have turned out differently, then. Hence, further exploring the individual rationales that determine victimisation and potential strategies that could reduce the risk of exploitation of the human factor is important to tackle fraudulent offences centred around the human factor.

Frauds that are centred around the human factor and that exploit it are referred to as using Social Engineering (SE) techniques (Mann, 2008; Hadnagy, 2010; Weber et al., 2020). SE uses psychological manipulation to deceive a respective target (Rusch, 1999; Ferreira et al., 2015; Bullée et al., 2015) and it can take on various vectors to carry them out (Krombholz et al., 2015; Mouton et al., 2016). It can use Trojan Horses as malicious programmes attached to deceptive emails, but it can take on a broad diversity of vectors either digital or analogous, with or without the use of technology. A social engineer can use emails, telephone or the direct physical interaction with the victim to carry out the fraud (Hadnagy, 2010; Bullée et al., 2016; Salahdine & Kaabouch, 2019). Recent incidents reflect the variety that this threat poses to organizations and to society. Elderly people, as well as employees are tricked by telephone-based Social Engineering Attacks (SEA) and are defrauded money (Blass, 2017; Hamann, 2017). The 2020 Twitter hack showed the dimension that SEA can have when cybercriminals used SE for hacking around 130 Twitter accounts (Iyengar, 2020). This SEA targeted the accounts of various politicians and celebrities. Their accounts were compromised, and their followers were encouraged to transfer an amount of a digital currency to a respective cryptocurrency account. On July 31st, 2020, the U.S. Department of Justice charged three individuals for their alleged role in the hack (DoJ, 2020). Those three individuals aged between 17 and 20 years. Based on criminological statistics (Killias, Kuhn & Aebi, 2012, p. 194), this corresponds with offender demographics of analogous crimes. Given this, at the time of the writing, most current example of an SE related cyberattack, the SE criminal seems to be not very different in terms of age than suspects of other criminal offences. However, the interconnected digital sphere offers possibilities for offences using SE techniques that are sparsely limited in time and space. This said, it is worth for practitioners and generally speaking for every individual that does not want to be tricked by a social engineer to be aware of those attacks and thus make SE a broader subject of discussion in criminology as well. Passwords,

Antivirus programmes, firewalls and the like are necessary components of building the security walls, reduce the risk of victimisation and to protect the valuable information and data. Nevertheless, as it comes with SE, it is the vulnerability and victimisation of the human factor that is targeted and exploited. A social engineer will exploit this human factor, as “*Social Engineering is all about exploiting social weaknesses, the ordinary weaknesses of you or I...*” (Barber, 2001). To keep it with the metaphor of the Trojan Horse at the beginning, the height of the Trojan walls, the force of their defence weaponry and armed forces have been irrelevant for the protection of their precious assets, when you let yourself being tricked and let in the enemy right through the front door.

At the time I began my research for this doctoral thesis, the exploitation of the human factor was already a severe threat and quite present in the Information Security, as the literature and literature reviews on the topic demonstrate (Mitnick & Simon, 2002; Hadnagy, 2010; Gupta et al., 2016; Aldawood & Skinner, 2018). It was in March 2020 when CoVid-19 hit the whole world and locked down almost the whole world economy. Even the research to this dissertation received a drawback, as scheduled dates for experiments could not take place as agreed, such that the effective completion was anticipated to take some months longer. Nevertheless, the pandemic exposed, that criminals and cybercriminals do use such extraordinary environmental factors for their sake. Although research suggests that there were no new fraudulent approaches but that criminals rather used CoVid-19 as the rationale for their schemes (Cross, 2020), it shows that the amount of reported online fraud and cyber-dependent crime increased during the CoVid-19 pandemic (Buil-Gil et al., 2020). In the United Kingdom CoVid-19 related frauds were seen to have increased by 400% in March 2020 (Georgiadou, 2021). Different law enforcement agencies reported offences that particularly used the topic of CoVid-19 as their primer to trick people and thus succeed with their online, but also telephone-based fraud schemes (BKA, 2020; EUROPOL, 2020; FBI, 2020; KAPO Zürich, 2020; NCSC, 2020). A lot of those crimes, like phishing or other frauds, naturally make use of the manipulative and deceptive SE techniques to frighten and influence people. The Corona CoVid-19 crisis in my opinion implied two major conclusions that are particularly relevant for the research significance of this dissertation.

First, offenders do not care about extraordinary humanitarian situations. Indeed, they used the CoVid-19 crisis for their gain (Boehm et al., 2020). Hence, people have to be aware about the rationales and techniques of SE, they have to be aware about the impact it could have on them, to be prepared to spot potential SEA and protect the financial and information assets

they care about. Organizations and employers in general should be particularly aware of the deceptive SE techniques and the impact it could have on their valuable corporate assets. Employers bear a specific responsibility in making their employees aware of the SE risks, reducing the victimisation risk of their employees not to fall prey for such scams and by this positively impacting the security of their corporate financial and corporate information assets. This rationale puts a specific spotlight on the importance of this dissertation that researches individual differences of SE victimisation and the effectiveness of preventive strategies.

Second, due to the lockdown, the rate of employees working from home took a steep increase and the general outlook for the future shows that people want to work more often from home (Chung et al., 2020; Reuschke & Felstead, 2020). Thus, this could put employees more regularly in a situation where they could be compromised by deceptive social engineers, as an explicit or implicit corporate control environment is not perceivably present. It could be assumed that CoVid-19 contributed to the velocity of the digital transformation. Simultaneously, this forced increase in the speed of digital transformation puts a high importance on the risk of fraud victimisation through SE, as it is now even more important to protect corporate information assets that are increasingly accessed remotely. In particular, the employees accountable for the information assets, such as management and financial employees, are seen to be among those with the highest rate of access to telework (Desilver, 2020). Thus, the opportunities for crimes that are facilitated by manipulative and deceptive SE techniques that victimise employees working from home might see a continued or increased appearance in case no countermeasures are taken. This implies an increased, but at least continuous, importance also for the research conducted in the regard of this dissertation project.

The remainder of this thesis is divided into eight chapters that present the basic definitions and concepts this dissertation utilizes (chapter 2), a literature review of the main concepts of the topics under investigation (chapter 3), , the operational framework of the empirical section (chapter 4), the research questions and the research hypotheses (chapter 5), the methodology (chapter 6), the results (chapter 7), a chapter concerning theoretical considerations (chapter 8), as well as the standard sections on discussion and conclusion (chapter 9 and chapter 10).

2. Definitions and Concepts

The following paragraphs present the definitions and further insights of the main concepts that build the foundation and that will be referred to throughout this thesis. In particular, the thesis deals with victimisation and victimisation models, personality traits, the evolution of fraud, social engineering, serious gaming, and experimental research designs.

Victimisation and victimisation models

Victimology is a relatively young direction (Fattah, 2010). It was not before 1948 that research almost exclusively focused on the offender side in studying crime and deriving policy implications (Fattah, 2010). In 1948 it was Hans von Hentig who first brought to the table the importance of studying the victim side as well, in order to bring a step forward the understanding of the offender-victim interrelation (Fattah., 2010). In his book *The Criminal and His Victim* he specifically proposed to take into consideration the individual vulnerability of people to be victimised. Thanks to this seminal contribution von Hentig is therefore understandably recognised as the father and inventor of the victimological vein (Fattah, 1991; Fattah, 2000; Dillenburger, 2007, Fattah, 2010). Other early contributors in the field that followed the direction paved by von Hentig were Mendelsohn (1956) and Wolfgang (1958). Former primarily focused on the specific typology of victims in the sense that he grouped victims into six different categories. On the one end of the scale ranges the completely innocent victim and on the other end ranges the imaginary victims (Sengstock, 1976). Wolfgang (1958) focused on patterns of criminal homicide with evidence that victims were not always passive recipients of crime.

Since the establishment of the victimology research vein by von Hentig over 70 years ago, the field has taken a tremendous step to advance the knowledge about the victim and to close a knowledge gap in the field (Fattah, 2010). Since then, four main theoretical models drive research in victimology (Lusignan & Marleau, 2010). In the 1970s and 1980s two seminal contributions with continuous relevance have broadened the understanding of what drives victimisation. First, there is the *lifestyle theory* approach defined by Hindelang, Gottfredson and Garofalo (1978) that defines individual's lifestyles and behaviours as explanatory variables for the risk of being victimised. Second, there is the *routine activity theory* proposed by Cohen and Felson (1979). It uses routine activities as a theoretical concept to explain victimisation. Two years after their contribution Cohen et al. (1981) contributed another theoretical concept that is known as the *opportunity model*. It says that the combination of lifestyles and routines

forms attractive opportunities for offenders. The *Dutch model* developed by van Dijk and Steinmetz (1982) defines proximity, exposure and attraction as main drivers of victimisation. Proximity is the social relation of persons in space to one another. Exposure defines the possibility for the offender to conduct a crime when meeting a victim and attraction defines tendencies within the offender triggered by the victim.

In a more recent article Zaykowski and Campagna (2014) evaluate the occurrence of victimology theories based on a content analysis approach of victimology textbooks and group them into different categories. Other classifications of victimology theories have been undertaken by Mawby and Walklate (1994), Fattah (2000) and Wilcox (2010). Table 2.1 presents the classification of Zaykowski and Campagna in an own illustration in more detail. It distinguishes among victim precipitation, exposure/opportunity, learning/culture, control and critical theories.

Table 2.1: Classification of victimology theories (Zaykowski & Campagna, 2014)

Theories	Focus	Author	Year
Precipitation	individual vulnerable characteristics	von Hentig	1948
		Mendelsohn	1956
	homicide victimisation	Wolfgang	1958
	sexual victimisation	Amir	1971
	victim-offender interaction	Luckenbill	1977
	Felson and Tedeschi	1994	
	deviant lifestyles	Sampson and Lauritsen	1990
Exposure and Opportunity	victim lifestyle	Hindelang Gottfredson and Garofalo	1978
	victim routine activities	Cohen and Felson	1979
	social structures	Miethe and Meier	1994
	fear of crime	Tillyer, Fisher and Wilcox	2011
Social Learning and Cultural	acceptance of violence	Wolfgang and Ferracuti	1967
	abusive relationships	Walker	1984
	cultural norms	Anderson	1994
		Berg, Stewart, Schreck and Simons	2012
Control	self-control	Gottfredson and Hirschi	1990
	characteristics of low self-control	Schreck	1999
	low self-control and risky lifestyles	Pratt, Turanovic, Fox and Wright	2014
Critical	victimisation of women	Brownmiller	1975
		DeKeseredy and Schwartz	2009
	abuse of power by elites	Mawby and Walklate	1994

It is fair to say that the classification provided by Zaykowski and Campagna (2014) provides a good overview of the respective theoretical approaches but is neither the only nor the ultimate classification. Different approaches as those by Mawby and Walklate (1994), Fattah (2000) and Wilcox (2010) also would qualify for a theory's comparison. The classification provided above, however, implicitly shows the evolution of the theoretical considerations in victimology. In the beginning of research in victimology, researchers mainly focused on individual characteristics as an explanation for victimisation (precipitation theories). Exposure and opportunity theories on the contrary take into consideration the social contexts that define victimisation. Theories of

lifestyle choices and routine activities take into account structural constraints, amongst others, as victimisation drivers. According to social learning and cultural theories, victimisation is the result of acceptance and regular appearance of crime within a society or parts of a society. Crime is understood to be part of the culture or the societal norms, such that specific victimisation patterns evolve out of these conditions. Control theories assume that victimisation is negatively related to internal and external controls. People with a high self-control, for example, are expected to demonstrate a lower probability of being victimised as those with a low self-control, such as a low level of tolerance or problem solving (Schreck, 1999). Lastly, critical theories look at victimisation from a broader perspective and suggest that it is a result of differences in social groups. Critical criminology therefore examines things like state crime, victimisation of women or crime committed by the rich and powerful (Zaykowski & Campagna, 2014).

Personality traits

Personality is referred to as the field of psychology that investigates “*the thoughts, feelings, behaviours, goals and interests of normal individuals.*” (Watson, 2019, p. 871). Since more than 2’000 years mankind is interested in investigating on the elements that describe an individual’s personality. Hippocrates thought that different body fluids, the so-called temperaments, are responsible for specific phenotypical behaviours (Fazeli, 2012). Galen, a Greek physician, further developed Hippocrates’ theory and introduced his conviction that personality and diseases are based on an individual’s imbalances of the four fluids. He distinguished among the choleric, the melancholic, the phlegmatic and the sanguine persons (Clark & Watson, 2008). This long-lasting theory was taken on and refined by philosopher Immanuel Kant who attached specific traits to the four categories, such as choleric persons being impulsive or melancholic persons being thoughtful (Stelmack & Stalikas, 1991; Eysenck, 2009). Moreover, psychologist Wilhelm Wundt (1874/1886) believed that it is more reasonable to divide the four categories based on two different axes. The first axis distinguishes between strong and weak emotional temperaments (choleric / melancholic vs. sanguine / phlegmatic), whereas the second axis describes the distinction between changeable and unchangeable temperaments (choleric / sanguine vs. phlegmatic / melancholic) (Eysenck, 2006). A different approach to describe personality was introduced by Sigmund Freud in the early 20th century (Freud, 1916-1917). His well-known psychodynamic perspective of personality was inevitably the first encompassing theory of personality. The introduction of the conscious and unconscious

was ground-breaking and although different of his perspectives are rejected or criticized from researchers in psychology nowadays, a lot of his thoughts are still prevalent. But even in his days there was no unison among scholars regarding his perspectives. Despite the general agreement on the importance of childhood experiences as personality drivers, neo-Freudians like Alfred Adler, Erik Erikson, C.G. Jung or Karen Horney disagreed with Freud on his centrism of sexuality as the essential force of explaining personality. In particular, the neo-Freudians believed that the social environment, as well as cultural differences are significant drivers of personality. Adler (1930 & 1961) believed that the power behind an individual's emotions, thoughts and behaviours are feelings of inferiority endured during childhood. Erikson (1958 & 1963) highlighted the importance of social relationships for the personality development and believed that a person's personality develops throughout her or his life. Horney believed that unconscious anxiety, built by unmet cognitive needs in childhood, drives the style of personality (Paris, 1994). Individuals cope with this anxiety either by moving towards, against or away from people (Burger, 2008). Lastly, Swiss psychiatrist C. G. Jung developed his theory of analytical psychology. He put a special attention on the approaches distinguishing the consciousness from unconsciousness. In his opinion, Freud's theory of the unconscious was incomplete as it only describes the personal unconscious and, in his opinion, lacks the collective unconscious (Jung, 1921). The archetypes, as he called them, are those ancestral memories that are commonly shared among society (Jung, 1959). Jung's most important and still prevalent contribution to personality psychology, however, is his proposal of psychological types (Jung, 1921) and the respective approaches to life. The concepts of introversion and extraversion (not extroversion, as it has been manifested in some languages over time. It is, however, extraversion (Jung, 1921, p. 36f.) are common descriptors when talking about peoples' personality and when assessing individual personality. Introverted people derive their energy from their inner psychic activity, whereas extraverted people derive their energy from being with other people.

Beyond those briefly discussed psychodynamic approaches to explain personality, other approaches to explain personality developed over time. In doing so, learning approaches focus on observable phenomena to describe personality. As they can be scientifically tested, they enjoy greater popularity nowadays compared to psychodynamic approaches. Learning approaches generally divide into behavioural, humanistic, cultural and trait perspectives (Dumper et al., 2019). Behaviourists like B.F. Skinner (1953) or Pavlov (1927) think that the reasons for all behaviour lie outside an individual and that the environment, a person is

confronted with, drives the resulting behaviour (Skinner, 1953). Mischel (1968) found that personality traits vary across situations, though are more consistent within situations and that behaviour is also consistent across equivalent situations over time. Humanistic approaches include those of Maslow (1954) and Rogers (1980). Former argued that psychoanalytic and behaviourist approaches do not respect human experience, but that personal experience indeed impacts personality. Rogers introduced the self-concept of the thoughts and feelings of ourselves to personality psychology. Biological approaches argue that personality is predefined through our genetical dowry. Biological predispositions and physiological processes are believed to drive our personalities (Burger, 2008). Cultural learning theories see the driving forces of our personalities in the environmental factors that we are exposed to dependent on the culture we live in (Triandis & Suh, 2002).

Finally, the trait theoretical approach of personality psychology says that an individual's personality can be described by specific traits and ways of behaving. Personality traits are said to *"reflect people's characteristic patterns of thoughts, feelings and behaviours.... Trait psychology rests on the idea that people differ from one another in terms of...basic trait dimensions..."* (Diener et al., 2019, p. 856). In an attempt to summarize all traits that describe an individual's personality, Gordon Allport (1936) identified almost 18'000 English words in the dictionary that could be used to describe a person. Cattell (1946 & 1957) reduced Allport's list to 171 traits and concluded that there are 16 dimensions that describe a person's personality, resulting in his 16PF assessment of personality. In another approach Eysenck (1947) theorized that people range within two specific dimensions, namely introversion/extraversion and stability/neuroticism and that these dimensions quite well describe a person's personality. Nowadays, the most common model of describing personality traits is the Five-Factor Model (McCrae & Costa, 1987; Goldberg, 1990; McCrae, 1992). The so-called Big 5 personality framework is one of the most widely used models for personality research and broadly accepted among scholars (Gosling et al., 2003; Lang et al., 2011; Rammstedt et al., 2012). It summarizes human personality traits under five broad categories (Extraversion, Agreeableness, Conscientiousness, Emotional Stability, Openness), with each having a bipolar counterpart (e.g. Extraversion vs. Introversion). Thus, it is possible to create a comprehensive personality profile of the test taker. In a revision of the Big 5 personality framework, Ashton and Lee (2004 & 2007) made some refinements on some traits and proposed a sixth dimension to the model. Their HEXACO-Model of personality traits builds on the Big 5 personality model, but further entails the dimension Honesty-Humility (see Table 2.2 for the definition of the sixth

dimensions). This dimension maps people on a scale from being fair and modest, when scoring high and being manipulative, narcissistic as well as being self-centred when scoring low. Another personality inventory that is frequently used to assess people is the Dark Triad, though it is looking at what is supposed to define the rather dark side of personality. Paulhus & Williams (2002) developed this inventory to measure peoples' expressions of the personality domains Narcissism, Machiavellianism and Psychopathy. In this regard, the Dark Triad categorizes people by their narcissistic expressions like grandiosity, pride, egotism or a lack of empathetic abilities; by their sense for manipulating other, a moral absence and a high self-interest as Machiavellian characteristic; and lastly by their psychopathic expressions like being antisocial, selfish or impulsive.

As in other domains and fields, there is probably no ultimate right or wrong when evaluating different approaches, but rather a continuous evolution of knowledge, as well as a subjective conviction and believe of appropriateness of theories. It is the beholder's subjective choice and point of view in deciding what the most appropriate tool for a topic under investigation is.

Table 2.2: Personality traits of the HEXACO-Model (Lee & Ashton, 2004)

Personality Trait	Definition
Honesty - Humility	The Honesty – Humility personality domain captures the personality facets Sincerity, Fairness, Greed Avoidance and modesty. Persons who score high in this domain are supposed to be fair, modest, avoid the manipulation of others, are less inclined to break rules, do not feel the need for wealth and do not thrive for social status.
Emotionality	The Emotionality domain incorporates the personality facets Fearfulness, Anxiety, Dependence and Sentimentality. Persons who score high in the Emotionality domain are said to fear of physical dangers, experience anxiety under stress, feel a need to be emotionally supported by others, are empathetic and sentimentally attached to others.

Extraversion	The Extraversion personality domain captures the personality facets Social Self-Esteem, Social Boldness, Sociability and Liveliness. Persons with high expressions in Extraversion are supposed to feel positive about themselves, feel confident in social interactions, enjoy social gatherings and the respective social interactions and are supposed to experience positive feelings of enthusiasm and energy.
Agreeableness	The Agreeableness personality domain incorporates the personality facets Forgivingness, Gentleness, Flexibility and Patience. Persons who score high in these dimensions are supposed to be more forgiving towards others who caused them harm, indulgent in judging others, cooperative and willing to compromise with others and are supposed to be more in control of their temper.
Conscientiousness	The Conscientiousness personality domain captures the personality facets Organization, Diligence, Perfectionism and Prudence. Persons that score high in these dimensions are said to be good in organizing their time and physical surroundings, are disciplined in working towards their goals, put a large focus in accuracy and perfectionism in their tasks and deliberately evaluate options in decision-making processes.
Openness to Experience	The Openness to Experience personality domain incorporates the personality facets Aesthetic Appreciation, Inquisitiveness, Creativity and Unconventionality. Persons with expressions in these domains are supposed to enjoy the beauty of art and nature, are inquisitive, have a good imagination and use it freely in everyday life, and have an interest in unusual ideas or people.

Fraud - A concise historical review

It is probably a hard task to define a specific start date in history when the act of fraud first appeared. Fraud is commonly seen as something unlawful and criminal. A quick look in the Oxford English Dictionary (2022) confirms that fraud is neither an unambiguous term nor a recent phenomenon. It is defined, amongst others, as “*Criminal deception; the using of false representation to obtain an unjust advantage or to injure the rights or interests of another*” or “*An act or instance of deception, ..., a dishonest trick or stratagem. A method or means of defrauding or deceiving*”. This definition carries aspects that are very important for the further understanding of the subject of this thesis as will be resumed in the following subchapter. Social engineers are deceptive tricksters too and thus fraudsters according to the definition above.

Scrolling further through these definitions shows that the English language makes use of the term in these senses since the 14th century. However, it would be careless to say that fraud did not exist before. Obtaining an unjust advantage against someone or something else for personal gains does not seem to be a matter of centuries of human history but rather a fact that is deeply rooted in human nature. Ever since humankind is organized in societal structures, there have been endeavours by people or groups of people to deceive their fellow tribesmen or fellow citizens to gain an advantage over them, may it be for the greater good, for the groups’ or tribe’s sake or just for a personal gain, as is the case in so many instances since money has been invented to attach a direct value to things and people and by this distributes wealth and power. The following lines will present some epochal fraud occasions and will show that generally, fraud has been there since long ago, but that the means by which it is carried out and the names for it have developed as society did too.

It is therefore no surprise that there is evidence that already in ancient Rome and Athens societal phenomena existed that can be considered a fraud in terms of the definitions presented above. Laws against the adulteration of food and beverages already existed more than 2’000 years ago (Sumar & Ismail, 1995), which imply a corresponding and preceding behaviour that was considered as unlawful. Food frauds such as the Melamine scandal in 2008, where milk was diluted with water and melamine was added to stimulate a certain protein content, or the chemical treatment of rotten meat from Brazil in the “Gammelflesich Scandal” of 2017 are therefore no new phenomena. We do not have to jump far in time to present another example of societal behaviour that lawful people would consider as unfair and deceptive. The usage of performance enhancing substances or methods for gain and fame in sport competitions is

nothing new. Competitors in ancient Olympic Games regularly used such methods to defraud their honest opponents for glory (Müller, 2010). The fabulous and glorious ancient time inspired other fraudsters as well. It is probably not a very well-known example among ordinary people, as to us the name of the following person does not come to our mind when we think of famous fraudsters, but rather when we think about famous artists. Probably, one of the greatest of all times. It is said that Michelangelo committed one of the first recorded instances of forgery. He forged an ancient Roman sculpture in 1496 and buried it to make it appear older before selling it as an historical piece. Besides that, Michelangelo is also known as a highly gifted copier. He made a business of copying artists' drawings while keeping the original and selling his copies (Amineddoleh, 2016). Our travel through time takes us to another highly skilled fraudster who made a fortune with faking gold and silver coins. In 17th century, William Chaloner, a counterfeiter and confidence trickster, was the greatest counterfeiter of gold coins and for a substantial period successfully tricked society and parliamentary members in a conspiracy. It was Isaac Newton who was the warden of the royal mint at that time and who finally succeeded in securing a conviction of William Chaloner at a trial in March 1699 (Iliffe, 2009). Although frauds like the one of William Chaloner defraud society by sometimes substantial financial value, the late 1800s and early 1900s inhibited frauds with more severe impacts on society's health. Back then, many medicines were marketed as patent medicines while promising therapeutical effects for the respective illness. In fact, the medicines were neither patented, nor did they have any therapeutic use beyond a placebo effect (Valuck et al., 1992). People are creative to satisfy their need and greed for a financial gain. Around the same time in early 19th century, a couple of men made a business by selling the Brooklyn Bridge to visitors, tourists and other people. One of them, a man named George Parker, managed to sell public structures in New York City for over forty years (Cohen, 2005; Yadon and Smith, 2011). Around the same time, two young women who were geographically separated in Europe and the United States are supposed to be the inventors of a scam that has become famous throughout the last two centuries. Between 1869 and 1880 the first incidents of what nowadays is known as the "Ponzi Scheme" were recorded. In Germany, Adele Spitzeder performed scams that promised large returns on investments that were repaid by continuously using investments of new investors. Similarly, in the United States at about the same time Sarah Howe promised female only investors large returns on their investment that she eventually would not pay back (Zuckoff, 2005). The scheme was later named after Italian businessman Charles Ponzi who in the 1920s deceived various people to make a huge amount of money by promising very high returns with

little risk originated from supposed businesses or business ideas that actually did not exist. One of the latest Ponzi Scheme incidents with worldwide media coverage was Bernard Madoff's multi-billion fraud. In late 2008, he was exposed to have stolen about \$65 billion by using the Ponzi Scheme over years (Quisenberry, 2017). Our journey through time takes us to another prominent scam that is regularly observed even nowadays. Since the 1970s, an African criminal network makes its fortune with the so-called Advance Fee Fraud. It has its roots in Nigeria where the influx of petro-dollars by oil revenues created attractive opportunities to defraud people. In its earliest form, the Nigerian Advance Fee Fraud scheme was a "contact non-violent crime" where the perpetrator meets physically with the potential victim, builds trust and sympathy by telling a hard-luck or business opportunity story. Once the victim is interested, the scammer reverts to the original plan of obtaining money from the victim under false pretences. The scam exists in many other variants and also makes use of technology nowadays (Salu, 2004; Ben Simon, 2009).

Technological innovation brings opportunities and inhibits threats. Society has evolved tremendously with and through technological innovation. The opportunities for criminal motivated people developed likewise. Using standard telephone lines to fool people has become common since the 1980s. Consumer are regularly fooled by criminal networks but also by ruthless companies while promising them attractive deals and products over the phone. Victims are either fooled by having to pay for the phone line connection or by agreeing on fraudulent deals over the phone (Kertz, 1992; Nettleton, 2006). Ever evolving technology provides more attack surfaces for the criminals as well. The processing of digital data exposes enormous opportunities. Credit card fraud where authorization rights of the legitimate credit card owner are compromised and exploited by the criminals for their financial gain are common attacks that involve technology (Barker et al., 2008). Identity theft scams that make use of the stolen identity for a financial profit are nowadays not seldom either (Dwan, 2004). Even natural and societal disasters, such as the CoVid-19 pandemic, are seized to deceive innocent people by exploiting them or their identities with scams that use digital attack vectors, such as phishing (Ma and McKinnon, 2021).

Regardless of the exact attack vector, the appearance over time and space or the technological status-quo, all the provided examples have one thing in common: the perpetrators successfully managed to fool the victims into acting to the offender's advantage. People like Michelangelo, William Chaloner, Adele Spitzeder, Sarah Howe, Charles Ponzi, Nigerian advance fee fraudsters or Bernard Madoff all have these skills in common. This might not be

that clear cut for the food fraud or sport fraud examples. However, those fraudsters also managed to trick people into seeing them as a trustworthy seller or athlete to cheer for or bet for. Otherwise, they would not have succeeded at the first place. These fraudsters know how to build trust and confidence in people such that their potential victims would not discover the fraudulent intention of their initial request. The rationales of these scams have not changed much over time, the tools and tricks that technological innovation has brought along in the evolution of society have, however, broadened the attack surface and the amount of attack vectors. Fraudsters that use these principles to succeed with their malicious campaign are also regularly named as con artists. They are artists in the sense that they very well understand how to persuade people from having confidence into them and their doings. The examples and the literature imply that those artists rather possess a specific set of personality traits and persuasion skills that are consistently inhibited in humankind than that the appearance of the first con artist dates back to a specific point in time. There was, however, an incident that shaped the common understanding of the terminology. In 1849, on a summer day in July a swindler was arrested by the police of New York City. The man was accused to have tricked people out of valuable possessions, such as gold watches. His modus operandi was always the same. He would approach perfect strangers in the streets of New York City and after a little conversation he would ask them: “Have you confidence in me to trust me with your watch until tomorrow?” Obviously, he would never turn back the watch. During his conversation with the perfect strangers the swindler would build trust in the victim that he is an old acquaintance and would convince his victim to be a trustworthy person. Besides building this kind of confidence in the target, he also acted confidentially throughout the whole scam and even actively used the word “confidence” in his swindle, which has earned him the name of the “Confidence Man” (Bergmann, 1969). Around 10 years after his arrest, the modus operandi and the term were common features of society, such that *The Rogue’s Lexicon* defined the term as (Matsel, 1859):

A fellow that by means of extraordinary powers of persuasion gains the confidence of his victims to the extent of drawing upon their treasury, almost to an unlimited extent...

As this definition shows, con artists and confidence men are masters in deceiving their targets into having confidence with them and eventually give away their precious possessions. The essence of fraud is independent of space and time or the geographical location. Neither does the technological status-quo hinder the fraudsters from committing their malicious campaigns. On the contrary, it provides them additional attack surfaces and vectors. Sociological and psychological circumstances effect frauds no matter its appearance:

...almost all fraud can be seen to contain the kernel of the “confidence game” procedure – the creation, by one means or another, of a relation of confidence, through which a swindle is effected. (Schur, 1957)

Social Engineering

Social Engineering (SE) is the deceptive exploitation of the human factor (Mann, 2008; Hadnagy, 2010; Weber et al., 2020) and in this regard links to the previous section. Social Engineers are con artists too and SE is an old fraud disguised in a modern terminology (Manske, 2000; Pimentel and Steinmetz, 2022). SE techniques rely on psychological concepts of influence, which were also the rationale of the successful intrusion method of our Trojan Horse example in the introduction part of the thesis. It is applicable for the Trojan Horse example, but SE techniques are applicable for various kinds of attacks on the human factor, as they target the psychological dimension of a victim. In the Oxford English Dictionary (2019) a social engineer is “*A person who uses centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society*” and has allegedly first been mentioned in 1842 by John Gray. The term *Social Engineering*, however, has, according to the Oxford English Dictionary (2019), first appeared in 1899 and is defined by the Oxford English Dictionary (2019) as “*Politics (orig. U.S.). The use of centralized planning to manage social change and regulate the future development and behaviour of a society*”. In the mid-20th century Karl Popper (1966) in his book “*Open Society and Its Enemies*” spoke about the techniques of SE in the sense of social change based on well-founded instrumental knowledge (Hansson, 2006). Originally, the term is therefore meant to reflect a socio-political normative intention on a macrolevel and does not relate in any way to the modern usage in relation to *Information Security* (IS) and the exploitation of the technology user. However, even nowadays the meaning of SE should not be seen as solely related to IS. As Hadnagy (2021), Bullée et al. (2017) and Mouton et al. (2016) note, SE is a technique of influencing people to reveal information by using *compliance principles*, also known as Cialdini’s *weapons of influence* (Cialdini, 1984 & 2021). The terms *influencing tactics* or *principles of persuasion* are used synonymously. Throughout the remainder of this thesis all those terms are defined as *psychological influencing tactics* (PIT). Ferreira et al. (2015) researched the use of PIT in SE, although limited to the use in phishing attacks. Nevertheless, social engineers use psychological techniques to interact with and deceive their targets (Rusch, 1999). The SE techniques therefore rely on rationales that define the interpersonal communication. Rusch (1999) and Atkins (2013) show that these rationales are properly discussed in the domain of social psychology. Social

psychology is a scientific field looking at the interrelation among humans with a special focus on how people “*think about, influence and relate to one another*” (Myers, 1994). Several authors derived a direct link between the findings of social psychology and the techniques of SE by showing how the process of deceiving people during a SEA refers to principles of human interpersonal, quite often subtle, communication (Long, 2008; Mann, 2008; Raman, 2008; Thompson, 2006; Workman, 2008). The precise description of the basic and most relevant principles of interpersonal persuasion techniques that are also applied in SEA is given in Robert Cialdini’s breakthrough work *INFLUENCE* (Rusch, 1999). Those principles of persuasion are used by everybody in everyday life, consciously or unconsciously, for the better or the worse (like in the case of fraudulent SEA), for selfish reasons or the common interest. Cialdini discovered those principles through various experiments, academic research and insights gained through the exposure to work of compliance professionals in field studies. These principles are the basic rationales of persuasion in social psychology that he observed to be universally valid. Cialdini’s principles of persuasion are:

- 1) *Reciprocation*
- 2) *Commitment and consistency*
- 3) *Social proof*
- 4) *Liking and similarity*
- 5) *Authority*
- 6) *Scarcity*
- 7) *Unity*

Table 2.3 highlights each principle with its characteristics, Cialdini’s guide on how to *protect* against the principle and a constructed example by the researcher of its application by social engineers.

Table 2.3: Cialdini’s “Weapons of Influence” (Source: *Rule & How to say “NO”* - Cialdini (1984); *Social Engineering Application* - own elaboration).

Weapon of Influence	
Reciprocation	
<i>Rule</i>	<p><i>“The rule says that we should try to repay, in kind, what another person has provided us.”</i></p> <p>Reciprocation possesses awesome strength and is probably the strongest of the compliance principles. It crosses distances, cultural differences, time and disconnects even self-interest. The rule enforces unwanted debts. People give back, although they cannot or didn’t like the gift. Reciprocation triggers unfair exchange. The indebting first favour can be independently chosen by the “attacker”, the return favour however can be larger, indeed. The exact extent of the return favour obviously depends on the target’s sense for obligation and probably on how well one matched the personal need for the gift and its personal valuation of what it is worth to the target.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Recognize that the rule is the opponent, not the requester using the rule. • A policy of blanket favour rejection is a choice but is ill advised for situations where they are indeed a favour. • Accept offers only for what they fundamentally are not what they are represented to be. • Learn to recognize, whether the initial offer is a compliance tactic to stimulate larger return favour. • Do not meet a compliance tactics with a favour
<i>Social Engineering Application</i>	<p>A social engineer sends the receptionist flowers thanking for helping with ordering a taxi. The next time the social engineer will use the built trust for asking for a favour.</p>

Commitment & Consistency	
<i>Rule</i>	<p><i>“It is, quite simply, our nearly obsessive desire to be (and to appear) consistent with what we have already done. Once we have made a choice or taken a stand, we will encounter personal and interpersonal pressures to behave consistently with that commitment.”</i></p> <p>Personal (inside) and interpersonal (outside) consistency pressures will lead us to behave in accordance to our earlier final decision. The rule is so strong, as inconsistency is seen as an undesirable trait and a high degree of consistency is perceived as a sign of personal and intellectual strength. Once a commitment is public, you have to act consistent to your commitment. Written statements require more effort than verbal ones and in this regard trigger consistent behaviour, such that commitment is met, and one acts compliant. Commitments are effective when they are made actively, publicly and with effort. However, one thing that is superior to the three mentioned conditions is that commitments are most likely to be met consistently when they stem from an inner choice.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • There are two physical signals that unmask dangerous mechanical consistency. <ol style="list-style-type: none"> 1) When we are trapped into a request we know, we do not want to perform, we usually have an unpleasant stomach feeling. 2) A split of a second before we intellectualize situations, we recognize our evaluated heart feeling. • Train yourself to be attentive, before the cognitive apparatus engages. • Tell the requestors exactly what they are doing by forcing you to act consistently.
<i>Social Engineering Application</i>	<p>A social engineer will acquire written agreement from a targeted person regarding the sale of a specific item. Afterwards the social engineer will enforce minor additional conditions to gather personal information, which the targeted person feels obliged to share for being consistent with the sale commitment.</p>

Social Proof	
<i>Rule</i>	<p><i>“The tendency to see an action as more appropriate when others are doing it normally works quite well. As a rule, we will make fewer mistakes by acting in accord with social evidence than contrary to it.”</i></p> <p>According to the rule, people follow the actions of a herd, as the thing the most people do is perceived the right thing to do. At the same time this is the principles major strength and major weakness. It provides a convenient shortcut on how to behave, but simultaneously makes us vulnerable using the shortcut. The more people behave in the same way, the better the principle works on us. The principle works best under conditions of uncertainty and is most powerful when the herd is characteristically similar to us, making us more likely to follow</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Try to recognize when the underlying data of Social Proof are in error. • Being sensitive for situations where Social Proof autopilot works with inaccurate information (1) when social evidence has been falsified on purpose (2) pluralist ignorance phenomenon. • Social Proof as an autopilot should never be trusted fully
<i>Social Engineering Application</i>	A social engineer convinces a target to release confidential information by stating and showing that others already complied with his or her request.

Liking & Similarity	
<i>Rule</i>	<p><i>“As a rule, we most prefer to say yes to the requests of someone we know and like.”</i></p> <p>The rule of Liking is used in a large number of different ways. However, Cialdini identified, based on accumulated evidence, the appearance of several dominant factors that generate liking. First, physical attractiveness is a strong factor that produces liking for good-looking people in others. Findings suggest that the factor has been heavily underestimated. Second, similarity plays an important role as well. We simply like people who are similar to us. Third, the use of compliments increases the likelihood that we like other people, as we feel flattered. Fourth, we are more probable to like things that are familiar to us, things or persons that we have had contact to previously. Lastly, we like things or people that are conditioned and associated with pleasant experiences or feelings.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Let liking factors work at the beginning. • Concentrate on the effect, rather than on the cause. • Being sensitive for one thing: Do we have come to like the compliance practitioner more quickly or more deeply than we expected?
<i>Social Engineering Application</i>	A social engineer visits the same online platforms as the target, building a relationship based on similarities and later uses the trusted relationship to gather passwords.

Authority	
<i>Rule</i>	<p><i>“In the case of obedience to authority, even a brief consideration of human social organization offers justification aplenty...where a legitimate authority has spoken, what would otherwise make sense is irrelevant. In these instances, we don’t consider the situation as a whole but attend and respond to only one aspect of it.”</i></p> <p>Authority is another strong persuasion principle rooted in the rules of social structures and human social organisations. An accepted system of hierarchy and societal authority leads to situations where what was spoken by persons of authority is not questioned, although it might not make sense. In those cases, only one aspect is evaluated, and the situation as a whole is neglected. Where authority is not given at first, it can be obtained and used by “attackers” easily through small but noticeable characteristics, such as titles, clothes or trappings. Titles imply a specific rank and position, take usually time to achieve and in this regard are a sign of authority. The same rationale relates to clothes. Respected authorities who reflect responsibility are usually dressed in a specific way. Fancy trappings additionally show one’s status or rank and imply authority as well.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Remove the element of surprise, but instead possessing a heightened awareness of authority power. • This can be achieved by posing two questions to ourselves: (1) Is this authority I am confronted with truly an expert? (2) How truthful can we expect this expert to be at this occasion?
<i>Social Engineering Application</i>	A social engineer masquerades as a policeman to induce the target via phone to release the information he or she wants to acquire.

Scarcity	
<i>Rule</i>	<p><i>“Since that encounter with the scarcity principle—that opportunities seem more valuable to us when their availability is limited— The idea of potential loss plays a large role in human decision making.”</i></p> <p>Scarcity is a powerful principle that is frequently used by marketing and compliance professionals in a wide-ranging and diverse field. The principle is so powerful as it operates on the worth, we assign things. It works on our weakness for shortcuts, due to the fact that we value items, which are difficult to possess better than items easily available. A secondary source of power is the loss of freedom. Scarcity means a decrease in available opportunities. People hate to lose freedoms they already have. Scarcity works best when specific conditions are met. Things are more desirable when they become scarce than when it has been scarce already. Moreover, competition for a scarce item enforces the powerfulness of the principle.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Recognizing a rise in emotional arousal from scarcity should be seen as a sign of compliance tactic with a need for caution. • Calm ourselves down and regain a rational perspective. • Asking ourselves why we want the item: (1) for the purpose of owning it – evaluate how much we want to spend for it (2) for the purpose of its function – remember that the item will function equally well, whether scarce or plentiful.
<i>Social Engineering Application</i>	A social engineer researched the needs of a targeted person and sends it a malicious mail stating the scarce availability and the unique purchase opportunity by clicking a link.

Unity	
<i>Rule</i>	<p><i>“People say yes to someone they consider one of them. The experience of “we”-ness (unity) with others is about shared identities – tribe-like categories that individuals use to define themselves and their groups, such as race, ethnicity, nationality, and family, as well as political and religious affiliations.”</i></p> <p>Unity is a powerful principle that is deeply rooted in humans’ psychological self. The experience of “we”-ness has defined our identities and our responses to requests since the tribal beginnings of society thousands of years ago. There are generally two distinctions inhibited in this principle. Unity can be observed in people of some groups with specific shared values, interests or other uniting criteria when people share the feeling of belonging together or secondly a feeling of acting together. Those two factors make it easy for group members to create a shared understanding of beliefs, interests, attitudes, behaviours and eventually creating mutual trust. Typical commonalities can be shared kinship, regional or local heritage, language, nationality, etc. But also shared experiences or attitudes towards politics are unifying factors.</p>
<i>How to say “NO”</i>	<ul style="list-style-type: none"> • Upon receipt of a request of a supposed group member, take a step back proverbially and take your time to process the information. Do not let yourself be trapped into a rush. • Test the supposed group member whether (s)he is really acquainted with specifics of the group. • Verify the request with other group members. Chances are high that not all group members share the same stance but are reacting to the principle instead as well. • Emphasise that despite shared group identities individualism brings variety to the group that ultimately advances the group as a whole.
<i>Social Engineering Application</i>	<p>A social engineer researches any kind of information that can categorize the targeted person to a specific group, tribe, or community. The target person might be part of a specific club, military battalion, religion, ethnicity, company, or fan of a specific sports club. These information can be used by the social engineer to build trust with the target in posing to be part of the same group. Followingly, the trust will be used to start the malicious attack.</p>

Although the seven different weapons of influence have each their own specific characteristics, they all work better under some conditions than under others. “*If we are to defend ourselves adequately against those weapons of influence, it is inevitably that we know their optimal operating conditions, in order to recognize when we are most vulnerable to its influence.*” (Cialdini, 1984, p. 98). For wise compliance decisions, panicky and feverish reactions do no good and will lead us to be deceived, eventually (Cialdini, 1984).

Since Cialdini’s publication, different authors with a special emphasis on psychological deception techniques in SE have elaborated on the PIT concept in more recent studies (Gragg, 2003; Stajano & Wilson, 2009). Gragg (2003) presents a multi-level defence mechanism against SEAs. In this regard, he refers to *psychological triggers*, as he terms them, that foster those attacks to be successful. Those psychological triggers have not been tested by himself, but rather refer to a summary of separate compliance principles. Thus, he specifically makes reference to Rusch (1999) who himself relates to the social psychology of Cialdini (1984). It is therefore no surprise that some of the psychological triggers presented by Gragg read similar to the weapons of influence by Cialdini, not only in their terminology but also in their description within Gragg’s publication. Whereas some can be used fully interchangeably with the compliance principles demonstrated by Cialdini, others also incorporate particular characteristics of the comparable weapon of influence. In general, Gragg distinguishes among seven psychological triggers:

- 1) *Strong Affect*
- 2) *Overloading*
- 3) *Reciprocation*
- 4) *Deceptive Relationships*
- 5) *Diffusion of Responsibility and Moral Duty*
- 6) *Authority*
- 7) *Integrity and Consistency*

By reading through the list of the seven psychological triggers, it is obvious that Reciprocation, Authority and, after further validation, also Integrity and Consistency present weapons of influence already discussed in Cialdini's work. Moreover, the psychological trigger "Deceptive Relationships" is discussed as being a tactic to build relationships for the purpose of subsequent exploitation of the person. This is achieved by a relationship that reflects joint interests or attitudes towards life, such that the target feels alike with the Social Engineer. This said, the psychological trigger Deceptive Relationships therefore, in the opinion of the researcher, does not present a completely new compliance principle, but rather builds on Cialdini's Unity principle and should not be counted as a separate fundamental PIT. This leaves us with three additional psychological triggers presented by Gragg that are new compared to Cialdini's weapons of influence when evaluating their applicability in SE situations. Those psychological triggers are: Strong Affect, Overloading and Diffusion of Responsibility and Moral Duty. They are more precisely described in Table 2.4.

Table 2.4: Gragg’s additional psychological triggers (Source: *Rule – Gragg (2003, p.6-8); Social Engineering Application – own elaboration*)

Psychological Triggers	
Strong Affect	
<i>Rule</i>	<p><i>“Strong Affect is a trigger that uses a heightened emotional state to enable a hacker to get away with more than what would be reasonable.”</i></p> <p>Strong Affect is induced when at the beginning of an interaction strong emotions are triggered by statements that let the victim feel a strong sense of surprise, anger or anticipation. Strong Affect implies counterfactual thinking, which disables the target to think reasonably.</p>
<i>Social Engineering Application</i>	<p>A social engineer can use Strong Affect by calling a victim. The victim is told to have won a prize, which will lead to surprise and counterfactual thinking. The social engineer will then collect personal information to validate the prize.</p>
Overloading	
<i>Rule</i>	<p><i>“Having to deal with a lot of information quickly affects logical functioning and can produce “sensory overload.”</i></p> <p>People become mentally passive when too much information have to be processed at the same time, such that they only absorb instead of evaluating the information. When people argue from new perspectives, people are usually overloaded without enough available time to process the new point of view. Arguments that should have been challenged are more likely to be accepted then.</p>
<i>Social Engineering Application</i>	<p>A social engineer will call a target, pretending to be in an emergency case and provides a lot of information in a short time. The social engineer eventually manipulates the victim to do the things he or she wants them to do.</p>
Diffusion of Responsibility and Moral Duty	
<i>Rule</i>	<p><i>“Diffusion of responsibility is when the target is made to feel that he or she will not be held solely responsible for his or her actions.”</i></p> <p>Although this seems to be connected to Cialdini’s Social Proof principle, moral duty enforces the trigger by taking from the target feeling guilt. The target made to feel that his or her decision is decisive for success or failure.</p>
<i>Social Engineering Application</i>	<p>A social engineer will masquerade as being an employee calling another employee, as he or she supposedly forgot to send an important mail, which is important for the company. The victim has the moral duty to decide about the company’s “success” and about the “colleague’s” job.</p>

In another more recent approach that investigated on the psychological methods of deception in SE, Stajano and Wilson (2009) present principles of human behaviour applied on scam victims deceived by SE techniques. The authors present different scam scenarios that have been tested and performed in the regard of a TV documentary series named “The Real Hustle”. It is a series where one of the authors is acting as a social engineer deceiving random targets with scam techniques. The objective of the show is to educate the spectators about the risks and the methods used by fraudsters or Social Engineers. The paper describes the principles of human behaviour used in those scam scenarios. In general, the authors distinguish among seven different principles like Gragg (2003) did too. Although the naming of the principles does differentiate from Cialdini’s principles as well, some of them do indeed relate to the weapons of influence like already in the case of Gragg. Stajano and Wilson explicitly mention the relation of some of their principles to Cialdini’s weapons of influence. While highlighting only a relation to Cialdini to a specific extent, a closer look shows that those related principles basically reflect the same rationale, however, applied and mastered to the scam and security environment. The authors distinguish among the following principles (Stajano & Wilson, 2009 p. 9-19):

- 1) *Distraction*
- 2) *Social Compliance*
- 3) *Herd*
- 4) *Dishonesty*
- 5) *Deception*
- 6) *Need and Greed*
- 7) *Time*

The authors themselves state that their principle Social Compliance refers to Authority, Herd refers to Social Proof and Time refers to Scarcity of Cialdini’s compliance principles (Stajano & Wilson, 2009 p.20). Additionally, they state that the Distraction, as well as the Need and Greed principle sometimes matches the compliance principle Liking. Nevertheless, the description of the two principles used for their scams does not totally overlap with the Liking compliance principle, such that Distraction, as well as Need and Greed are respected separately. However, the principle Deception deserves some extended critique. While reading through the description of the principle, the reasoning lacks some logic to classify it as a stand-alone principle. The authors themselves state that almost all scams fall under the proposed principle of Deception. In case a principle covers all variations of scams, deception, or compliance

situations, it should be considered as being superior to others. This reasoning holds true when remembering that the usage of weapons of influence or generally speaking the usage of PIT, is an act of deception. This act of deception can be achieved by applying different principles like Authority, Social Proof, etc. and thus they can be interchangeably called a tool for deception. Therefore, classifying the principle of Deception as a tool for deception would cancel itself out of the equation and should not be respected on the same level as the other principles. It should rather be accepted as a superior, general description. Stajano & Wilson's human behaviour Time should be evaluated similarly. The authors were initially unsure, whether this principle qualifies as a behavioural trait. After reviewing the literature, they argue that time plays an important role in human decision-making processes. When forced to decide quickly, humans will act on impulse without thinking clearly about the possible alternatives. Hence, whenever an attacker is putting time pressure on his or her target, it is easier to deceive, as it relies on impulse for conclusions and uses short-cuts for the decision-making process. Interestingly, Cialdini (1984) describes that the compliance principles work, as humans seek short-cuts for convenience. Following the behaviour of a mass of people is a short-cut for a decision-making process, as it is believed that a majority obviously behaves correctly. The word of authorities is less questioned, as the state of authority is a sign of correctness and therefore acts as a short-cut as well. Although a lack of time forces people to use short-cuts for their decision-making process, I argue that this principle is superior to the other principles presented by Stajano & Wilson, as it intensifies the effect of the remaining principles once time pressure is put on the target during the application of any compliance principle. Time should therefore rather be respected as a universal accelerator of deception during a compliance process than as a stand-alone PIT. Hence, this leaves us with three additional principles of human behaviour, namely Distraction, Dishonesty as well as Need and Greed that will be presented in Table 2.5 in more detail.

Table 2.5: Stajano’s & Wilson’s additional principles of human behaviour (Source *Rule - Stajano & Wilson (2009, p. 9;14;17); Social Engineering Application – own elaboration*)

Psychological Triggers	
Distraction	
<i>Rule</i>	<p><i>“While you are distracted by what retains your interest, hustlers can do anything to you, and you won’t notice.”</i></p> <p>Distraction is an ingredient of most magic performances enabling the magician to be “one step ahead”. The distraction principle guarantees the success of this one step ahead strategy. Distracted targets focus on what is most interesting to them and what seems to be the most important action, thus people care about what they want to do and distracts them from the task of protecting themselves. This rule is also highly effective in espionage settings and is easy to administer in a group of Social Engineers.</p>
<i>Social Engineering application</i>	A social engineer distracts the targeted person by randomly starting a conversation or jostle the one and secretly install spying gadgets. More efficiently this is done in a group of two Social Engineers.
Dishonesty	
<i>Rule</i>	<p><i>“Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help once you realize you’ve been had.”</i></p> <p>Anything illegal a victim does will be used against them, making it harder for the victim to seek help once the victim realizes it has been conned.</p>
<i>Social Engineering application</i>	A social engineer sends mails to targets with the offer for free access to pornography entailing a Trojan horse programme. When corporate users fall prey to it, they have strong incentives not to cooperate with the forensic investigator to avoid the associated stigma, even if the incident affected the security of the whole company network.
Need and Greed	
<i>Rule</i>	<p><i>“Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you.”</i></p> <p>The Need and Greed principles covers all the aspects a human needs and desires. People are highly vulnerable, once an attacker targets people’s needs as point of starting the deception.</p>
<i>Social Engineering application</i>	A social engineer targets an employee that is indebted and offers him or her a lottery win, which is obviously faked. The victim will fall for the scam and give the social engineer the envisaged information.

Social engineering relies on the application of psychological persuasion principles. In the literature, different approaches for psychological persuasion are found, with Cialdini’s weapons of influence being the most fundamental ones. Gragg, as well as Stajano and Wilson provide an extended view with a particular focus on SE situations. Differences and similarities of the principles have been discussed and duplicates with the same meaning or principles evaluated as being superior to the rest of the principles have been excluded. Table 2.6 presents the remaining set of PIT, representing different psychological rationales for the concept of SE to be successful:

Table 2.6: Collection of different PIT (w/o duplicates of same reasoning or superiority)

Cialdini	Gragg	Stajano & Wilson
Reciprocation	Strong Affect	Distraction
Commitment & Consistency	Overloading	Dishonesty
Social Proof	Diffusion of Responsibility and Moral Duty	Need & Greed
Liking & Similarity		
Authority		
Scarcity		
Unity		

SE in the modern understanding should reflect a global definition for exercising influence on somebody, such that the person being influenced acts in the intended way. Burkett (2013) even argues that national intelligence agencies should be more aware of Cialdini’s principles in their SE approaches for their agent recruitment. On the contrary, Muhly et al. (2021) give advice on how executives can use the principles to influence a security aware corporate culture. Psychological persuasion techniques that are the fundament of the SE rationale and its deceptive techniques in its modern understanding therefore drive the definition set by the researcher hereafter. Throughout this dissertation the term is used to mean the following:

Social Engineering is a form of carrying out influence on a target person or party with the intention to steer their behaviour in the preferred and envisaged direction in order to acquire and exploit information, with or without the use of technology.

Serious Gaming

The playful process of Serious Gaming derives from the term Serious Game (SG). SG are currently seen as “*games that do not have entertainment, enjoyment or fun as their primary purpose*” (Michael & Chen, 2005; Susi et al., 2007; BinSubaih et al., 2009). Similarly, Vermillion et al. (2017) describes SG as being used “*for purposes beyond entertainment*”. This definition is widely accepted and therefore the most current designation within the evolution of the definition of the term (Djaouti et al., 2011). According to Djaouti et al. (2011), these definitions all have been derived from the one set by Sawyer & Rejeski (2002) who, with their whitepaper, paved the way to the current understanding of applying SG with technology for training and education. The authors made a decisive contribution to the SG industry with their publication. Further, they also invented the “*Serious Game Initiative*” and SG conferences like the “*Serious Gaming Summit*” or “*Games for Health*” (Djaouti, 2011). The origin of the term’s definition and the first use of the term “*Serious Games*” or “*Serious Gaming*” dates back to the 1970s. The first precise specification of the term “*Serious Game*” is found in the work by Clark Abt (1970). In his book “*Serious Games*” he describes the use of games for training and education purposes and how decision-makers in different occupations like industry, government, education and personal relations can be trained by those games and simulations (Abt Associates, 2020). Although nowadays SG are commonly perceived as being related to virtual computer games and, by definition, are assumed to be limited to the digital sphere (Zyda, 2005; Rudman, 2019), the definition originated from Abt (1970, p. 9) is rather open and does not use terms related to technology.

“Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining.”

The fact that SG nowadays are commonly attached to the digital sphere should be contributed to the technological progress since the 1970s and the possibilities of transferring concepts to the digital world rather than thinking that SG are meant to be purely digital. In an offline application of a SG that educated students about the US politics mechanisms, Jansiewicz (1973) researched their suitability for educating people about complex concepts like politics. Games that are played by incorporating human interactions are better suited to teach complex matters (Linehan, 2009; Jansiewicz, 2020). Moreover, interactive experiential learning

methods, like SG are, ideally fit the purpose to assist participants in understanding implicit and subtle concepts, such as deception (Arcos & Lahnemann, 2019).

SG are applied in a broad range of domains, such as military, education, healthcare, communication, politics, etc. (Djaouti et al., 2011). The first specified domains for the application of SG refer to those mentioned by Abt (1970). He explicitly described that they could train and educate decision-makers in different occupations (industry, government, education, etc.). He created different games, digital and non-digital, that were used by schools for educating pupils or by the military for training officers in Cold War simulations (Djaouti, 2011). Since then, SG application has widened and releases of SG accelerated (Djaouti, 2011). The continuous improvement in digital or virtual computer capabilities contributed to this increase as well. Moreover, SG application domains are almost limitless according to Abt’s definition, as their educational and training purpose, fostering an informed decision-making, applies to a vast number of different domains. Almost every domain or industry where knowledge and awareness creation is needed to support people’s understanding of principles, processes and rationales could be a possible SG application area. Current applications of SG were used by scholars for researching human behaviour in emergency scenarios or disaster communication, anti-terrorism training, engineering and information systems, healthcare, military, educational system purposes, the application of SG in environmental contexts, the application in the policing context or for researching the effect of gaming approaches in Cybersecurity trainings. Table 2.7 provides a selection of domains that were featured in academic literature about SG. It is a snapshot of the identified publication domains at the point of writing, and it does not claim to be complete.

Table 2.7: Selected domains of Serious Gaming application in academic literature

Disaster Communication	Healthcare
Anti-Terrorism training	Military
Engineering and Information Systems	Education
Policing	Cybersecurity

Experimental Research Designs

Aspirations to research criminal trajectories and the underlying principles of criminal behaviour have been studied using experiments already since the mid-1930s. The Cambridge-Somerville Youth Study was an “*innovative*” and “*rigorous*” experimental study that is known as being the first experiment focusing on delinquency prevention and the first longitudinal experimental design generating criminological insights (Welsh et al., 2019). Its intention was to experimentally assess the differences in the development of potential delinquent behaviour among a group of boys that were split into an experimental group, receiving a treatment, such as family guidance or medical and academic assistance (McCord, 1959 & 1992), and a control group without support. The idea behind this approach was derived from work of Sheldon and Eleanor Glueck (1936) who say that criminal behaviour often originates from events in early childhood and that preventive stimuli must be given already at this stage. In McCord’s (1959, p. 96) words “*the program must be regarded as a magnificent experiment*” and to be considered a success for its incorporation of a control group and the fundamental insights produced by the collected information that are essential for future studies researching crime prevention.

Other seminal experiments conducted in the field include the Manhattan Bail Project by the Vera Institute of Justice, researching the role of collected, verified information about the convicted person’s character and roots in the community in order to be successfully released on parole (Ares, 1963), the Havant Policing Scheme established in the 1960s looking at the effects of reforms in neighbourhood policing (Neyroud, 2007) and the Minneapolis Domestic Violence Experiment, which “*was the first scientifically controlled test of the effects of arrest for any crime*” (Sherman & Berk, 1981, p.1).

Since then, experimental criminology has gained traction. The establishment of various organizations in the 1990s and 2000s like the Crime and Justice Group of the Campbell Collaboration, the Coalition for Evidence-based Policy, the Academy of Experimental Criminology or the Experimental Criminology division at the American Society of Criminology mainly contributed to the rise of Experimental Criminology (Mazerolle & Bennet, 2011).

Its increase in academic popularity, especially within the last two decades, shows that experimental research designs are an important method to research, amongst others, criminal behaviour, criminal offences and the effectiveness of potential crime prevention programmes. Experimental research designs are usually conducted in field settings outside the laboratory and are profitable approaches for explaining and evaluating the causes of phenomena under investigation (Maxfield & Babbie, 2017). Experimental designs are procedures where one or

more sample groups are treated in a specific way and where the outcome of different treatment measures among a treatment group and a control group is compared against each other to derive conclusions about the treatment's effectiveness. (Fischer, Boone and Neumann, 2014). An experimental study that is most appropriate as primary evidence for the examination of questions of effectiveness is the Randomised Controlled Trial (RCT). RCTs minimise biases by the application of randomisation and using a control group (Greenhalgh, 2010).

Experiments are known to act as a powerful tool for constructing criminal justice policy and can be applied for many different conditions (Weissburd, 2000). The classical experiment is configured in three stages consisting of an intervention stage where the target population is split into an experimental group that receives a stimulus and a control group without receiving the treatment. Pre- and post-test stages measure potential differences in a dependent variable among the experimental and the control group. A central feature of the classical experiment is that the group assignment follows a random allocation process, with the experimental and control group being statistically equivalent (Maxfield & Babbie, 2017). Such randomised experiments are a valuable tool for public policy evaluation (Farrington, Ohlin & Wilson, 1986). Where randomisation of the experimental groups does not take place, the research design is labelled as being quasi-experimental. In general, randomised experiments are less common in criminology research than nonexperimental research methods are (Weissburd, 2000; Farrington & Welsh, 2005). Nevertheless, randomised experiments increased in quantity since the 1950s, with 35 experiments being published in the period of 1957 and 1981, compared to 83 experiments in the period 1982 and 2004 (Farrington & Welsh, 2005). Farrington and Welsh (2005) present a classification they have used to categorize published experiments. They summarize experiments into five categories, namely Policing, Prevention, Corrections, Court, Community but nevertheless state that it is to a certain degree arbitrary and that experiments could be allocated to multiple categories.

Since the 1990s the field of experimental criminology shows exponential growth, which is also linked to the establishment of above-mentioned key organisations, but still few studies, using experimental designs, researched the effectiveness of crime prevention or crime control interventions (Mazerolle & Bennett, 2011). In this regard, some leading experimental criminologists give advice on how to improve the field and what future research designs using experimental methods should focus on for a lasting knowledge creation process.

In a review of randomised experiments, Farrington & Welsh (2005) present an overview of conducted randomised experiments between 1982 and 2004, comparing them to the review

results of an earlier period. They conclude that the significant increase of the amount of performed experiments is good news for the academic field. Theirs review has nevertheless shown a need for studies like the dissertation at hand. They call for more geographical diversity of published experiments, as most of the reviewed studies were conducted within the United States of America, leading to a high geographical homogeneity. They note that researchers are still quite often confronted with multiple hurdles in successfully conducting randomised experiments. A lack of permission and collaboration challenges a successful randomisation process. Additionally, serious differences between assigned treatments and delivered treatments were registered frequently. Moreover, the administration and in particular the reporting of experiments is unsatisfactory, such that often basic information of the samples or the experimental process are missing in the publications. Based on this, a valuable contribution to the field can be made by applying randomised experiments in a setting outside the United States of America, with a thorough experiment reporting and a careful experiment administration, allowing for replication and thus further generalisation of the research findings.

3. Literature Review

This chapter presents the results of a literature review for three main directions of interest, namely social engineering and fraud, personality traits and fraud, as well as serious gaming and crime prevention. The aim of the review was to scan literature to identify studies dealing with the directions of interest and finally highlight research gaps. It was intended to identify literature that investigated the topic of *social engineering* as a technique of *fraud*. Second, it was intended to identify literature that interrelated individual *personality traits* with *fraud*. Lastly, literature that interrelated *serious gaming* as a method of *crime prevention* was searched.

The literature scan was performed by searching the databases for the terms Thus, databases were searched for *social engineering AND fraud*, *personality traits AND fraud* and *serious gaming AND crime prevention*.¹ In the latter case, a search variation between *gaming* and *game* was also applied as different results from these searches were to be expected. Table 3.1 provides an overview of the selected search systems and the respective databases. Insights derived from Gusenbauer and Haddaway (2020) were respected for the search system and database selection.

¹ The literature scan was performed by doing a keyword search of the exact terms and term combination using online search systems and databases

The covered terms of this literature review are each applicable in a broad field of studies, but when combined would reduce the pool of relevant search hits. Apart from the term fraud, the remaining search terms are a combination of two words of which each alone would produce a huge amount of search results not or not directly related to the objectives of this study. It was therefore imperative to choose search systems and databases that are relevant for the field of study, but that also perform effective and efficient searches when using the Boolean operator “AND”, as well as parentheses to retrieve the exact combination of the term. Gusenbauer and Haddaway (2020) show that these requirements are not given for all the search systems they studied. In this respect, an additional remark may be made to Google Scholar and OVID. The authors show that the former search system does not manage to efficiently and effectively perform searches that use Boolean operators and parentheses. The application of those instruments was, however, critical to the review at hand to retrieve relevant results in an efficient way. Google Scholar was therefore not used as a search system tool in the process. The latter, and in particular the database PsycInfo, was included for the search, as some of the search terms also relate to the field of psychology. The search results of the keyword search were, then exported into Microsoft Excel where they were prepared to be sorted in a databank including the author’s name, the publication year, the title, and, where possible, keywords and abstract. For the term social engineering, only literature that used the term in the meaning of the definition presented in chapter 2, was respected. Literature that did not study the term in the sense of a deception technique, but rather as a macro-level normative approach (Popper, 1966) to steer society behaviour, was not respected. Only literature that was available in a language understood by the researcher, that is English, German or French, was kept in the list. Duplicates were also erased from the list. Based on the findings of Gusenbauer and Haddaway (2020) it was assumed that the selected search systems reliably searched the databases for the exact and combined search terms. Consequently, the exact terms should be jointly present in the retrieved results. Their mere presence in the publication does, however, not guarantee a focused dispute with the topic of the terms. Thus, the columns title, keywords and abstract of the Excel lists were searched for the respective keywords and synonyms, like deception or manipulation and their respective adjectives for the term social engineering. The retained results were summarized in an overview list.

Table 3.1: Utilized search systems and databases.

Selected Search System	Database
BASE	Full Index
ERIC	Full Index
JSTOR	Full Index
OVID	PsycInfo
PubMed	Full Index
ProQuest	ProQuest Dissertations & Theses Sociological Abstracts
Science Direct	Full Index
SpringerLink	Full Index
Web of Science	Full Index
Wiley Online Library	Full Index

3.1 Social Engineering & Fraud

The literature search for the respective terms discovered that the general prevalence of literature relating to the search terms has a rather current concentration. The first researcher that discussed SE as a technique of internet fraud was Rusch (1999). Despite a continuous increase of publications in this direction since then, most of the observed literature concentrates on the years since 2010. The screening of the selected literature results in different conclusions. First, Phishing as method of fraud is a frequently discussed topic among the search results (Schipke, 2006; Barnes, 2006; Long, 2013; Ferreira et al., 2015; Choo, 2016; Choi et al., 2015; Sun & Yeh, 2017; Marriot, 2018; Lancaster, 2021). Barnes (2006) and Sun and Yeh (2016) provide insights on how to prevent Phishing. Choo (2016) and Lancaster (2021) research different Phishing detection techniques. Although Phishing uses SE rationales it is, however, only a part of the SE repertoire, though a prevalent and important one. Not surprisingly, other researchers take a broader stance when investigating SE as a technique to conduct fraud (Nagy et al., 2010; Townsend, 2010; Tetri & Vuorinen, 2013; Fan et al., 2017; Junger et al., 2017; Stirnimann, 2018; Böck, 2018).

Second, frauds that use digital means as attack vector receive particular interest in academic literature. Cross (2014 & 2020) researched the online romance fraud and the business email compromise scam (BEC). Other researchers (Algarni et al., 2014; Wilcox et al., 2014 & 2015; Njenga, 2018) investigated the importance of SE in relation to the use of social media and social networking sites. Weber et al. (2020) also explored the importance of SEA on cryptocurrency users. The universal usage of digital and online appliances in business and private sphere is understandably a good reason to investigate SE fraud from this perspective. It

is nevertheless not the only application dimension. Deceptive methods can also be used either as direct or as intermediary non-digital means to gather information. Bullée & Junger (2020) demonstrate the application of SE techniques via telephone, email and person-to-person experiments. Chen (2015 & 2016) researched SE as an attack technique in telecommunications fraud. A fraud where people are lured into divulging information or transferring funds to fraudulent bank accounts. Tabron (2016) investigated the impact that creating urgency in such telecommunication fraud scenarios has. Becker et al. (2010) provided insights on how to detect telecommunications fraud.

Third, SE relies on psychological persuasion techniques as rationales for successfully scamming victims (Atkins, 2013; Ferreira et al., 2015; Bullée et al., 2018). Clearly not all of the viewed literature highlights the importance of the psychological principles behind the fraudulent usage of SE techniques. It is, however, crucial to understand that the fundamental driver of attack success depends on these psychological human elements that drive the likelihood of falling prey to the attacks (Junger et al., 2017; Fan et al., 2017).

Fourth, SE fraud appears to be subject of research in various industries. Kleist (2012) investigated the importance of IT controls of Casino slot machines to counteract SE fraud. Long (2013) for instance discusses the usage of Phishing and SE awareness among financial employees. Einarsen (2019) researched the origin of the wine investment fraud. Hove (2020) researched SE mitigation strategies for the payment card industry. Cross (2020) created an overview of the origin and impact of the business email compromise scam (BEC) that took a large toll on organizations of various industries globally with an estimated total loss of \$26 billion since 2016.

Fifth, researchers use different approaches to look at the topic. Some use qualitative methods like interviews or observations (Einarsen, 2019; Hove, 2020; Trim & Lee, 2019) while others use quantitative methods like surveys or experiments (Barnes, 2006; Longe et al., 2010; Davinson & Sillence, 2010; Choo, 2016; Altaher, 2017; Sun & Yeh, 2016; Moreno-Fernández et al., 2017; Aladawy et al., 2018; Aviv, 2019; Bullée & Junger, 2020; Schneider, 2020). Bullée & Junger (2020) used different experiments to look for the success of SEA in telephone-, email- and person-to-person based scam scenarios. Other researchers used different experimental designs to research Phishing (Barnes, 2006; Longe et al., 2010; Davinson & Sillence, 2010; Choo, 2016; Altaher, 2017; Sun & Yeh, 2016; Moreno-Fernández et al., 2017; Aviv, 2019). McConnell (2020) researched the effect of a security education, training and awareness

workshop on the information security policy compliance of databank administrators in healthcare organizations using a pre- and post-test in an uncontrolled experimental design. Aladawy et al. (2018) tested the effectiveness of a SE serious game in an uncontrolled pre- and post-test experiment to create awareness about SE among participants.

Finally, there are studies that research potential SE mitigation strategies. While some specifically research how to mitigate phishing (Parno, 2006; Moreno-Fernández et al., 2017; Shaw, 2020) others try to provide a more universal mitigation approach. Nagy et al. (2010), Fan et al. (2017) and Hove (2020) elaborated on a broader perspective of SEA and provide different strategies, human and or software focused, that help to prevent SEA being successful. In a similar vein, Bullée and Junger (2020) performed a meta-analysis to study the differences in the effectiveness of SE interventions across different experimental studies, which focused on researching the effectiveness of at least one intervention for reducing SE victimization. They found substantial differences for effect sizes of the survey interventions, ranging from highly effective to showing no effect at all. Moreover, the results of studies with fully randomized study group allocation were found to be not statistically significantly different from quasi-randomized studies or studies that used no randomization at all. Highly intensive interventions and those with more focused content were also found to be more effective to reduce the vulnerability for SE fraud.

3.2 Personality Traits & Fraud

The literature search for the respective search terms has shown that the discussion of personality traits in relation to fraud already appeared in the early 20th century. Hartshorne and May (1928) studied how to measure deception and show that it is the offender's conscientiousness and sensitiveness towards the possibility of being caught that finally helped him or her to get away. Since then, research involving personality and fraud is of increasing importance and comprises different directions and methods. The screening of the identified literature produced different conclusions. First, there are various approaches to look at the interrelation of the two rationales. While most of the publications take a more universal perspective on personality traits in relation to fraud, there are authors that only discuss specific personality traits. Narcissism as a personality trait is of interest to research fraud and white-collar crime (Kent, 2008; Alalehto & Azarian, 2018; O'Reilly, 2018). Many other researchers investigate on the relation of psychopathy and fraud (Haapasalo, 1992; Puig-Verges & Schweitzer, 1996; Bailey, 2017; Lingnau, 2017; Alalehto & Azarian, 2018). More recently, scholars investigated on the third component, Machiavellianism, of the Dark Triad triangle and fraud. Shafer (2018) researched

the impact of Machiavellian personality expressions on taxpayers' compliance. Carré (2020) shows a significant correlation among Machiavellianism and the perception of illegal opportunities for profit. Moreover, the personality dimension Honesty-Humility of the HEXACO inventory was subject to explain different types of cheating and dishonest behaviour (Cropsey, 2018; van Rensburg et al., 2018; Schild, 2020). Purdioux (2015) used the personality dimensions Agreeableness and Openness to explain individual ability of detecting deception situations.

Second, there is a difference in looking at personality traits of the specific individual in the way that the identification of prevalent personality traits can be viewed from the offender's perspective or from the victim's perspective. The former perspective is clearly dominating in the literature, while the victim's perspective is under-represented compared to the research on the offender's personality traits. The offender's perspective is, amongst others, subject to research looking at white-collar crimes (Keen & Fitness, 2011; Perri, 2011; Craig & Piquero, 2016; Ribeiro et al., 2019) deviant tendencies in students (Bailey, 2017), CEO fraud (van Scotter et al., 2018), the possibility to neutralize Dark Triad personality traits for cybersecurity behaviour (Padayachee, 2020) or identifying the HEXACO personality traits prevalent in deceptive offenders (Semrad et al., 2020). Research from the victim's point of view in relation to fraud talks about fraud victimisation in general (van Wyck & Benson, 1997), workplace victimisation (Parker, 2019), online or digital victimisation (Holt & Turner, 2012; Garrett, 2014; van de Weijer et al., 2017; Williams et al., 2017; Annisette & Lafreniere, 2017; Kirwan et al., 2018; Kilovaty, 2019; George et al., 2020). In this regard, literature that takes into account a general perspective of the rationales and principles of deceptive fraud appears to be under-represented. Fischer et al. (2013) investigate on the psychological determinants that are responsible for people falling prey for fraudulent scam communications. Jones et al. (2016) developed a theory based on biological rationales to research the drivers of deception from a victim's perspective.

Third, it appears that there are different approaches in terms of research methodology, particularly in terms of studying personality traits with specific personality inventories. Among the identified literature, there are studies that use personality inventories to research the topic of interest, but most do not use any personality inventory. Mainly three types of personality inventories are commonly used among the publications. The Big 5, the HEXACO and the Dark Triad personality inventory. However, personality inventories appear to be more frequently used to research personalities of offenders than the personalities of victims. For the Dark Triad

this seems reasonable, as the respective included personality dimensions are stated to be typical for malevolent behaviour (Muris et al., 2017; Wright et al., 2017). Big 5 personality traits and fraud are studied in cybercrime victims (van de Weijer et al., 2017), older people's vulnerability to fraud and their personality traits (Xing et al., 2020) or the effect on reflective thought of social media and texting users resulting in moral shallowness (Annisette & Lafreniere, 2017). In another approach, Judges et al. (2017) use the HEXACO inventory to investigate the personality of aged fraud victims. The authors show that older victims to fraud demonstrate a lower level on the Honesty-Humility and the Conscientiousness dimension than non-victims do. Similarly, George et al. (2020) use the HEXACO inventory to complement a measure of gullibility in researching the psychological profiles of students exposed to phishing emails.

Finally, other researchers (Norris et al., 2019) look for specific psychological components that make one vulnerable to internet fraud victimization. In a systematic review they divided among message, experiential and dispositional factors that would define the proneness of someone to fall for this type of fraud. Clearly, personality traits fall under the category of dispositional factors. They identified 21 studies that classify for this category, although not all specifically focus on a personality theory. Those who did, used probability models (Cho et al., 2016), experiments (Pattinson et al., 2011; Hong et al., 2013; Alseadoon et al., 2015) or cross-sectional surveys (Buchanan & Whitty, 2014; Chuchuen and Chanvarasuth, 2015) to perform their research. In further research, scholars particularly look on the relevance of Big5 personality traits and fraud. Shappie et al. (2019) reported a positive effect on information security awareness for people scoring high in the Emotionality dimension, meaning that more fearful and anxious people seem to have a somewhat better awareness towards information security. Strong evidence for extraverted people being at higher risk to experience cybercrime victimization is found in other research studies. Alseadoon et al. (2015) reports that the score of the extraversion scale is positively correlated with individual compliance with phishing scams. Similarly, Albladi and Weir (2017) show that persons frequently engaged in social networks, which is considered with a higher risk of cyber victimization, show higher score on extraversion. Other theories also relate a high score on the extraversion domain with a higher risk of cybercrime victimization (Van de Weijer & Leukfeldt, 2017). Uebelacker and Quiel (2014), Hadlington and Murphy (2018) as well as Shappie (2019) say that there is a positive interplay among the domain Agreeableness and cybersecurity practices. In their opinion, people who are more agreeable might be more likely to show compliant behaviour towards malicious SE requests. People with good ability to self-control themselves and with a

low degree of impulsivity are likely to score higher on the domain conscientiousness and represent careful decision-makers (McRae & John, 1992; Lee & Ashton, 2004). A high score on this dimension is therefore considered to result in better decision and behaviour regarding information and cybersecurity (Bossler & Holt, 2010; Uebelacker & Quiel, 2014; Shappie et al., 2019; Hadlington & Murphy, 2018). Lastly, people that are more open to experience and inquisitive about new ideas and other people score higher on the dimension Openness. A high score is also considered as being positively related to cybercrime victimization (Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017). Indeed, personality traits as predictors for fraud, and in particular SE fraud victimization, have become a popular subject for academic research in recent years.

3.3 Serious Gaming & Crime Prevention

Among the three directions of interest, the literature search on the topic of SG for crime prevention produced the smallest amount of relevant search results. The playful process of using SG as an educational tool is prevalent in literature since the 1970s (Abt, 1970). The small sample of the obtained results shows however that SG in relation to crime prevention is a rather young application of the method. Ruskov et al. (2012 & 2014) developed a SG for the purpose of teaching crime prevention. Wendorf (2016) evaluated the effectiveness of a SG as an “*active entertainment-education*” for preventing the sexual exploitation of children. Lastly, Cozens (2018) researched how the use of gaming engines support the visualization of crime prevention through environmental design.

Obviously, there is no large pool of literature that directly relates SG as a method of crime prevention. Although other publications do not explicitly mention SG for crime prevention, there are some studies that highlight this educational approach for the purpose of anti-terrorism training (Bruzzone, 2009; Sormani, 2016), in the policing context (Sorace et al., 2018; Akhgar et al., 2019) and for making use of it with respect to cybersecurity (Newbould & Furnell 2009; Denning, 2013; Adams & Makramalla, 2015; Olanrewaju & Zakaria, 2015; Beckers & Pape, 2016; Aladawy et al., 2018; Hart et al., 2020). An early and seminal example of a gamified approach that tries to raise awareness for malicious SE techniques among players is the game Anti-phishing Phil (Sheng et al., 2007) developed at Carnegie Mellon University. It is an online game that teaches players ways to identify phishing attacks. The researchers tested its effectiveness by evaluating a player’s ability to spot fraudulent websites compared to the abilities of study participants who did not play the game. The researchers recruited 42 participants on campus who were split into three study groups. Although phishing is a very

prevalent type of SE attack, it is only one attack vector in the malicious repertoire of social engineers. The literature search does, however, show that the overall number of academic contributions in this direction is rather small. The literature that researched the application of SG as a measure of crime prevention has a rather manageable size.

3.4 Summary

The chapter provided a comprehensive and narrative review on the existing literature discussing SE in relation to fraud, personality traits in relation to fraud and SG approaches as crime prevention methods. Throughout the course of the literature review, gaps in the literature have been discovered that will form the research questions and hypotheses addressed in the further sequence of this dissertation.

Literature discussing SE and fraud appears to be a relatively new direction of research with the first noted publication in 1999 (Rusch, 1999), but gained traction especially with the increasing importance of online communication, transactions, and the associated increase of criminal activities in the digital sphere since the early 2000s. Not surprisingly, academic research reflects a focused consideration of SE, and in particular Phishing as a technique of SE, with respect to the online domain. Phishing is without doubt a prevalent scamming scheme and deserves particular focus. It is, however, rather an extract of possible SE techniques than a universal perspective on the rationales behind SE. As SE is a present threat to society and to the economy, it is worth to broaden research on the SE rationale, in order to tailor more effective mitigation strategies against those types of attacks. The literature review has shown that little is known about the individual differences that makes one vulnerable to SEA fraud. Some studies present and discuss the psychological principles behind SE persuasion techniques and research which principles are most effective (Ferreira et al., 2015; Bullée & Junger, 2020), but the victim perspective is however not that readily present in the literature.

Academic studies that discuss personality traits as an explanatory variable for fraud are most popular among the three literature review directions. Personality traits and different inventories to measure them are commonly discussed. The discovery of relations among personality traits and crime, either from the offender or the victim point of view, were already subject of research in the early 20th century. At the same time, efforts to further investigate on the deceptive rationales of the SE phenomena seem to be a promising approach. Different scholars provide insights into the relation between deception and crime, predominantly from the offender perspective. The victim perspective to study fraud scenarios appears to a minor

degree. Although there are some studies that researched the relation between personality traits and vulnerability for SE fraud (mostly Phishing), endeavours to look for interrelations among victim's personality traits and the general psychological deception principles underlying SE fraud seem to have received little attention in academic research so far. Overall, the literature review shows that research focussing on the personality composition of fraud victims is a direction not yet exhaustively researched. Further, the HEXACO personality model (Lee & Ashton, 2004; Ashton & Lee, 2007) is a personality inventory that has received little attention in studying personality traits of fraud victims. More specifically, there are no such studies that look at the interrelation of HEXACO personality traits and SE fraud and IS behaviours and attitudes that are linked with SE victimization. Judges et al. (2017) show that people with a low expression on the Honest-Humility domain, meaning people that are rather unfair, dishonest, wealth oriented and with a high self-esteem seem easier to be scammed. It seems fruitful to use the HEXCO personality inventory for researching individual personality differences of potential fraud victims in a broader and extended manner with respect to SE fraud and with respect to behaviours and attitudes that drive SE victimization.

SG appears to be a promising but under researched tool to be tested as a preventive measure in keeping people aware about specific rationales. The literature review has shown that there are generally only a few studies that explicitly discuss SG for crime prevention. There are more studies that implicitly apply a SG approach to educate law enforcement personnel, educate people against anti-terrorism or use it to convey cybersecurity rationales. The application of a SG approach for SE awareness creation appears to be a field with minor attention. Moreover, the few studies that applied SG for a SE context do either present only a small sample size in the verification process, applied the game in an uncontrolled experimental environment and/or administer the game online. I argue that for counteracting SEAs, which are the result of a creative process of psychological deception and quite often do entail human interaction sequences, it is essential to incorporate the human element in an approach suitable to act as a crime prevention tool, may it online or offline.

Lastly, the literature review has shown that randomised controlled trials are rather scarce among the identified publications. Especially for the domains SE and fraud, as well as SG and crime prevention there seems to be little application of this approach. This view is supported by research of Farrington & Welsh (2005) who show that the field of experimental criminology is growing but based on the review of current publications still lacks extent in terms of quantity, especially outside the United States of America.

The identified gaps in the literature of each direction of interest show that studies exploring SE fraud from an universal perspective rather than specifically looking at attack vectors like Phishing, proposing effective mitigation strategies based on empirical evidence collected during randomised controlled trials and using a SG approach to do so are scarce and even non-existent when taking into account individual differences that could drive the likelihood of victimisation of potential SE targets. The following chapters will provide the fundament to approach these research gaps with an empirical study.

4. Serious Gaming against Social Engineering as Operational Framework

In this section I present the operational framework of this thesis that helps to address the research questions and hypotheses. The operational framework consists of a serious gaming approach that is administered as a training for SE awareness creation. An approach of Beckers & Pape (2016) was utilized, amended, and researched for improvement potentials with a field observation in three samples in research conducted between December 2019 and February 2020 (Muhly et al., 2021).²

Game Design

Chapters two and three already presented the SG prominence as a tool for SE in literature and has shown that it is a rather new evolution of pedagogical instruments for this purpose. Additionally, the review showed that academic literature in the field is relatively small. Academic work that presents SG in the field of criminology, including policing and law enforcement, exists, but none of them uses SG as an interactive experiential learning tool for SE. In order to sensitize people about the concepts of SE and prepare them for the variety of SEA, it is reasonable to integrate an interactive human component like in an offline SG approach. Conveying knowledge and rationales by only putting the player in front of a screen, externalizes the human component and makes it more intangible again. The underlying SG approach therefore is administered as a physical table game. The game is played by teams of 2-3 persons with 4-5 teams per game table and is led by a game master. At the end of the game, each game table has a winner team. The game material and corresponding fictitious game environment consists of a situation plan of a fictitious company (office) and a set of fictitious employees, each characterized by job position, computer skills and personal strengths &

² Annex A provides the associated study with the detailed research design and its results, whereas annex B provides an overview of the utilized game material and data. The remainder of this chapter presents, the initial game design and the improvement potentials derived from the field research, which are applied in an improved SG version that is then tested for its effectiveness as a mitigation measure in the remainder of this thesis.

weaknesses. Additionally, the game set consists of two stacks of cards. There is one set that covers all PIT, which are the foundation of SE deception techniques for building trust. The second set incorporates different SEA. This game material helps people to familiarise with the concept of SE and enabling them to better understand and be able to detect SE attack techniques by putting them into the shoes of a social engineer. The game can be played a couple of iterations. For each iteration, the teams are asked to create a SEA based on the available information. Each team needs to define a target asset they want to “steal” from the fictitious company. This can be financial information, other intangible or physical company assets like patents and important documents or simply passwords. After an initial familiarization phase with the situation plan and the fictitious employees of about 10 minutes, each team draws 3 cards from the PIT and from the attack technique stack. The teams now have to formulate a reasonable SEA, for which they have available about 10 minutes, again. Based on the cards they have drawn, they need to figure out a combination of PIT and SE attack technique that, in their opinion, best fits to one of the fictitious characters. Subsequently, they formulate an attack that incorporates a detailed description on how they deceived one of the characters by using a combination of PIT and attack techniques applied to their chosen fictitious character. After this preparation phase the teams present each other their formulated attack. Each team’s attack gets evaluated by the other teams at the table based on a pre-defined point scale. Therefore, the point rating acts as an instrument of proof, whether the SE concepts and the underlying compliance principles have been understood, correctly. This process is done for each team at the table. Once all teams at the table have been evaluated, another iteration of this process can take place. The team that accumulated the most points over the total of iterations is the winner of the SG per table. Although winning is not the sole purpose of the SG, its playful character and the motivation to perform good, engages participants to familiarise with the concepts. At the end of the SG there is a joint discussion on the participants’ experiences and opinions with the SG, giving them time to reflect and to reinforce the concepts of SE they were confronted with during the game.

Improved Game Design

In the course of a field research with a total of 97 participants in three field observations and unstructured interviews the game design described above was researched for potential procedural and administrative improvements (please see annex A for the detailed research design). It was the researcher's intention to observe participants' game involvement and instruction compliance during the game and to look for improvement potentials that could make it effective as an experiential learning tool and SE mitigation measure. The conclusions that were derived from the field research are presented in Table 4.1 below. They are respected in an improved version of the initial SG design in an experimental application through the remainder of this dissertation:

Table 4.1. Summary of key improvement potential applications for the serious game

Dimension/Area	Briefing	Complexity level	Other
Game Material	Provision of introductory sheet	Provision of target person sociogram in second iteration	
Game Process	Stimulating introductory presentation	Two iterations approach. Mutual attack improvement proposals only in second iteration.	Sustainable training of game masters
Game Purpose			Usage as risk assessment and insider threat detection tool

Besides pure socio-dynamic observations, it was possible to identify valuable insights on how to adapt the layout and the administration of the SG to make it more accessible, less generic and hopefully effective for the purpose of raising awareness among the participants towards the rationales and techniques of SE. Moreover, in two of the three samples the researcher observed deviant behaviour and thoughts, which might hint on the applicability of the game as a detection tool for insider threats.

Based on the research findings, three improvement dimensions were derived: the game material, the game process and the game's purpose. Each dimension can be improved in the

following areas: the briefing, the level of complexity and other. Eventually, I propose the following adaptations for the game. First, to increase participants' involvement and instruction compliance, the players need to be briefed more sustainably. This will be achieved by conducting a stimulating SE introductory presentation and by providing an introductory sheet at the beginning of the game. Moreover, game masters need to be more sustainably briefed, as they take on *focal role in stimulating active learning* (Hart et al., 2020) and thus foster the degree of participant involvement with the game. Second, it seems to be beneficial for the awareness creation process to apply an increasing level of complexity by adding different levels of difficulty during the game process. This implies that, ideally, the game process should convey more than one iteration, whereas in the second iteration players will be provided a sociogram of the target persons as an additional layer of difficulty that highlights the importance of interpersonal trust relationships which can be seized for SE manipulation. Moreover, they will be provided the possibility to propose attack improvements on other teams' SEA during the mutual evaluation phase in the second iteration. This will further deepen participants' reflection and understanding of the rationales. Third, an interesting finding that shows the importance and added value of field observations for research, refers to the observation of deviant intent during the game. In two of the three samples deviant behaviour and deviant thoughts were discovered among a participant, each. In case deviant intentions can be readily observed among participants, the game could act as a method of detecting insider threats by identifying those persons. Game participants who during a playful approach, where everybody can act impartially, show effective, real criminal intentions, might act criminally in other occasions in their daily life as well.

5. Research Questions and Hypotheses

The objective of this study was twofold. First, it is of particular interest to research individual differences in personality and their impact on the proneness towards SE fraud and victimization. Extraverted, open people that are generally trusting, who become easily distracted and perform their duties with a lack of responsibility, might be assumed to be an easier target for social engineers as those who do present characteristics with complementary expressions. Thus, I argue that for a holistic victimisation risk mitigation strategy against SEA, all those dimensions do matter in the assessment of target proneness. There exist a couple of studies that researched the relation between personality traits and proneness to SE online fraud (mostly phishing) (Pattinson et al., 2011; Hong et al., 2013; Chuchuen and Chanvarasuth, 2015; Cho et al., 2016; Judges et al., 2017). Uebelacker and Quiel (2014) proposed a Social Engineering Personality Framework that links the Big 5 personality traits with Cialdini's compliance principles used by social engineers. In another approach, Hadlington (2017) links impulsivity as a personality indicator with attitudes towards cybersecurity and risky cybersecurity behaviour. However, the literature that directly combines and researches the link between an individual's proneness towards SE and different dimensions of personality is rather small. Further to mapping the individual performance in SE deception situations with personality expressions, answering research question I also creates insights on how personality characteristics perform as additional variables explaining the individual proneness towards SE deception rationales.

I: How do individual differences in personality impact the proneness towards SE deception rationales?

Following the above considerations and the research question leads us to the respective research hypotheses. The hypotheses are:

H 1.1: People high on the personality domain Honesty-Humility are more prone towards SE deception rationales.

Lee and Ashton (2004) describe people that score high in this domain as being fair and modest. Those people might possess a well aligned moral compass and could be more prone to deceptive social engineers that ask for help with a supposed legitimate request.

H I.2: People high on the personality domain Emotionality are more prone towards SE deception rationales.

A high score on the domain Emotionality is associated with empathy and attachment to people whereas people low on the domain are considered to have fewer social capabilities (McRae & John, 1992; Lee & Ashton, 2004). Thus, deceptive offenders might find it easier to manipulate people that have a pronounced emotional personality.

H I.3: People high on the personality domain Extraversion are more prone towards SE deception rationales.

A high score on the domain is associated with people who are more outgoing and socially active (McRae & John, 1992; Lee & Ashton, 2004). Extraverted people are said to find it easier to connect with other people. A motivated offender therefore might find it easier too to successfully trick those who score high on the domain Extraversion. Current research on cybersecurity and cybercrime victimization confirms these theoretical considerations (Alseadoon et al., 2015; Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017).

H I.4: People high on the personality domain Agreeableness are more prone towards SE deception rationales.

A pronounced Agreeableness defined by a high score reflects people that are more lenient in judging others and more willing to cooperate with others than do people who score low. Social engineers might be able to trick those who score high easier than the ones scoring low on the domain.

H I.5: People low on the personality domain Conscientiousness are more prone towards SE deception rationales.

This domain maps whether one is disciplined, organized and acts carefully when making decisions or not (McRae & John, 1992; Lee & Ashton, 2004). People scoring low are said to be satisfied with little quality in their doings and make decisions on impulse rather than reflecting them in advance. For motivated offenders such a personality expression might help them to successfully trick their targets. Researchers found positive dependencies among high scores in this dimension and better cybersecurity behaviour (Uebelacker & Quiel, 2014; Bossler & Holt, 2018; Hadlington & Murphy, 2018).

H1.6: People high on the personality domain Openness are more prone towards SE deception rationales.

As the term already suggests, people high on the domain are more open to new experiences and unusual ideas or people (McRae & John, 1992; Lee & Ashton, 2004). People with a pronounced personality expressions in the Openness dimension might be successfully exploited by social engineers in the regard of their deceptive attacks. Openness to experiences is found to be positively connected with cybercrime victimization (Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017).

Based on the above considerations it was of further interest to the researcher to investigate on potential empirical evidence that would enlarge the research performed in the field of personality psychology and cyber victimization. In particular, there was a special interest to look at self-reported risky cybersecurity behaviour and attitudes towards cybercrime and cybersecurity in relation to the collaborating organization that possesses system relevant importance for national security. To the best of my knowledge, there exist no such studies that researched the interrelation among HEXACO personality traits and self-reported risky cybersecurity behaviour, as well as self-reported attitudes towards cybercrime and cybersecurity. The research questions that followed these considerations are thus:

II: Is cyber risk behaviour measured by a self-report inventory dependent on individual personality traits?

III: Are attitudes towards cybersecurity and cybercrime measured by a self-report inventory dependent on individual personality traits?

The researcher derived the research hypotheses following the literature previously presented above. The hypotheses that shall be tested refer to both the relevance of individual personality traits for risky cybersecurity behaviour and to their relevance as predictor for attitudes towards cybercrime and cybersecurity per each dimension of the HEXACO personality framework. Thus, this results in a set of six hypotheses per each inventory of interest:

H II.1: People high on the personality domain Honesty-Humility are less engaged in self-reported risky cybersecurity behaviour.

H III.1 People high on the personality domain Honesty-Humility show favourable self-reported attitudes towards cybercrime and cybersecurity.

Lee and Ashton (2004) describe people that score high in this domain as being fair, modest and have little temptation to break rules. Those people might possess a well aligned moral compass one could say and thus could show less risky cybersecurity behaviours and more favourable attitudes towards cybersecurity.

H II.2: People high on the personality domain Emotionality are less engaged in self-reported risky cybersecurity behaviour.

H III.2 People high on the personality domain Emotionality show favourable self-reported attitudes towards cybercrime and cybersecurity.

A high score on the domain Emotionality is associated with empathy and attachment to people. At the same time, they experience more fear to dangers. (McRae & John, 1992; Lee & Ashton, 2004). Thus, those scoring high might be more careful in their cybersecurity behaviour and show positive attitudes towards cybersecurity.

H II.3: People high on the personality domain Extraversion are more engaged in self-reported risky cybersecurity behaviour.

H III.3 People high on the personality domain Extraversion show less favourable self-reported attitudes towards cybercrime and cybersecurity.

A high score on the domain is associated with people who are more outgoing and socially active (McRae & John, 1992; Lee & Ashton, 2004). Those people might demonstrate less favourable cybersecurity attitudes and behaviours, as it would limit their freedom in connecting and communicating with people. Current research on cybersecurity and cybercrime victimization confirms these theoretical considerations (Alseadoon et al., 2015; Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017).

H II.4: People high on the personality domain Agreeableness are less engaged in self-reported risky cybersecurity behaviour.

H III.4 People high on the personality domain Agreeableness show favourable self-reported attitudes towards cybercrime and cybersecurity.

A pronounced Agreeableness defined by a high score reflects people that are more lenient in judging others and more willing to cooperate with others than do people

who score low. It is probable that those who score high on this domain are more willing to follow cybersecurity instructions and have more favourable attitudes towards these policies.

H II.5: People high on the personality domain Conscientiousness are less engaged in self-reported risky cybersecurity behaviour.

H III.5 People high on the personality domain Conscientiousness show favourable self-reported attitudes towards cybercrime and cybersecurity.

This domain maps whether one is disciplined, organized and acts carefully when making decisions are not (McRae & John, 1992; Lee & Ashton, 2004). People scoring low are said to be satisfied with little quality in their doings and make decisions on impulse rather than reflecting them in advance. People high in this dimension therefore might reflect more favourable cybersecurity behaviours and attitudes. Researchers found positive dependencies among high scores in this dimension and better cybersecurity behaviour (Uebelacker & Quiel, 2014; Bossler & Holt, 2018; Hadlington & Murphy, 2018).

H II.6: People high on the personality domain Openness are more engaged in self-reported risky cybersecurity behaviour.

H III.6 People high on the personality domain Openness show less favourable self-reported attitudes towards cybercrime and cybersecurity.

As the term already suggests, people high on the domain are more open to new experiences and unusual ideas or people (McRae & John, 1992; Lee & Ashton, 2004). People with a pronounced personality expressions in the Openness dimension might therefore be less disciplined in following cybersecurity policies and instructions. Openness to experiences is found to be positively connected with cybercrime victimization (Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017).

Second, SG as an experiential learning tool is relatively new and to the best of my knowledge, there exist no studies in criminology that experimentally research such an approach as a preventive measure against SE. Generally, only a few studies attempted to research its application for SE (Newbould & Furnell, 2009; Olanrewaju & Zakaria, 2015; Beckers & Pape, 2016, Aladawy et al., 2018). Those studies mark the beginning in using gamified approaches for the training of individuals against SE threats.. These approaches added new perspectives to the literature and were innovative. Nevertheless, crime preventive measures require to be

effective in specific situations by, amongst others, enabling potential targets to avoid risky behaviours. Thus, knowing what SE is, is beneficial but does not guarantee correct behaviour in SE situations without being exposed to the rationales and techniques underlying this deceptive approach. It is therefore reasonable to research the effectiveness of a SG as a preventive measure against SE. The research question that follows these considerations is:

IV: Is SG an effective tool to decrease individual proneness towards SE deception rationales?

Following the previous considerations of the respective research question catalyses the research hypotheses. The hypotheses are:

H IV.1 People that have participated in the SG against SE are less prone to SE victimization than those who have not.

An interactive tabletop game that conveys knowledge and the rationales of SE in a playful manner to the participants might be helpful in increasing their resistance against SEA. Thus, decreasing their individual vulnerability to SE deception rationales.

H IV.2 Participants' perceived knowledge gain about SE positively depends on their perceived usefulness of the SG.

An interactive tabletop game that conveys knowledge and the rationales of SE in a playful manner to the participants might be helpful in increasing their resistance against SEA. Thus, decreasing their individual vulnerability to SE deception rationales.

H III.3 Participants' perceived gain in awareness about SE threats positively depends on their perceived usefulness of the SG.

The interactive tabletop game is able to sensitize the SG participants in way that they feel more aware with the topic and SE threats. Thus, creating a basis for resilient behaviour.

H III.4 Participants' perceived likelihood of the training helping them to avoid future SE victimization positively depends on their perceived usefulness of the SG

The interactive tabletop game is able to create confidence in the participants in a way that they perceive themselves less vulnerable to SE victimization in the future.

6. Methodology

This chapter presents the methodology and the approach of the experimental design that empirically investigated the research questions and hypotheses formulated in the previous chapter.

6.1 Research Design

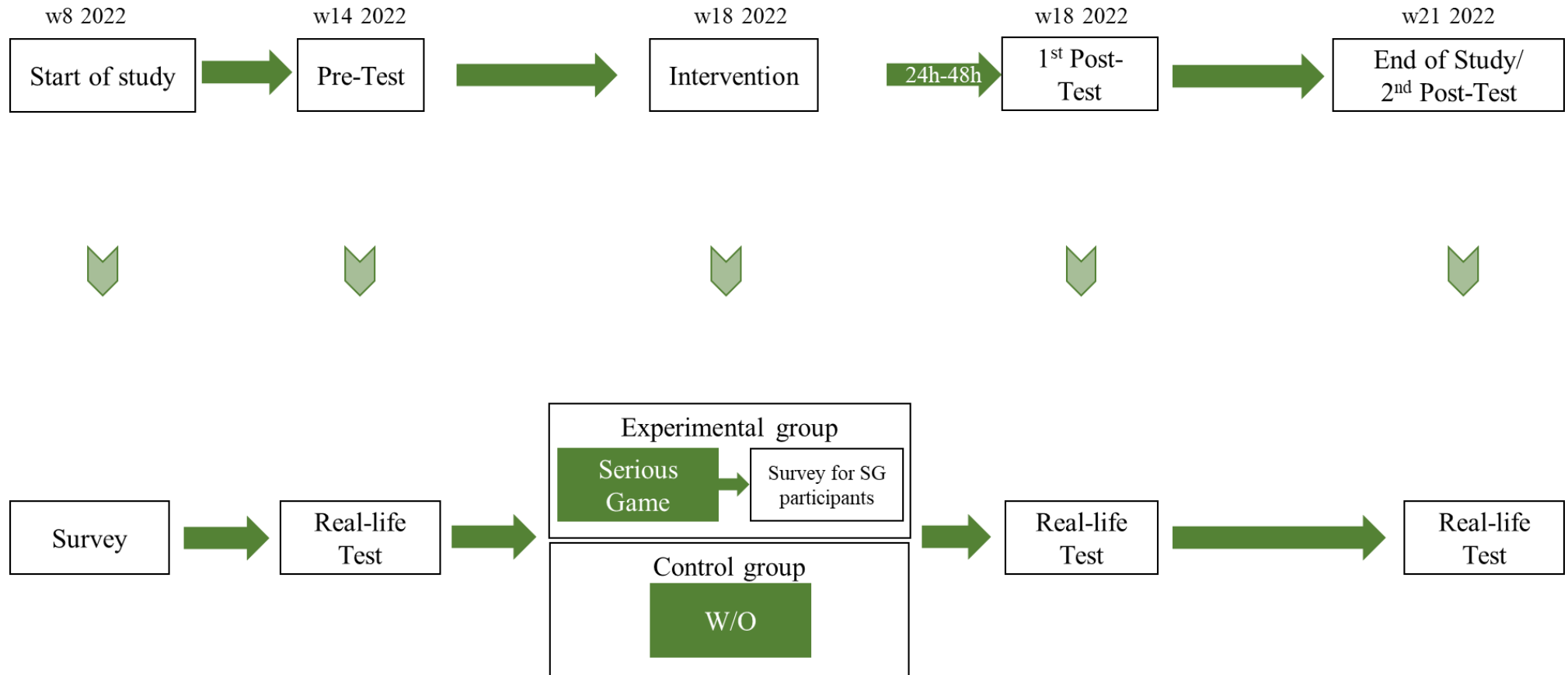
The current study was conducted using a quantitative research approach which included a survey and a classical experiment with an intervention stage, as well as pre- and post-test stages. The survey was used to recruit study participants and to corroborate on research questions I – III and the respective hypotheses by gathering knowledge about participants' personality traits, as well as their cyber fraud victimization attitudes and behaviours. Figure 6.1 represents the outline of the research design. It was intended to produce knowledge about the effectiveness of a serious game presented in the operational framework as a tool for decreasing individual proneness towards deceptive social engineering rationales and about the role that individual factors, namely different personality expressions of potential victims, play as explanatory variable in the course of those deceptive SE approaches. An experimental study that is most appropriate as primary evidence for the examination of questions of effectiveness is the Randomised Controlled Trial (RCT). RCTs minimise biases by the application of randomisation and by using a control group (Greenhalgh, 2010). A RCT was considered an appropriate methodological choice for the research purpose of the study at hand.³

The experimental research design of this study researched the effects of an independent variable, namely the *participation in the serious game* as a stimulus, on the dependent variable, namely the *individual proneness towards SE rationales*. In a control setting, participants did not receive a treatment. For deriving reliable and valid insights on individual proneness towards SE, the application of deceptive techniques had to be as realistic as possible. Independently of doing this explicitly or implicitly, ethical considerations had to be respected. Purposefully using deceptive techniques in an academic setting could be considered as unethical. However, it is especially profitable to produce knowledge about individual behaviour in specific SE situations for the prevention of crimes that use the power of social psychology grounded rationales, rather

³ Experimental research designs are usually conducted in field settings outside the laboratory and are profitable approaches for explaining and evaluating the causes of phenomena under investigation (Maxfield & Babbie, 2017). Experimental designs are procedures where one or more sample groups are treated in a specific way and where the outcome of different treatment measures among a treatment group and a control group is compared against each other to derive conclusions about the treatment's effectiveness. (Fischer, Boone and Neumann, 2014).

than, for example, asking participants about their likely behaviour. The study at hand therefore gathered approval from the ethical commission board of the school of Criminal Justice of the University of Lausanne (see annex D) for the sections of the experimental design that applied the principles of social psychology to test participants' actual behaviour. Moreover, the study and its design were reviewed by the legal department of the Swiss military, the collaborating organization. As this study was supported by the chief of the Swiss Armed Forces and as participants were recruited from a technical battalion of the organization, compliance with organizational standards and regulations had to be respected for safety and reputational purposes of both the organization and the researcher. Thus, recommendations given by the legal department of the Swiss Armed Forces concerning participant recruitment and data protection were respected in the research design. These recommendations referred to the effective method of participant recruitment. The legal department proposed a flyer that would accompany the marching order for the yearly repetition course of the respective battalion as recruiting method. Moreover, data protection and privacy matters were addressed too. The researcher countersigned an ethics agreement among the representing generals (the respective battalion and the Swiss military academy that was the researcher's place of work at that time) and him outlining, amongst others, that any personal identifiable data will only be handled by the researcher and only for the time until the successful completion of this PhD thesis. It was agreed that stored data will be wiped and deleted from all storage media after the successful completion of the PhD thesis.

Figure 6.1: Outline of the research design



6.2 Data & Data collection

Sample Recruiting and Characteristics

The study was conducted in collaboration with the Swiss military between February 2022 and May 2022. The researcher used his affiliation as a scientific collaborator at the faculty of Defence Economics at the Military Academy (MILAK) at the Swiss Federal Institute of Technology (ETH) Zurich to recruit study participants from reserve soldier resources. It was intended to recruit a study population from a technical battalion of the Swiss military that is by nature exposed to information technology systems and to handling important, partially critical, military information. In an informal request, the researcher asked the chief of the Swiss Armed Forces, Lieutenant General Thomas Süssli, for supporting the research. This request was endorsed and contact persons of the respective brigade of interest were accompanying the researcher in his endeavour to carry out the research. After the content and research design was confirmed by the organization, the legal department of the Swiss Armed Forces was consulted to authorize the study and in particular the participant recruitment strategy, as well as the respective data protection efforts. Voluntary participation and an active declaration of consent were key components for the recruitment of study participants. Eventually, Swiss reserve soldiers were recruited by the initial online survey.

Following these administrative requirements, the study was ready to be initiated. Participant recruitment took place by disseminating a flyer (see figure 6.2 and annex E) in February (week 8) 2022 to the members of a specific technical battalion of the brigade in the course of the official marching order for their next service. Prior to sending the flyer, the researcher's counterpart in the brigade created a list of participant-IDs. Each reserve soldier was allocated a unique participant-ID that was highlighted on the individual study flyer. This was necessary to track participants throughout the study. The two-sided flyer appeared in the organizational colour design, presented the purpose, design and requirements of study participation, as well as the individual participant-ID. Interested reserve soldiers were directed to a LimeSurvey questionnaire by scanning the QR-code on the flyer. Prior to topical questions, the questionnaire required the interested participants to read and accept the study information and declaration of consent sheet. By doing so, participants declared their voluntary participation in the study. In the beginning of the questionnaire, participants were asked to provide their participant-ID and their personal email address.

Participant recruitment was active for four weeks between week 8 and week 12 2022. Thereafter, a participant list with email addresses and participant-IDs was generated and sent to the researcher's counterparts in the organization. This step was necessary to initiate pre- and

post-test stages and to correctly allocate voluntary participants to either experimental or control group. The random assignment of participants to either experimental or control group was a desired feature by the researcher for the experimental design. Participants were allocated to either experimental or control group by the researcher's counterparts in the Swiss military while respecting given conditions of the military service that the voluntary participants were obliged to perform during the study. This said, the final experimental design cannot be considered as a randomized controlled trial but a quasi-experiment instead, as the allocation to either the control or the experimental group was non randomized.

Eventually, a group of 182 Swiss reserve soldiers of a technical battalion was recruited. During the experiment, 2 participants requested to opt out of the study (one participant per study group). Hence, the experiment data of 180 study participants were analysed. The experiment was conducted with a treatment and a control group, whereas 138 participants were allocated to the control group and 42 participants to the experimental group due to their availability during the military service. The group consisted of 100% male reserve soldiers with an age ranging between 21 and 36 years of age. Most of the study participants mentioned German to be their first language, whereas 2 said that their first language is French, and 4 participants mentioned Italian as their mother tongue.

Figure 6.2: Flyer for the recruitment of Swiss reserve soldiers



SOCIAL ENGINEERING

Social Engineering – (K)eine Spielerei

Cybersicherheit ist auch menschlich – Ihre Teilnahme an der Forschungsstudie zählt!

Hier geht es zur Studie:

Mit Ihrer Teilnahme an dieser experimentellen Forschungsstudie helfen Sie der Schweizer Armee bei der Evaluation von Verteidigungsstrategien gegen Cyber-Trickbetrug und tragen massgeblich zur Steigerung der Cybersicherheit in der Schweizer Armee bei.

SCAN ME

Ihre Teilnehmer-ID: **001**

Die Teilnahme an der Studie ist freiwillig. Die Studie beginnt mit einer 15-minütigen Umfrage nach dem Scannen des QR-Codes und Ihrer Einwilligung zur Teilnahme an der Studie.

Der Faktor Mensch der Cybersicherheit
 Bei sehr vielen Cyberangriffen ist der Mensch die unmittelbare Angriffsfläche für Cyberkriminelle und für andere motivierte Akteure. Im Rahmen von sogenannten Social Engineering Angriffen erlangen Angreifer durch Methoden des Trickbetrugs Zugang zu Informationen, die Sie für finanzielle oder Spionage-Zwecke verwenden können. Auch Verteidigungseinrichtungen bleiben vor solchen Angriffen nicht verschont. Effektive Verteidigungsstrategien gegen solche Angriffe sind immer noch Mangelware. Diese Forschungsstudie leistet einen Beitrag dazu, dies zu ändern.

Ziel und Verwendung der Forschungsstudie
 Das Ziel der Forschungsstudie ist es, die Effektivität eines interaktiven Brettspiels mit Rollenspielcharakter als Methode zur Verringerung der persönlichen Anfälligkeit für Cyber-Trickbetrug experimentell zu testen. Ihre freiwillige Teilnahme an der Studie unterstützt uns, Verteidigungsstrategien gegen solche Angriffe zu evaluieren und zu verbessern. Mit Ihrer Teilnahme an der Studie tragen Sie massgeblich zur Steigerung der Cybersicherheit in der Schweizer Armee bei.

Ablauf der Studie

- QR-Code scannen (bitte halten Sie Ihre Teilnehmer-ID bereit und bewahren Sie diese auf)
- Durchlesen der Information zum Forschungsprojekt
- Abgabe der Einwilligungserklärung zur freiwilligen Teilnahme
- An Umfrage bis **spätestens 28.01.2022** teilnehmen
- Einen halben Tag Ihres WKs an einem Brettspiel mit anderen Kameraden teilnehmen (effektive Zuteilung durch Kdt. ██████████) ... und
- ...das Spiel ist aus!

Weitere Informationen zur Studie

Die Studie umfasst Fragebögen, Cyber-Trickbetrug Tests sowie ein interaktives Brettspiel. Der Fragebogen beinhaltet demografische Fragen, Fragen zur Selbstwahrnehmung und zur (Cyber-)Risikoeinstellung. Bei bestimmten Fragen steht es Ihnen frei, nicht zu antworten. Hierzu klicken Sie bei der betreffenden Frage einfach auf „Weiter“.

Ihre Daten werden gestützt durch Art. 4 Abs. 5, 13 und 22 des Bundesgesetzes über den Datenschutz (DSG/RR 235.1) erhoben und lediglich durch den Studienleiter bearbeitet.



Pre-Experiment Survey

The study started with a questionnaire (see annex C) (Fig. 6.1). The online administered survey was active during four weeks between February 25th, 2022, and March 27th, 2022. This pre-experiment survey served two purposes: participant recruitment and data gathering. Recruiting participants without obliging them to participate was a main challenge. Based on a consultation with the legal department of the Swiss Armed Forces and in accordance with ethical guidelines in academics, the online survey served the purpose of recruiting reserve soldiers. Voluntary participation with an active declaration of consent was key to recruiting participants. At the same time, this provided the opportunity to gather data about the voluntarily participating reserve soldiers. The main data of interest were personality traits to solve research question I-III. The survey also collected data on other individual characteristics that could provide interesting results and an added value for the Swiss Armed Forces. Hence, data concerning dimensions, such as cyber risk behaviour or attitudes and victimization patterns were collected too. The inclusion of these dimensions created the opportunity to elaborate on research questions II and III.

The questionnaire was administered by using LimeSurvey. In total, the questionnaire incorporated 129 questions in 5 sections. The arithmetic mean of processing time among recruited participants was 21 minutes and 42 seconds. While the survey was accessible via a QR-code, it is fair to believe that participation was mainly conducted using mobile devices. It was administered by a question-by-question structure without allowing backward navigation. It was intended to avoid revisions of previous answers and top-down selection of the same answer when answers would have been presented group by group. However, by doing so the click and selection process increased significantly. The QR-code for accessing the survey was scanned 276 times of which 182 totally completed the survey and 94 only partially and/or repeatedly took part in the survey.

The survey was administered in different languages. Participants had the opportunity to take the questionnaire in 3 of the 4 Swiss national languages, namely German, French and Italian as well as in English for respondents that are not fluid in one of the three languages mentioned before. However, the majority 96.7% of study participants answered in German, which is not a surprise given the fact that the battalion is predominantly German speaking too. In terms of layout, the survey was held simple without the use of too many colours or fonts. Bolding of text was used for each section heading and the key elements in the question, as well

as a minimum of text was intended to be employed making the questions easier and faster to read, yet understandable (Maxfield & Babbie, 2017, p. 236 ff.). The survey was completely built via LimeSurvey⁴. LimeSurvey is an online survey site that allows the easy and fast creation of questionnaires and provides various templates and analysis tools, making both the creation and analysis process easy and efficient. The questionnaire was tested by the researcher and colleagues prior to the usage in the study. The questionnaire incorporated the standard section asking for specific demographics like age, gender and mother tongue. Moreover, in this first general part of the questionnaire, participant-ID and email address were asked for too. It was asked to input the unique participant-ID that participants were provided the flyer prior to the experiment. This procedure allowed to distinguish among treatment and control group participants, as well as instrumentalizing the variables that define their belonging to the respective group in retrospect. Additionally, participants had to answer questions about prior experiences with information security trainings and their individual opinion about the importance of information security in personal and military settings. The survey consisted of consecutive sets of closed-ended and multiple-choice questions which are less complex and faster to answer by the respondents. Moreover, closed-ended questions are easier to compare and therefore simplify the analysis process.

The second and third group of questions reflect explanatory variables, that illustrate individual differences in personality expression and individual victimisation. Personality trait questions were based on the HEXACO inventory introduced by Ashton & Lee (2009). This 60-item (HEXACO-60) based inventory is a reliable tool to measure the personality framework that summarizes human personality under six broad categories (Honesty-Humility, Emotional Stability, Extraversion, Agreeableness, Conscientiousness, Openness), with each having a bipolar counterpart (e.g. Extraversion vs. Introversion). Moreover, the HEXACO-60 allows to further refine each personality category in four facet-level-scales. Under the Honesty-Humility domain the facets sincerity, fairness, greed avoidance and modesty are summarized. The usage of the HEXACO inventory for researching fraud victimisation is accepted among scholars and already has received attention (Judges et al., 2017; George et al., 2020). Based on the HEXACO, the questions were administered with responses on a 5-point Likert scale: (5) Strongly Disagree, (4) Disagree, (3) Neutral (neither agree nor disagree), (2) Disagree, (1) Strongly Agree.

⁴ <https://www.limesurvey.org/de/>

In the third section, study subjects were asked questions about victimisation. In a set of 5 questions, personal victimisation with respect to fraudulent information requests via email communication was assessed. Participants had to answer questions about whether they in the last 12 months have ever received information requests via email, opened them or answered to those requests and if so, how often this was the case in the last 12 months and whether they reported the case to the police or not. Moreover, the perceived future victimisation concluded this section. Personal perception of future victimisation reflects past experiences but also to some degree the fear of future victimisation. Research shows that fear of crime is a good indicator of past personal victimisation or victimisation among family members that are supposed to share common beliefs and attitudes. Fear of victimisation therefore provides a good approximation of future victimisation (Killias, Kuhn & Aebi, 2012, p. 348 ff.).

In two concluding sections, the questionnaire assessed participants Attitudes towards Cybersecurity and Cybercrime in Business (ATC-IB) with a set of 25 questions on a 4-point Likert scale and Risky Cybersecurity Behaviour (RCsB) with a set of 20 questions on a 7-point Likert scale. The set of questions refer to the questionnaires developed and validated by Hadlington (2017) in prior research. In his publication he presents the application of the ATC-IB and RCsB inventories. These inventories provide a “*further step in understanding individual differences that may govern good cybersecurity practices*” (Hadlington, 2017, p.1-2) and therefore provide a good tool to be used for the objectives of this study as well. The ATC-IB consists of 25 items evaluated on a 4-point Likert scale: (4) Strongly Disagree, (3) Disagree, (2) Agree, (1) Strongly Agree. Based on the outline of the inventory, advantageous cybersecurity behaviour correlates positively with the achieved score in the inventory. Thus, the higher the score a participant achieves, the more positive his/her engagement and higher the attitude towards cybersecurity is and vice versa. The particular application of the inventory in a military environment implied that the questions had to be adapted slightly. Terms like *company* or *management* had been replaced by *army* or *military command* respectively. For instance, instead of asking survey takers: (2) *I am aware of my role in keeping the **company** protected from potential cybercriminals*, survey participants were asked (2) *I am aware of my role in keeping the **army** protected from potential cybercriminals*. The RCsB consists of 20 items, asking the participants how often they engaged in risky cybersecurity activities in the last 6 months, with response opportunities ranging on a scale from 0 – 6 (0 = never and 6 = daily). For instance, participants were asked how often in the last 6 months they were *using free-to-access public Wi-Fi*. The higher the score in the RCsB, the riskier the cybersecurity

behaviour of the respondent. Finally, the survey was closed with a thank you note for participation.

Intervention

The intervention consisted of the serious game as presented under section 4. Before the actual intervention was given as experimental treatment, the respective game masters had to be trained. The actual SG was administered by three game masters in each SG setting. Each of them took control of a game table with up to 8 participants grouped in teams of two to three participants. The game masters were all male, aged between 25 and 36 years and had no direct relation to the battalion or the Swiss Armed Forces during the period of the study. These facts were important to limit instrumentation and authority bias that could have been present in case the game masters had a direct relation to the battalion or any military function and rank superior to the participants' rank. Another potential threat for the validity of the study could have emerged from the ability of the game masters to administer the game table. In prior research (Hart et al., 2020; Muhly et al., 2021) argue that game masters obtain a vocal role in the proceedings of the game with respect to participant involvement and knowledge transfer. Thus, the game masters that were subject to the experiment received a collective introduction to the game and the game proceedings, such that they were in possession of a common pool of didactical and informational instructions, as well as familiar with their tasks throughout the game. The game masters were trained by the researcher on their specific tasks during the game in a game master instruction training on April 21st, 2022. The game masters were trained by following the exact outline of the intervention. First, they were confronted with the introductory SE presentation before playing the full game (2 iterations) as described in 5.2 and in annex B. Afterwards, the researcher was explaining to them their precise tasks and responsibilities during the game. Finally, the game masters received a detailed instruction cheat sheet (see annex B.2) for utilization during the intervention that served the purpose of standardizing the game proceeding and instruction process as best as possible. The actual intervention stage as the third procedural component of the research design took place on May 4th, 2022. The 182 study participants recruited with the pre-experiment survey were distributed into an experimental and a control group. The allocation of the participants to either group was performed by the responsible counterparts of the battalion taking account of the actual military service plan.⁵ The organizational fact that only soldiers that were currently active in service were able to be

⁵ The researcher did not have any influence of the effective allocation other than asking the responsible military counterparts to make safe that groups are evenly distributed as best as possible.

ordered the participation in the game limited the ability to distribute the study population into even samples.⁶ The remaining study participants were at the time of the planned intervention not in service, but in their regular job, and could therefore not be approached to take part in the serious game. Thus, the experimental group consisted of 42 study participants. They received as a treatment the social engineering serious game as described under the operational framework in section 4 and in annex B. There were two SG administrations. Group A performed the SG in the morning session between 8:00 and 12:00, whereas the second experimental group, group B, received the SG as experimental intervention in the afternoon between 13:30 and 17:30. By doing so, the researcher aimed to limit diffusion bias, as there was only 1.5 hours in between the two SGs that would limit the possibility to exchange information among participants. The serious game was administered in a bright and climatized room with three pools of tables providing enough space for 8 players and one game master. The game started with a joint introductory presentation of the SE rationales and specific case studies before each game table played two iterations of the game. A 15-minute break was given between iteration one and two. Time was kept centrally in each of the game's different stages, ensuring that the tables concurrently started and finished the game. The game material was distributed by the game masters to the groups of players after the introductory presentation and was collected after the game officially finished. Consequently, it was avoided that single study subjects familiarized with the game material prior to the start of the game or took with them game material what could have effects on their performance in the post-test surveys.

The control setting consisted of a group that did not receive the treatment. The administration of a control group served two purposes. First, the control group allowed to control for any effect the experiment itself had on the participants. Second, it allowed to compare the performance of experimental group participants and control group participants with respect to the effectiveness of SG for SE in reducing individual proneness to SE rationales.⁷

⁶ However, research shows that uneven distributed samples might even give more power to the study results, when the control group is larger than the experimental group (Riniolo, 1999; Oldfield and Haig, 2016).

⁷ Other researchers used different techniques as experimental treatment for testing its effectiveness in SE related situations. Heartfield et al. (2016) used a security education to test its effectiveness against semantic SEAs. In similar SE experiments (Aburrous et al., 2010; Ivaturi, 2014), participants had to actively distinguish among fraudulent and harmless emails or websites. Subsequently, the researchers analysed the differences among the control and experimental group in post-tests. Bullée (2017) conducted different SE experiments using leaflets, posters and security awareness trainings as an intervention. Beckers and Pape (2016) experimentally tested the effectiveness of a SG for SE as an intervention strategy with a small population size in an uncontrolled setting in an academic environment.

Post-Serious Game Survey

Directly after the completion of the SG intervention, experimental group participants were asked to fill out an online questionnaire administered in LimeSurvey about their experience and satisfaction with the SG administration. The questionnaire consisted of 10 questions and participation took around 3 to 5 minutes. Annex G shows the content of the questionnaire. Experiment group participants were able to access the questionnaire via a QR-code projected at the wall in the room where the SG was conducted. For the case that participants did not have their smartphone with them, each game master was provided the questionnaire on paper for distribution and subsequent collection. Participation in the survey was voluntary and the researcher did not instantly control whether all experimental group participants successfully filled it out. However, none of the 42 participants denied filling it out, such that a complete dataset of 42 respondents was derived. The questionnaire intended to ask them different questions about their satisfaction with the training, the usefulness of the content and their perceived likelihood of being resilient towards SEA due to their participation in the training. The training consisted of the introductory presentation and the SG. Questions were structured accordingly. Participants were asked to input their participant-ID at the end of the questionnaire, though on a voluntary basis. Thus, a direct link with the post-test phishing performance could not be established for the whole sample, as some of the training participants chose not to disclose their participant-ID. Additionally, they were asked questions about game improvement potentials.

Pre- and Post-Test

The pre- and post-test stages each consisted of phishing mails that intended to test participants' proneness to fall for PITs, implemented into a realistic phishing scenario, before and after the intervention.⁸

The pre-test phishing took place on April 8th, 2022, whereas the post-test phishings took place on May 6th, 2022, and on May 27th, 2022, for the second post-test. Each of them was sent on a Friday like is so often the case in the real world to induce pressure and increase information

⁸ Different researchers (Jagatic et al., 2007; Mohebzada et al., 2012; Butavicius et al., 2016; Bullée, 2017) used phishing to test study participants' proneness to SE. Although phishing is not the only vector to carry out SE rationales, it has certain advantages for conducting research on the topic. First, phishing is an easy to apply method of testing the proneness, as it does not require large amounts of manpower. It is easily scalable, and a large number of recipients is simultaneously approachable in contrast to individually administered SEA over telephone or in person. Second, it is relevant. Despite its advantageous applicability in academic research compared to the beforementioned other SE forms, it is also highly relevant in practice. Phishing is one of the most used vectors for cybercriminals to gain access to potential victims, their financial possessions and their information. According to Proofpoint (2022), 83% of respondents in their 2022 State of the Phish Report experienced a successful email-based phishing attack in 2021.

asymmetry by taking away the possibility to directly raise some suspicion to fellow workers or in our case soldiers about the email receipt. The technical implementation and execution of the phishing was performed by a vendor of the Swiss Armed Force's cybersecurity and awareness team who have no direct relation to the battalion. The researcher created four (4) realistic phishing scenarios that each applied PIT(s) and asked mail recipients for information that were requested to be inputted by clicking a link in the mail (see annex F). There were two purposes for this rationale. First, it was of interest who and how many study participants would click the link and thus would fall for the phish as they assumably trusted the sending mail address and/or the scenario described in the mail.⁹ Second, once tricked participants clicked the link, they were requested to input specific information such as name, location of military service, subjectively perceived physical and digital security risks, or other personal identifying information that would threaten the battalion's information security on a dedicated landing page.. In each phishing scenario, mail recipients were explicitly requested to follow through with the demanded action within 72 hours. This addition served two purposes. First, it created urgency and implied the overarching principle Time of the PIT repertoire. Second, it served operational and validity purposes. In this regard, results of the pre- and post-tests were downloaded and stored 72 hours after the phishing mails had been sent. Participants that fell for the scam after the 72 hours were not included in the results. However, defining a precise period of data collection that is standardized among the different pre- and post-test data collection processes was imperative for a valid comparison of the results among the test stages. The four phishing scenarios were proofread by the cybersecurity and awareness team of the Swiss Armed Forces and were discussed with the phishing service vendor for its reasonableness and implementation adequacy. Based on the team's experience with internal phishing campaigns, it appeared that the scenarios were rather sophisticated and would imply a high phishing success rate. On a scale of difficulty from easy (1) to very difficult (5), the team rated the researcher's phishing scenarios as very difficult (5) compared to the usual phishing campaigns conducted by them. They advised the researcher to aim for scenarios that would reflect a medium difficulty (3). However, the researcher chose to conduct the experiment with the initial scenarios to apply the highest degree of difficulty and accordingly test the effectiveness of the serious game under this condition. Figures 6.3 to 6.5 and annex F show the initial phishing scenarios that were eventually applied in the research and the respective landing pages as well. The screenshots of

⁹ There is evidence (Abraham & Chengular-Smith, 2010; Wüest, 2010; Liu & Zhong, 2017; Zimba, 2017) that even clicking a link may infect a user device.

the phishing emails and landing pages were taken by the researcher from the test emails that were sent by the service provider to the researcher prior to sending the emails to the study participants. Upon receipt of the test emails, the researcher was confused by the adding “Difficulty 3” in the title of the email. Initially, the service provider stated that the scenarios, as created by the researcher, would reflect a difficulty of 5. The researcher reassured himself by asking the service provider about that fact. The service provider confirmed that the scenarios as created by the researcher and as were eventually sent to the study participants reflected difficulty level 5. The adding to the title in the test emails only reflected the standard used in test mails. Landing pages of the links where information was requested to be inputted, were created by the vendor too. Moreover, it was also controlled for mail receipt information to reduce the probability of deriving false conclusions in case not clicking due to not receiving the phishing mail at all was interpreted as not being prone to the phish. Overall, it was a beneficial opportunity for the researcher having access to this service. The professional service and experience of the vendor that offers phishing penetration tests as its product provided a certain degree of execution security and professionalism to the study. Prior to the execution of the pre-test phishing, the researcher provided the cybersecurity and awareness team a list with participant-ID and email addresses that were gathered with the questionnaire during the pre-experiment survey. After each phishing stage, the researcher obtained an analysis file that contained information about who fell for the phish and whether information inputs were executed on the landing page. It is important to say that click and information input behaviour was communicated to the researcher only by associating the behaviours to the participant-ID of the respective participant. It was neither possible to derive insights on precise information that were inputted by the respective participant nor was it possible for third parties to derive direct conclusions about the respective participant as a person. These were conditions that were discussed with and confirmed by the legal department of the Swiss Armed Forces prior to the launch of the study.

The phishing scenarios were constructed in a way that applied the principles of persuasion, the PITs, that were discussed in chapter 2 of this thesis. It is needless to say that the application of all 13 PITs that were defined in the regard of this thesis was not possible. However, in each of the scenarios two to three rationales were applied. The overarching Time principle was applied in each of the scenarios by requesting the participants to follow through with the requested behaviour within a specific period of 72 hours. Additionally, the Authority,

Unity and Reciprocity rationales were used to frame the message of the phishing scenarios. Please see annex F for a precise description of the phishing scenarios and the applied PITs.

The administration of the pre- and post-test phishing took place three and a half weeks (3.5) prior to the intervention and within three and a half weeks (3.5) in two independent post-tests after the treatment. This process follows two reasonings. First, the chosen time span between the different stages of the experimental design account for potential learning effects induced by the repeated receipt of military related emails via a personal email account. The phishing tests were independent, and the scenarios were different among pre- and post-test. An insufficient time-lag between them could, nevertheless, have had learning effects on respondents' answer behaviour in the post-test phishing. Second, the administration of two post-tests served the purpose to gather knowledge about the treatments' possible retention effects of their contents on participants. Both rationales follow the conclusions deduced from the *forgetting curve* theory of Ebbinghaus (1885).¹⁰ Transferred to the study at hand, this means that a phishing email, which tests participants' likely behaviour in SE situations will not be remembered precisely already after one week since it was submitted. It is obvious that in a corporate or organisational environment, but also in student life, the daily business, private and professional activities play the most important role, such that a supposedly "one-time" receipt of a specific mail assumedly does not claim long-term cognitive resources.¹¹ Military related mails on the personal email account are not regularly recurring events in the daily life of the research subjects, as most communication regarding military service is performed by postal mail and thus, it was hypothesised that the sample population would remember quite well after one week the existence of the email receipt, though not precisely the topics. It was therefore fundamental to launch the pre-test stage sufficiently enough before the treatment in the intervention stage in order to neutralize as good as possible any learning or remembering effect induced by the email receipt. The pre-test phishing mail was therefore sent three (3.5) weeks before the treatment of the SG in the intervention stage. The post-test was submitted to the experiment population within 24 hours after the intervention and in a second post-test three (3.5) weeks after the intervention. This rationale also followed the principle of the forgetting curve and intended to discover retention effects of the treatments. It was not opted to fully

¹⁰ According to the theory, newly learned information remains consciously present at a decreasing rate over time, with almost 80% of the information learned not being correctly repeated after seven days. In similar, more recent studies those results were replicated and, besides some variation, confirmed (Murre and Dros, 2015; Radvansky, 2017; Fisher & Radvansky, 2018).

¹¹ Nevertheless, results also show that descriptions or occurrences of specific events are longer remembered and follow a rather positively than negatively accelerated curve, meaning that memory of specific event description is retained longer, but abruptly forgotten after around 12 weeks (Radvansky, 2017; Fisher & Radvansky, 2018).

integrate the conclusions derived from Radvansky (2017) and Fisher & Radvansky (2018) in the design of the experiment, as a period of 12 weeks between the different stages of the experiment would have had limiting effects on the operability and the internal validity, as the likelihood of maturation, demoralization and experimental mortality was very likely to increase.

About two hours after the pre-test phishing mail had been sent, the researcher was contacted by his supporting counterpart at the Swiss Armed Forces notifying him that the Swiss National Cybersecurity Centre (NCSC) had contacted them to report malicious activity. It seemed that either a participant or other red flags had notified the centre about this supposed malicious activity. The centre was informed about the purpose and origin of the research and that there is no need to block neither the landing page nor the email address.

Figure 6.3: Snapshot of the pre-test scenario test mail and landing page

The image shows a screenshot of an email and a corresponding web landing page. The email, from @vtg.admin.ch, is titled 'TEST: Développement de la brigade – formation des cadres (Difficulty 3)'. The body of the email discusses the upcoming 'Nouvel An' (New Year) and mentions several strategic projects: 'Cyber Bat 42', 'projet Cyber commandement', and 'projet TKA'. It asks the recipient to vote on their interest in a 'formation de cadres' (cadre training) within the next 72 hours. Below the email is a screenshot of the landing page at 'https://vtg.admin.ch/fr/Formation_des_cadres.html'. The page is for the 'Armée suisse' (Swiss Army) and features a navigation menu with options like 'Actualité', 'Service', 'Mon service militaire', 'Carrière', 'Organisation/Troupe', and 'L'Armée suisse'. The main content area is titled 'Formation des cadres' and includes an 'Information' section about COVID-19 adjustments and a 'Manifestation d'intérêt pour la formation des cadres' form. The form has fields for 'Nom' and 'Prénom Nom', radio buttons for 'Oui' and 'Non', and an 'Envoyer' button. The browser's address bar and taskbar are also visible.

Figure 6.4: Snapshot of the 1st post-test scenario test mail and landing page

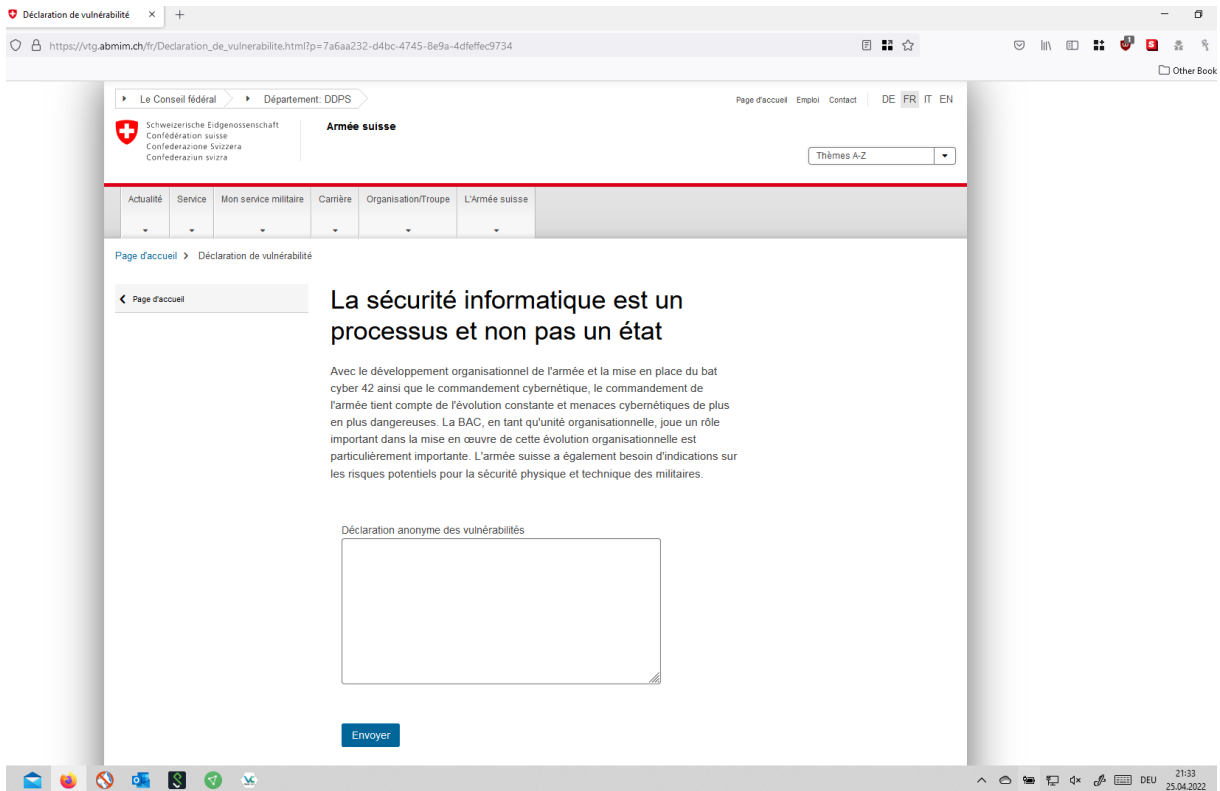
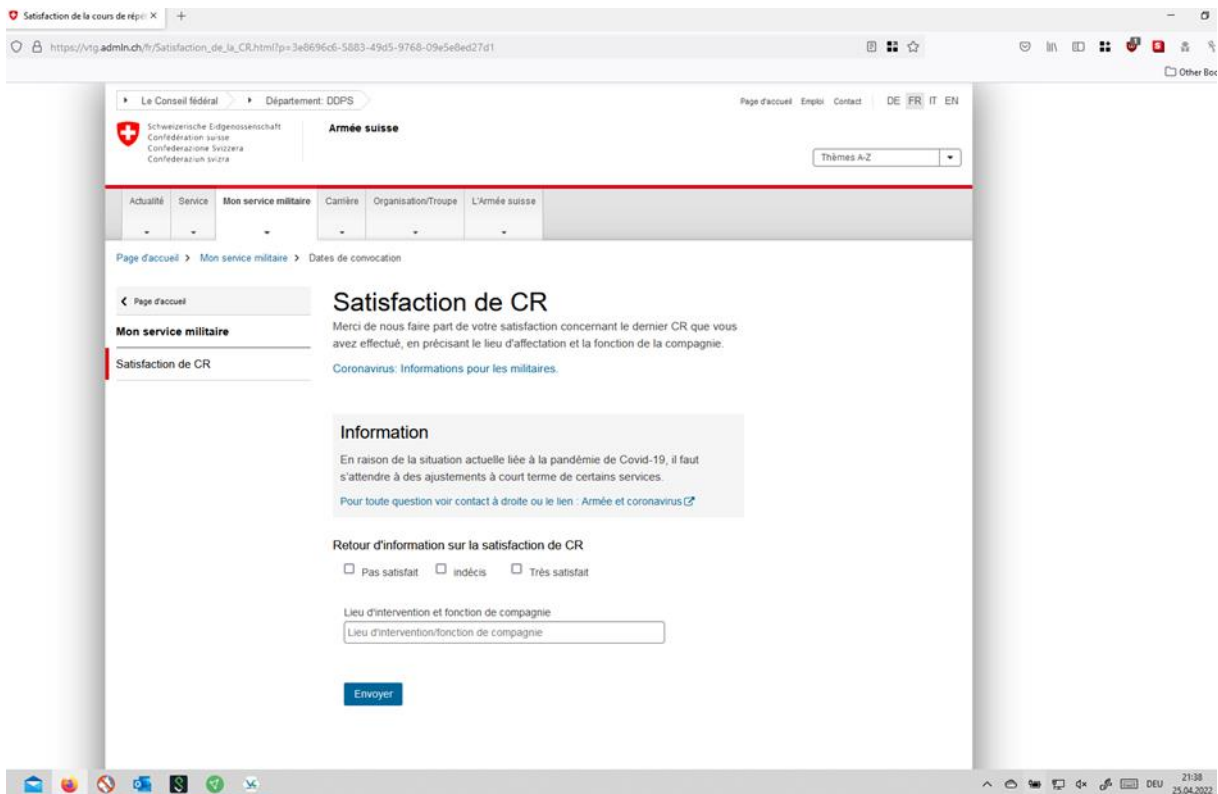
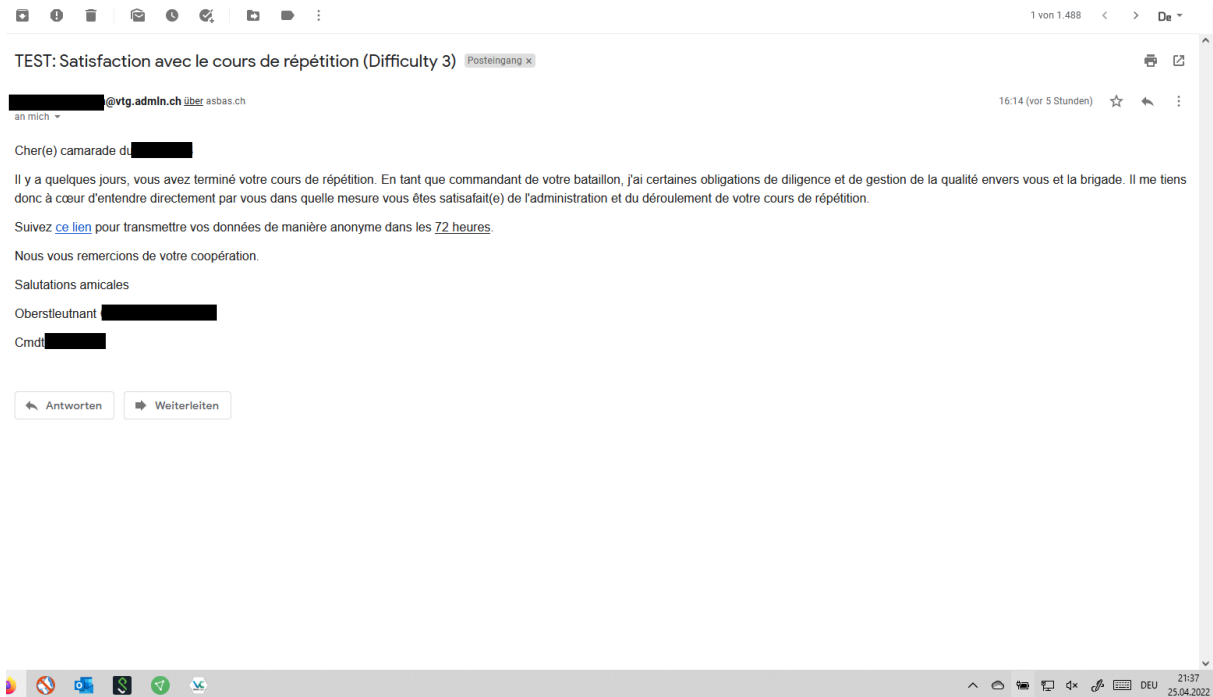


Figure 6.5: Snapshot of the 2nd post-test scenario test mail and landing page



Variables

The variables used in the data gathering process were: gender, age, mother tongue, prior participation in information security training (PIST), individual perception of information security importance (IPISI), HEXACO personality traits – Honest-Humility, Emotionality, Extraversion, Agreeableness, Conscientiousness, Openness – past individual victimization (PIV), individual victimization expectation (IVE), RCsB, ATC-IB, participation in serious game (PSG), as well as clicking on the link in the phishing email (Link) and inputting information on the respective landing page (Info). However, some variables were excluded, as there was no variance observed. General demographics were particularly of minor interest, as homogeneity of gender, age and mother tongue was very high in the study group at hand. Please see table 6.1 for an overview of the variables. The independent variable PIST_{PI} measured whether the subject completed an information security training about the protection of personal information in the last 12 months prior to the study at hand. Analogously, the independent variable PIST_{MI} measured whether the subject completed an information security training about the protection of military related information in the last 12 months prior to the study at hand. The dichotomous variables were dummy coded as 0 = did not participate and 1 = did participate. The independent continuous variable IPISI_{PI} measured the importance of the protection of personal information to the subjects, whereas the independent continuous variable IPISI_{MI} measured the importance of the protection of military information to the subjects. Importance was measured on a 5-point Likert scale (1 = not important at all, 5 = very important). The independent continuous variables Honest-Humility, Emotionality, Extraversion, Agreeableness, Conscientiousness, Openness measured subject's individual expressions in these personality dimension. Dimension expression was measured on a 5-point Likert scale (1 = Strongly disagree, 5 = Strongly agree) with several items being reversed coded as by Ashton, and Lee (2009). The independent dichotomous variable PIV measured whether the subject experienced an online phishing attack in the last 12 months prior to the study at hand that requested the personal information. The dichotomous variable was dummy coded as 0 = No and 1 = Yes. The independent continuous variable IVE measured subject's individual expectation of becoming a victim in the next 12 months. IVE was measured on a 5-point Likert scale (1 = very unlikely, 5 = very likely). The independent continuous variable RCsB measured the frequency of risky cybersecurity behaviour of the subject, whereas the independent continuous variable ATC-IB measured the attitudes towards cybersecurity and cybercrime in business of the subject. The variables were measured on a 7-point Likert scale (0 = never, 6 = daily) and 4-point Likert scale (1 = strongly disagree, 6 = strongly agree), respectively. Coding

was performed according to Hadlington (2017). The independent variable PSG measured whether the subject was part of the control or the experimental group that received the serious game as intervention. The dichotomous variables were dummy coded as 0 = did not participate and 1 = did participate. The dependent ordinal variable IPSE measured whether the subject complied with the request in the phishing mails in the pre- and post-test scenarios (0 = did not comply, 1 = did comply by clicking the link, 2 = did comply by clicking the link and inputting requested information).

Confidentiality and Data Management

The commander of the military academy, as a military representative, and the researcher countersigned an agreement concerning data protection of the data of study participants. The researcher agreed that all collected data of reserve soldiers, besides those that are necessary to guarantee the study process, will be used and processed only by him, will not be disclosed to any other internal or external party, and will be deleted after the successful completion of the doctorate, the latest. Publication of study results shall be anonymous, and a report of the consolidated results shall be made available to the organization afterwards. Raw data from survey results were transferred from LimeSurvey to Microsoft Excel by exporting the respective data sheets and data from pre- and post-testing were transferred from the phishing service platform of the supporting counterpart at the Swiss Armed Forces to Microsoft Excel as well. The data files were merged, such that all data per study subject were ready to be analysed in one sheet. Hence, in addition to the data gathered through the initial survey, columns for serious gaming participation, as well as pre- and post-test results were reflected in the data sheet. Subsequently, data were checked for outliers, completeness and were edited to obtain a unified layout. For HEXACO, RCsB and ATC-IB data, an overall score was calculated on a dimension level for the HEXACO and on indicator level for RCsB and ATC-IB. Afterwards the data were loaded into the statistical computing software R, where it was further prepared and analysed for testing the hypotheses.

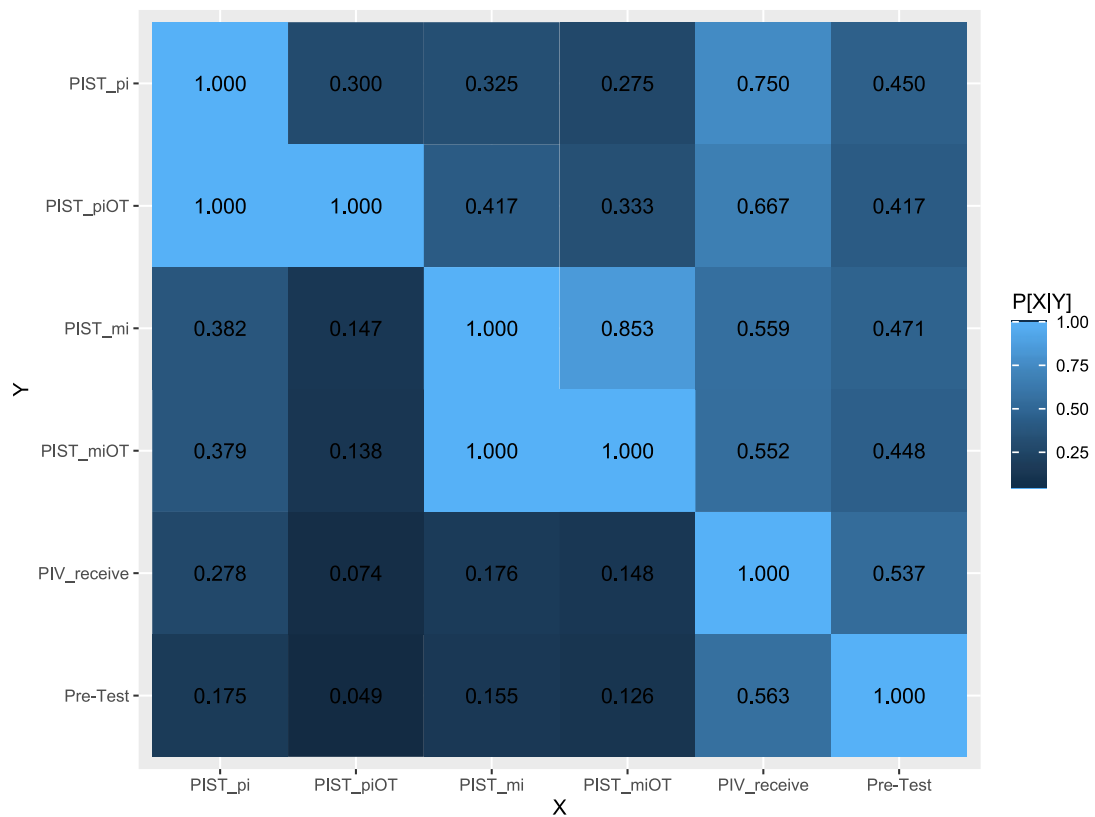
Table 6.1: Variable description

Variable	Code Name	Scale	Content	Data Source
IPSE - Clicking on link in phishing email	Link	binary	-	Pre- & post-tests
IPSE - Inputting requested information on dedicated landing page	Info	binary	-	Pre- & post-tests
Participation in serious game training	PSGpart	binary	-	Serious game
Post-test 1	time1post	binary	Results of post-test1	Post-test
Post-test 2	time2post	binary	Results of post-test2	Post-test
Honesty-Humility	Hone	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Emotionality	Emot	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Extraversion	Extr	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Agreeableness	Agre	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Conscientiousness	Cons	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Openness	Open	5-point Likert scale	60-item HEXACO personality inventory	Pre-experiment survey
Previous information security training for personal information	PIST_pitru	binary	Have you attended any training in the last 12 months that focused on the protection of personal data and information?	Pre-experiment survey
Previous online information security training for personal information	PIST_piOtrue	binary	Was it an online training?	Pre-experiment survey
Previous information security training for military information	PIST_mitru	binary	Have you attended any training in the last 12 months that focused on protecting military data and information?	Pre-experiment survey
Previous online information security training for military information	PIST_miOtrue	binary	Was it an online training?	Pre-experiment survey
Previous individual victimization	PIV_receivetrue	binary	In the last 12 months, have you ever received an email link from someone asking you to provide sensitive information such as personal identification, bank and credit card details, and passwords?	Pre-experiment survey
Individual victimization expectation	IVE	5-point Likert scale	In the next 12 months, how likely are you to provide personal information online to someone who asks you to provide sensitive information (e.g., personal identification, bank and credit card information, and passwords) via email?	Pre-experiment survey
Risky cybersecurity behavior	RCsB_Mean	7-point Likert scale	20-item inventory concerning self-reported cybersecurity behavior	Pre-experiment survey
Attitudes towards cybersecurity and cybercrime in business	ATCIB_Mean	4-point Likert scale	25-item inventory concerning self-reported attitudes	Pre-experiment survey
Perceived usefulness of serious game	U_SG	5-point Likert scale	How useful was the interactive serious game to you?	Post-SG survey
Perceived knowledge gain about social engineering through serious game	KC_SG	5-point Likert scale	How much do you agree with the following statement: The serious game has contributed to my knowledge about social engineering?	Post-SG survey
Perceived social engineering threats awareness increase	SET_AC	5-point Likert scale	How much do you agree with the following statement: I am now more aware of the threats posed by social engineering than before the event.	Post-SG survey
Perceived confidence in avoiding social engineering victimization	SEV_avoid	5-point Likert scale	How likely is the event to help you avoid becoming a victim of social engineering?	Post-SG survey

Dataset of Pre-Experiment Survey

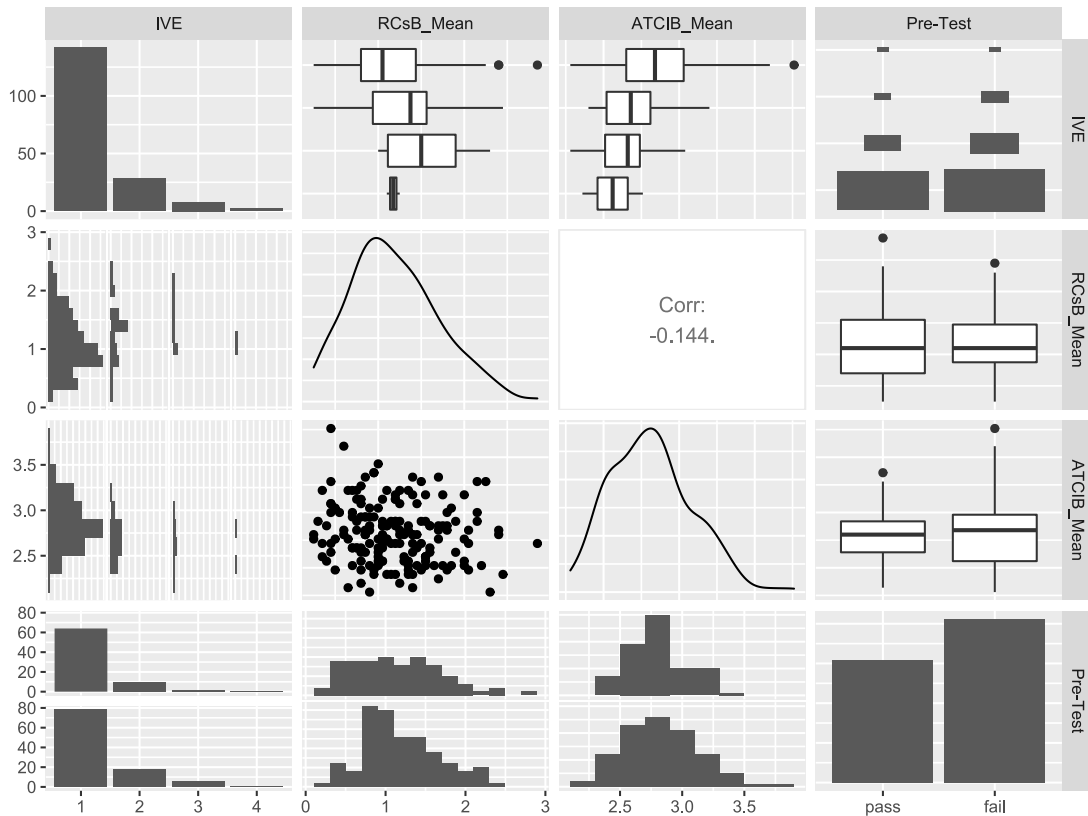
The dataset of the pre-experiment survey consisted of the variables highlighted in table 6.1 above. Data were collected with regard to participants' personality traits, previous IS training experience, previous and expected individual victimization and to cybersecurity behaviour and attitudes. A set of indicators looked at previous participation in training sessions during the 12 months prior to the research. It is differentiated between personal and military training and whether the training was held online or in person. An additional indicator relates to previous victimization, namely if a phishing email similar to the tests was received by the participant during the 12 months preceding the study. These variables shall be summarized in the set \mathcal{H} as before. As a note, the indicators for whether the previously received emails were opened and information was lost are left out from the analysis, since this was negative for over 95% of participants. The following figure illustrates relative dependencies of those variables in the dataset, whereas light blue cells represent high relative probabilities and dark blue cells low relative probabilities. One can see that e.g. there is $P = 0.750$ for participants having received a phishing email within the 12 months preceding the survey and participants' participation in an information security training in the same period. Thus, there was a 75% chance that when randomly selecting a participant from the ones who reported that they were victim of a phishing email, this participant also attended an information security training that dealt with the protection of personal information in the same period. Moreover, one can see that regardless of the nature of the security training – military or personal information related – the means of administering these trainings was to 100% online. Interactive offline trainings as the one subject to this thesis were therefore not common to the study participants before participating in the study.

Figure 6.6: Relative probabilities matrix



Further sections in the questionnaire were used to measure first of all the individual victimization expectation for the future as well as evaluations of risky cyber security behaviour and attitude towards cyber security. The statistical characteristics of the results of these sections are illustrated in figure 7.4 below.

Figure 6.7: Variable matrix



Dataset of Test Stages

The quantity of interest in the test stages were multiple indicators $Y_{a,i}^t$ describing whether a participant fell victim to a phishing attack or not. The participants are enumerated by $i = 1, \dots, N$ and the number of participants that were part of the study is $N = 180$. There are two types of indicators Y_a with $a \in \{\text{link}, \text{info}\}$ for different severities of the failed test, namely if a participant merely pressed the link in the phishing email and secondly if a participant also entered information on a dedicated landing page. Additionally, the tests were conducted at three different times $t \in \{0, 1, 2\}$ giving a full set of six indicators per participant with respect to the different SE phishing tests in the regard of the research design.

The following figures show the absolute and relative number of participants that failed the tests of both assessment types (only clicking the link or clicking the link and also disclosing information) along the three points in time. Clearly, only clicking the link happens more often than entering information and it can also be observed that the number of failed study participants shrinks from the pre-test to the first post-test.

The treatment to be studied is the participation in a training with a SG and its effect on the performance in phishing emails, as well as the influence of personality traits. The time of the test indicators $Y_{a,i}^t$ is relative to this training with the first one $t = 0$ being the pre-test 4 weeks before the training, then $t = 1$ being directly 1 day after and $t = 3$ being the post-test 4 weeks after. The participation in the SG training is indicated by the variable P_i for each participant. Both groups look very similar with respect to the percentage of participants that failed the tests.

Figure 6.8: Percentage of failed participants in either test stage (N=180)

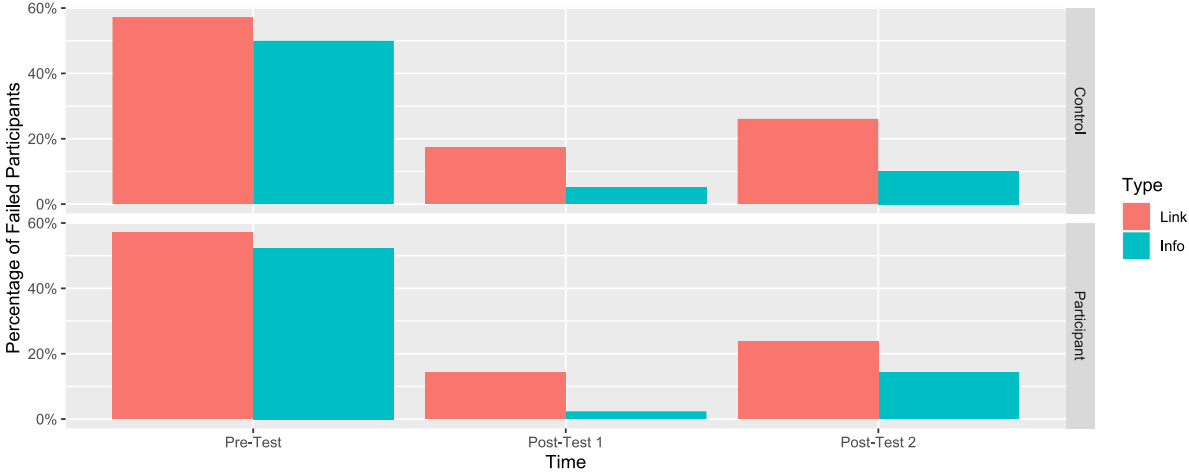
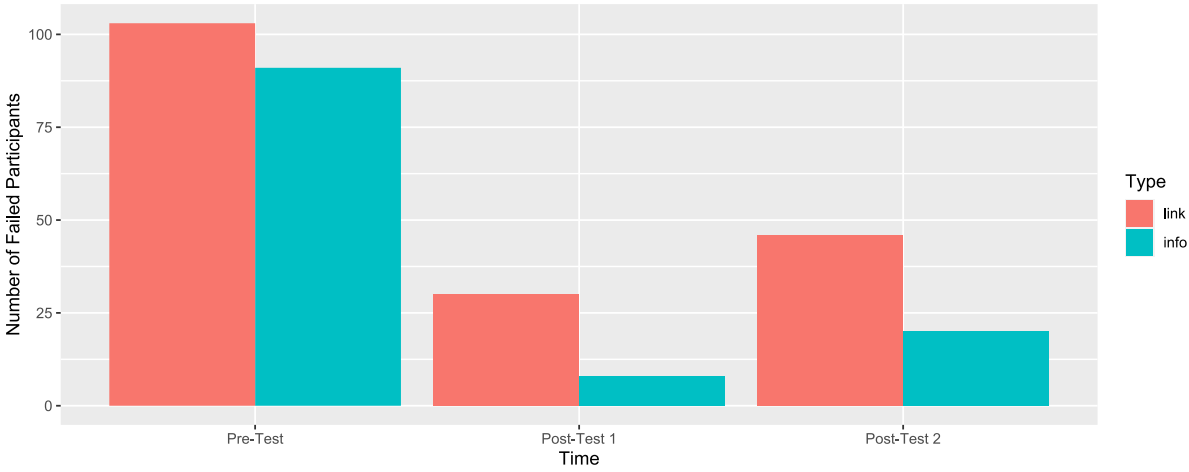


Figure 6.9: Number of failed participants in either test stage



Dataset of Post Serious Game Survey

The following pages present the data of the post-serious game survey in a descriptive manner. First of all, it was of interest for the researcher how satisfied experimental group participants were with the training in a whole, namely the introductory presentation and the SG. Out of 42 training participants, 34 (81.4%) reported that they were satisfied or very satisfied with the whole event. Only one person reported that he was not at all satisfied with the event.

Afterwards, experimental group participants were asked to state their individually perceived usefulness of the introductory presentation that showed the participants the rationales and techniques of SE, as well as report of a real-life SE example conducted by the instructor. Among the training participants, 86% evaluated the stimulating introductory presentation as either useful or very useful. Only one person did not find the presentation useful.

Another question related to participants' satisfaction with the game master of their table. This question is of huge importance, as the game masters obtain a focal role in the administration of the SG. Knowledge acquisition and the understanding of new rationales and concepts specifically depends on the ability and experience of the respective game master. The individual perception of these dimensions by the players gives a good indication whether these conditions were intact, as if not, the game participants would have struggled to grasp the core of the topic. The survey results support the view that the game masters were well capable of doing their job knowledgeably.

Next, respondents were asked about their individually perceived usefulness of the SG. Different to the results of the questions before, answers were less extreme distributed, though only slightly. Still, almost three quarters found the interactive SG useful or very useful to them, whereas a bit less than a quarter did neither find it useful nor useless. Only 2 participants did not see any usefulness in the game.

Further, experimental group participants were asked to state their perception that the game helped them to increase their knowledge about SE. 74.4% of training participants either agreed or even strongly agreed that this was the case for them. Only three people stated that the game did not provide any new insights for them into the rationales and concepts of SE. This result is particularly interesting, as all the study participants were part of a technical battalion that also deals with topics of information security to a certain degree. On the other hand, this result shows once more that SE as a socio-technical method of conducting fraud or intelligence operations

is still not commonly known in its facets even with people who have a pronounced understanding of cyber and information security risks.

Similar results were obtained for the next question in the survey. Training participants were asked whether, in their opinion, the whole event helped them to become more aware of the threats of SE. Almost seven out of ten respondents either agreed or strongly agreed that the event helped them to become more aware of SE threats. Again, only three respondents did not see any value in the event for this purpose.

The second last question of the survey asked training participants to report their perceived likelihood that the event helped them to avoid a future SE victimization. Less than half of the training participants (48.8%) were confident that the event likely or very likely helped them to not become victim of SE. The vast majority of respondents chose a neutral answer to this question, feeling that the event might help or might not help to resist targeted attacks.

Table 6.2: Relative responses of post serious game survey

	5	4	3	2	1
Satisfaction with the whole event	20.9%	60.5%	16.3%	0.0%	2.3%
Perceived usefulness of the introductory presentation	39.5%	46.5%	11.6%	2.3%	0.0%
Perceived satisfaction with game master	46.5%	44.2%	9.3%	0.0%	0.0%
Perceived usefulness of the interactive serious game	11.6%	60.5%	23.3%	2.3%	2.3%
The serious game has contributed to my knowledge about social engineering?	39.5%	34.9%	18.6%	7.0%	0.0%
I am now more aware of the threats posed by social engineering than before the event	39.5%	30.2%	23.3%	4.7%	2.3%
Perceived likelihood of the event helping to avoid future SE victimization	9.3%	39.5%	41.9%	9.3%	0.0%

(5 = Very satisfied/very useful/very likely/strongly agree; 1 = Not at all satisfied/not at all useful/very unlikely/strongly disagree)

Finally, the researcher was interested in any improvement potential of the event as a whole, of the introductory presentation, of the interactive game or improvement potentials categorized as «other». Around 30% of training participants provided suggestions. Most of the improvement potentials referred to administrative aspects of the event. A couple of respondents perceived the personal effort that was necessary to attend the event as too high. Although all experimental group participants were part of the same battalion and had their repetition course at the same time, they belonged to different troops stationed at different sites of service in Switzerland. For some training participants this demanded a huge effort to travel to the event site. Clearly, those soldiers were, to a certain degree, somewhat exhausted before event even started.

Besides pure administrative remarks, a couple of participants provided improvement proposals that referred to the game and the pre-test phishing. According to them, the game would profit of erasing the scoring system and providing more or better examples. With respect to the phishing tests, one participant suggested to use tracking pixels, such that it can be evaluated whether the mail went to the junk or was received by the recipient but not opened.

6.3 Analytical strategies

The analysis was performed by using the statistical computing software R. For the research questions under investigation different analytical strategies were performed. Table 6.2 shows an overview of the strategies and tests, as well as the dependent and independent variables that were used for corroborating the respective research hypotheses.

Table 6.2: Analysis strategies and statistical tests used

Research Hypothesis	DV	IV	Analysis	Test
<i>H I.1 - H I.6</i>	Link Info	Hone Emot Extr Agre Cons Open	Logistic regression model	Likelihood ratio test
<i>H II.1 - H II.6</i>	RCsB_Mean	Hone Emot Extr Agre Cons Open IVE	Linear regression model	F-Test
<i>H III.1 - H III.6</i>	ATCIB_Mean	Hone Emot Extr Agre Cons Open IVE	Linear regression model	F-Test
<i>H IV.1</i>	Link Info	PSGpart	Cross-sectional Longitudinal Difference-in-Differences Generalized linear mixed effects model	Chi ² Test Fisher's exact test Bootstrapped Odds Ration Variation McNemar Test Likelihood ratio test Likelihood ratio test
<i>H IV.2 - H IV.4</i>	KC_SG SET_AC SEV_avoid	U_SG	Linear regression model	F-Test
Validation and verification of H I.1 - H I.6 and H IV.1 with general classification model respecting the whole dataset				
			Logistic regression model Decision Tree Random Forest Power Analysis What-If Analysis	Chi ² Test

The data were analysed using different types of analysis, which depended on the respective research hypothesis and the corresponding type of data. Whereas for hypotheses *H I* to *H III* less statistical variety was applied, this was different for hypothesis *H IV.1*. This was necessary due to the sophisticated design of the research with data across different points in time and across study groups. Finally, advanced statistical analyses were applied to derive hypothetical conclusions about the dataset.

Less statistical variety was necessary to investigate on the hypotheses of research question I, II and II. As the dependent variable, namely the performance in the phishing tests, is categorical, generalized linear analysis was used to determine the model and the selected variables of personality traits as predictive indicators. Likelihood ratio tests were performed for the goodness of fit of the model and the predictors. Further, bidirectional variable selection was used to come up with the variables with the strongest effect on the estimated results. In addition, Fisher's exact test was performed to verify the results. For the analysis of research *H II* and *H III* a linear regression model was used. Data on either side of the equation were scaled ordinal, such that the most appropriate analysis was the linear regression model. This said, F-Tests were used to test the significance of the impact the independent variables had on the dependent variable.

More statistical variety was used in order to evaluate the potential effects the serious game could have on the study participants' performance in phishing tests. The experimental design of this research incorporated a control and an experimental group, that were exposed to the phishing tests at different points in time, prior and after a serious gaming intervention. This set-up allowed to look at the collected data in various forms. First, it was analysed whether there is any statistically significant cross-sectional indication of a dependency among the variables of having participated in the serious game and having failed the phishing tests. To do so, a chi-squared contingency table was created, and a chi-square test performed. It must be mentioned that for a chi-square analysis two data assumptions must be met. There has to be independence among the data and a minimum frequency of five observation per cross-tabulation cell (Field et al., 2012). Only if both assumptions are met, the chi-square test provides accurate results. Otherwise, the Fisher's exact test (Fisher, 1922) has to be performed. The fact that categorical data were used, satisfied the requirement of independence. However, the category participation in the serious game while simultaneously failing the post-test only showed one observation, such that the second requirement was not met. The Fisher's exact test was performed additionally in this case. Second, in order to study potential effects of the serious

game over time, a longitudinal analysis of the odds ratios and risk ratios of the two groups was performed. By doing so the hypothesis *H IV.1* was corroborated, namely whether it is correct that the serious gaming helps to decrease the odds or risk of failure in the experimental group but not in the control group. Looking at odds ratios for categorical variables has advantages and is common in criminology (Farrington and Loeber, 2000; Wilson, 2001), such as they are quite often more realistic and a better measure of relationship for those variables than the correlation indicators (Farrington and Loeber, 2000). Moreover, a non-parametric bootstrap sample was created from the data set to test the statistical variation of the measured odds ratios. The statistical method of bootstrapping was first introduced by Efron (1979) and is used for different statistical endeavours. For the research at hand, it served mainly two purposes. First, it was of interest to see what would happen to the results, if, from the basic data set, repeated samples would be created synthetically at random. Thus, creating a random selection by replication or resampling of the original data (Hardle et al., 2004). Second, by performing this approach, it is possible to smoothen the effects of the non-random participant allocation to either study group by the persons in charge of the collaborating organization. Resampling the original study data and creating a synthetic random selection of the whole data set, allows to smoothen the impact of the non-random study group allocation and look at the statistical variation of the measured odds ratio with a bias-corrected accelerated bootstrap confidence interval. In a further step, McNemar tests (McNemar, 1947) were performed to determine any statistically significant change among matched pairs in the experimental and control group for having passed or failed the pre- and post-tests. This is a common approach to test categorical experimental outcomes (Agresti, 2003; Amin et al., 2011; Dorr et al., 2020).

The most appropriate way to look at data of a sophisticated experimental design with several different data points over time among different study groups is a difference-in-difference analysis. In particular, those analyses are commonly used in criminology and are also applicable for natural or quasi-experiments (Meyer, 1995; Bertrand et al., 2004; Ariel, 2012; Kondo et al., 2015; Grossrieder et al., 2017). Lastly, a Generalized Linear Mixed Effects Model was constructed and tested. Those models take into account the correlation between the results of each participant by also looking at the error terms of each participant in addition to the standard errors of fixed-effects models. The power of such a model will be lower since the correlation of the results of each participant is taken into account, but comparing models is more accurate. Likelihood ratio tests were performed to evaluate whether the inclusion of the difference-in-difference parameters has any statistically significant effect or not. Likelihood

ratio tests are common tools to test the goodness of fit of different statistical models in hypothesis testing. They are also used in victimology and research about situational crime prevention (Miethe and Mc Dowall, 1993; Shane et al., 2015).

Further data analysis was performed to derive possible additional insights while looking at the whole dataset at once including personality traits and other variables. Logistic regression was used while including all parameters to produce a general classification model. Again, a stepwise selection in both directions of the most valuable and statistically significant variables was used to end up with a model that includes only variables that promise to add statistically significant meaning to the model and estimation. In a last step, a chi-square test was performed on the eventual model to see whether adding the variables that were left out from the final model do indeed not change the estimates significantly anymore. Two further steps were taken to verify the results of the logistic regression. First, a decision tree analysis was performed to generate further insights on how the phishing test results are clustered and to look at possible interaction effects. The method of decision tree building is a fast and effective way of classifying data of large, complex, or erroneous datasets (Aitkenhead, 2008). Decision tree analysis is a predictive approach that can be used in statistics or machine learning by mapping conclusions about a variable's target value to its observation in the dataset (Ivan et al., 2017). Second, a random forest analysis was used to derive increasingly effective predictive models. With bootstrap aggregation, individual trees are used to derive importance scores.¹²

In a separate analysis, the statistical power of the investigations regarding the statistical significance of the variable PSG was performed. With a statistical power analysis one can estimate the strength of a research design or estimate the necessary size of a sample that would lead to a predefined level of statistical power in the research and model under investigation (Britt and Weissburd, 2010). The power analysis took the results of the chi-squared tests and the McNemar tests that evaluated the effects of serious gaming and derived the desired sample size that would be necessary to detect a statistically significant effect on the 5% level. The power analysis used an assumed power level of 80% to do so. Lastly, the researcher used a "What-If" analysis to check the impact of the participation in the serious game with hypothetical scenarios (LaFleur and Greevy, 2009; Chihara and Hesterberg, 2022). It uses resampling of the original dataset to derive synthetic data. By resampling a synthetic dataset with an equal amount

¹² Random forest analysis is a machine learning approach that develops prediction models (Speiser et al., 2019). This approach was first introduced by Breiman (2001) which uses a collection of decision trees, creates a synthetic aggregation and permutes them into scores that can rank their importance. Thus, making it possible to evaluate which variables represent importance for the question under research.

of study participants that passed and failed the post-tests, one can infer the amount of control and experimental group participants in a hypothetical way.

6.4 Methodological Limitations

The experimental part of this research study applied a pre- and two post-test stages, a treatment and a control setting with a non-random participant assignment. The advantage of a classical experiment is that its set-up reduces the likelihood of different validity threats (Maxfield & Babbie, 2017). The study at hand nevertheless had to deal with limitations that had an impact on its explanatory power. In particular, the elimination of six threats had to be considered prior to the study, whereas two additional methodological limitations evolved during the study.

First, the generalizability of the study's results heavily depends upon the selection and size of the target population. The study was conducted with reserve soldiers of a battalion of the Swiss Armed Forces. It is for certain that this very specific group of population neither reflects (Swiss) society nor the Swiss Armed Forces as a whole. The size of the study population of 180 does reflect only a minor part of the before mentioned base populations, such that derived results are limited in their transferability and applicability to a broader public. The relatively small sample size does not allow to derive universal conclusions. However, compared to other researchers who used SG in similar settings (Beckers & Pape, 2016; Hart et al., 2020) the sample size was nevertheless significantly above the average.

Second, the researcher had to deal with the threat of experimental mortality. The experiment was designed in a way that it made use of the forgetting curve rationale (Ebbinghaus, 1885) to reduce the likelihood of learning effects induced by the surveys on the one hand and to derive conclusions about the treatment's retention effect on the other hand. The effective time span between the different experimental stages was set to three weeks to account for operability and experimental mortality. Further, the initial survey for participant recruiting and data gathering was constructed in a way that the expected time burden did not exceed 20 minutes. In total, the survey was accessed 276 times of which 182 reserve soldiers successfully completed it and initially took part in the study. This ratio confirms that time burden might not have been a large issue although the data gathering process has been extensive indeed. Opting out in the recruitment process mainly happened at the beginning of the questionnaire when the personal email-address had to be disclosed. The fact that the intervention was administered during the yearly repetition course of the battalion, that participation in the study was granted a half day of the service and the fact that the service is mandatory provided some security barriers that limited experimental mortality. Additionally, recruited participants had to confirm

not only the data protection information but also their consent to participate in the whole study in advance to the initial survey for increasing the likelihood of keeping up with the study. This approach seemed to have been successful, as of the 182 committed participants only 2 requested their exclusion from the study. The experimental mortality was obviously rather low.

Third and fourth, there are justified concerns that participants who were not assigned to the SG will either be demoralized or will compensate their non-selection with additional effort in the test stages. Moreover, there are also justified concerns that discussions among the study subjects about the contents of the treatment will affect their post-test performance. The experiment design took these considerations into account by separating the groups and keeping anonymity among the participants as best as possible. Only study subjects of the treatment group were able to get to know each other personally and exchange information during and after the treatment. Study subjects of the control group were not specifically disclosed to the participants of the experimental group. However, there was a valid concern that control group members that were in the same troop and service as the experimental group members or part of the group may have been demoralized due to their non-selection. However, in the flyer that promoted the study among the battalion and that was the initial step to recruit participants, it was clearly stated that effective allocation to the SG will be done by the battalion commander. Thus, with their voluntary participation, study participants should have been aware with the probability of non-selection in advance. On the contrary, explicitly mentioning the probability of non-selection in the recruiting flyer might have limited the number of recruited participants at first. The SG was administered in two rounds on two consecutive days to reduce the likelihood of diffusion before the first post-test, which took place within 24 hours after the intervention stage.

Fifth, Hart (2020) showed that there is a justified concern of instrumentation threat stemming from the usage of multiple game masters in the treatment setting. The differences in game master ability to administer the game, as well as explaining to the study subjects the game proceedings and the material could significantly impact the post-test performance within the experimental group. Therefore, the researcher selected five game masters sufficiently prior to the experiments and trained them about their role as game masters, the game material, and the game proceedings in a joint half-day training. Further, the researcher provided the game masters a leaflet outlining the precise proceeding of the game and their responsibilities that guided them during the game (see Annex B.2).

Lastly, another validity threat that had to be respected refers to the researcher himself. The active participation of the researcher in the SG as a game master would have led to a researcher bias in the way that he probably would favour the supervised study subjects to perform particularly good (Hart, 2020). It was therefore opted to assign the researcher an observing position during the treatment.

Additionally, two further methodological limitations evolved during the study and were to a certain degree out of the researcher's control. First, a random assignment of the voluntary study participants to either the control or the experimental group was not possible as initially planned and discussed with the cooperating organization due to administrative and organizational conditions in the battalion that were not possible to overcome. Allocation to either the control or the experimental group was performed by the Swiss Armed Forces as they had to respect the availability of, as well as securing the operational capability of the battalion. It was therefore not possible for the researcher to randomly assign the participants to either of the two groups. Participant assignment had to be accepted as given. The research of Bullée and Junger (2020) shows, nevertheless, that quasi-experimental SE intervention studies do not perform worse than full randomized studies. Second, the pre- and post-test instruments could have been insufficiently measured the response rate to the phishing scenarios. Pre- and post-test have all been administered by the vendor of the Swiss Armed Forces that also does phishing campaigns with civil employees in the organization for cybersecurity awareness building. The researcher gratefully accepted the opportunity to collaborate with the vendor, as it provided efficiency and internal know-how of what must be respected when performing phishing tests within the organization. Further, it simplified a major obstacle, namely study authorization. As a Swiss Armed Forces contracted vendor the service provider underwent several background and service checks, which would have been necessary in case any other third-party service was used instead. Nevertheless, it turned out that responses to phishing mails only measured the opening of an email and whether information were inputted on a dedicated landing page. The service of the vendor did not measure whether mails went to the spam or junk folder and thus were not opened. The researcher asked the vendor whether it is possible to test the phishing emails in advance with certain email providers. Study participants were asked to disclose their private email address to take part in the study. It was therefore crucial to test whether these mails make it into the inbox of the accounts of such providers as gmail or hotmail. During these tests, the researcher experienced no issues that this was not the case. However, this is no

guarantee that all of the 182 initial study participants received the email in their account inbox and therefore reflects another a methodological limitation of this research.

7. Results

7.1 Personality Traits and SE Fraud Victimization

The first research question of this dissertation asks whether individual personality traits play a role in the individual proneness towards SE fraud. The effect of the personality traits on participants' proneness towards SE email phishing is observed in the pre-test. The test results of the participants are correlated with their results in the HEXACO personality test. The test has six dimensions (1: Honesty, 2: Emotionality, 3: Extraversion, 4: Agreeableness, 5: Conscientiousness, 6: Openness) denoted by $x_i^h, h \in H = \{1, \dots, 6\}$. The values are measured averages of a 5-point Likert scale and hence in the domain $x_i^h, i \in \{1, \dots, 5\}$. For each of the HEXACO personality dimensions a separate hypothesis was constructed in order to answer the research question more detailed. The null-hypotheses for each of the six dimension are denoted as follows:

H I. 1₀: People high on the personality domain Honesty-Humility are not more prone towards SE deception rationales.

H I. 2₀: People high on the personality domain Emotionality are not more prone towards SE deception rationales.

H I. 3₀: People high on the personality domain Extraversion are not more prone towards SE deception rationales.

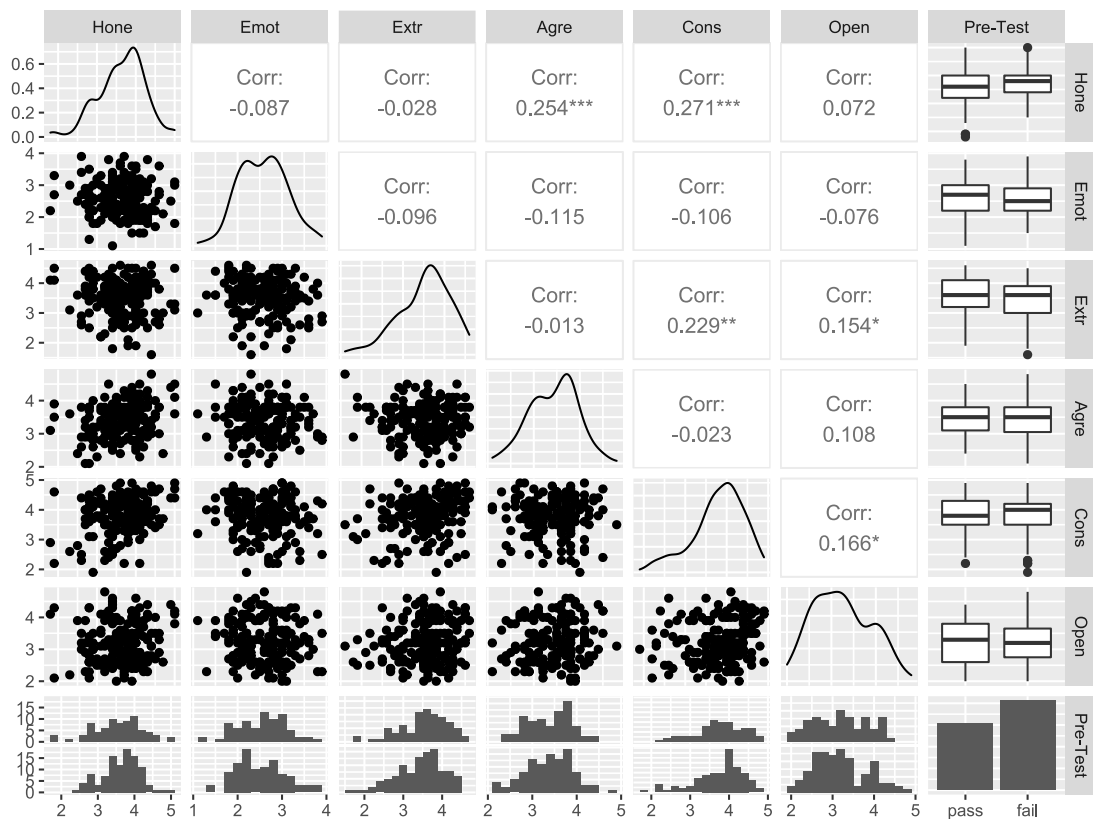
H I. 4₀: People high on the personality domain Agreeableness are not more prone towards SE deception rationales.

H I. 5₀: People low on the personality domain Conscientiousness are not more prone towards SE deception rationales.

H I. 6₀: People high on the personality domain Openness are not more prone towards SE deception rationales.

Figure 7.1 shows the correlation matrix of the HEXACO variables and the pre-test results, including scatter plots and distribution graphs for each of the six variables and a histogram for the pre-test – HEXACO results relation.

Figure 7.1: Correlation matrix of HEXACO variables and pre-test results



Generalized linear analysis quickly shows the estimated parameters for each of the six personality dimensions. One can easily see that for the link test stage Honesty-Humility and Openness seem to have a positive effect on falling for the test, whereas the remaining four dimensions show a lower ratio and thus would indicate a negative impact of a pronounced personality trait on the proneness. Things stay the same for the info test stage, except for the dimensions Agreeableness and Conscientiousness, where effects change directions. These insights are contrary to the hypotheses presented in chapter 5, except for the dimensions Honesty-Humility, as well as for Agreeableness in the info stage and for Openness in the link stage. This analysis is crucial but nevertheless of less importance when looking at their statistical significance. None of the surveyed HEXACO personality traits in \mathcal{H} have significant influence on the pre-test results. The table below shows the measured multiplicative effects together with their p-values.

Table 7.1: Logistic regression results for HEXACO variables on pre-test results

	Link		Info	
	Est.	p	Est.	p
(Intercept)	4.272	0.467	1.207	0.924
Hone	1.387	0.247	1.508	0.144
Emot	0.853	0.579	0.816	0.473
Extr	0.742	0.254	0.948	0.837
Agre	0.824	0.534	1.105	0.744
Cons	0.935	0.801	0.816	0.441
Open	1.010	0.967	0.852	0.508

Among the six dimensions, it is the dimension Honesty-Humility that somewhat shows to be the best predictor of the performance in the pre-test, though not statistically significant.

A χ^2 likelihood ratio test shows that no evidence is present that the test results depend in any straight way on the personality traits. Comparing this linear model with likelihood ratio tests finally confirms with p-value 0.771 for the link assessment level and p-value 0.661 for the info assessment level that the effect of personality traits is not significant for the results of the pre-test.

Table 7.2: Results of the χ^2 likelihood ratio test

type	Resid. Df	Resid. Dev	Df	Deviance	Pr(>Chi)
link	179	245.764	NA	NA	NA
link	173	242.466	6	3.298	0.771
info	179	249.511	NA	NA	NA
info	173	245.396	6	4.115	0.661

The research hypotheses shall be evaluated in the following paragraph. Table 7.3 illustrates the evaluation result.

Table 7.3: Research hypotheses evaluation

Link		Info	
<i>H0</i>		<i>H0</i>	
H I.1	not reject	H I.1	not reject
H I.2	not reject	H I.2	not reject
H I.3	not reject	H I.3	not reject
H I.4	not reject	H I.4	not reject
H I.5	not reject	H I.5	not reject
H I.6	not reject	H I.6	not reject

7.2 Personality Traits and Cyberfraud Victimization Behaviour and Attitudes

The second and third research question looks at the interdependencies of HEXACO personality traits as independent variables and variables for cybersecurity behaviour and attitudes. For each of the HEXACO personality dimensions a separate hypothesis was constructed in order to answer the research question more detailed. The null-hypotheses for each of the six dimension are denoted as follows:

H II. 1₀: People high on the personality domain Honesty-Humility are not less engaged in self-reported risky cybersecurity behaviour.

H III. 1₀: People high on the personality domain Honesty-Humility do not show favourable self-reported attitudes towards cybercrime and cybersecurity.

H II. 2₀: People high on the personality domain Emotionality are not less engaged in self-reported risky cybersecurity behaviour.

H III. 2₀: People high on the personality domain Emotionality do not show favourable self-reported attitudes towards cybercrime and cybersecurity.

H II. 3₀: People high on the personality domain Extraversion are not more engaged in self-reported risky cybersecurity behaviour.

H III. 3₀: People high on the personality domain Extraversion do not show less favourable self-reported attitudes towards cybercrime and cybersecurity.

H II.4₀: People high on the personality domain Agreeableness are not less engaged in self-reported risky cybersecurity behaviour.

H III.4₀: People high on the personality domain Agreeableness do not show favourable self-reported attitudes towards cybercrime and cybersecurity.

H II.5₀: People high on the personality domain Conscientiousness are not less engaged in self-reported risky cybersecurity behaviour.

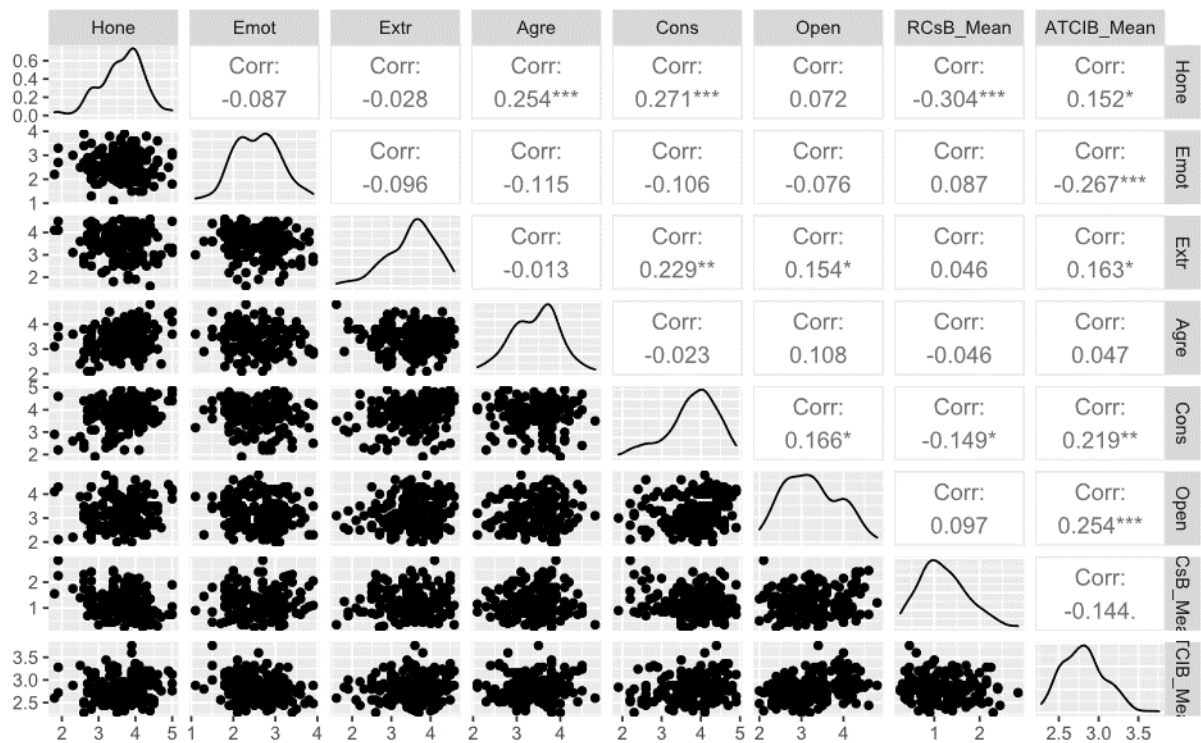
H III.5₀: People high on the personality domain Conscientiousness do not show favourable self-reported attitudes towards cybercrime and cybersecurity.

H II.6₀: People high on the personality domain Openness are not more engaged in self-reported risky cybersecurity behaviour.

H III.6₀: People high on the personality domain Openness do not show less favourable self-reported attitudes towards cybercrime and cybersecurity.

The interdependencies among the variables of interest is illustrated in a correlation matrix in figure 7.2. Looking at this pairwise correlation matrix shows a couple of weak but significant values. It seems as if there is significant evidence for self-reported risky cybersecurity behaviour being negatively correlated with the Honesty-Humility dimension and positively correlated with the dimension Conscientiousness. This evidence would support *H II.1* but not *H II.5*. There are even more weak but significant correlations for self-reported attitudes towards cybercrime and cybersecurity. All except of the dimension Agreeableness seem to add valuable information for explaining study participants' self-reported attitudes towards cybercrime and cybersecurity. The directions of the effects do however not always correspond with the ones hypothesized. To confirm the dependency of these observed first results, a linear model for each of the latter two variables is built.

Figure 7.2 correlation matrix of variables of interest



A look at table 7.4 provides information about the descriptive statistics of the sample. It is easy to see that the variation of participants' age is rather small, which is no wonder given the organizational background of the study participants. Interesting to see are absolute values of the RCsB and ATC-IB score. Former is a scale that ranges from 0 to 120 and latter from 25 to 100, with higher values being associated with risky behaviour for the former and with more favourable attitudes towards cybersecurity for the latter. The table shows that for either instrument the means are respectively low /high. The self-reported behaviours and attitudes are therefore rather favourable for desired behaviours and attitudes.

Table 7.4: Descriptive statistics

	N	Min	Max	Mean	Std.
Age	180	21	36	26.88	3.48
Hone	180	1.80	5.00	3.64	0.59
Emot	180	1.10	3.90	2.58	0.54
Extr	180	1.60	4.60	3.52	0.62
Agre	180	2.10	4.80	3.43	0.52
Cons	180	1.90	4.90	3.80	0.62
Open	180	2.00	4.80	3.23	0.64
RCsB	180	5	57	23.83	10.22
ATC-IB	180	57	94	70.38	6.79
RCsB Mean	180	0.25	2.85	1.19	0.51
ATC-IB Mean	180	2.28	3.76	2.82	0.27
IVE	180	1.00	4.00	1.28	0.60

We obtain the results for the estimated linear model as presented in table 7.5 below, once the model is built and regression is run through the statistic software.

Table 7.5: Results of linear regression model

	RCsB_Mean			ATCIB_Mean		
	Est.	Std.	p	Est.	Std.	p
(Intercept)	1.621	0.477	0.001	2.395	0.243	0.000
Hone	-0.231	0.067	0.001	0.037	0.034	0.277
Emot	0.042	0.070	0.548	-0.103	0.035	0.004
Extr	0.038	0.062	0.541	0.046	0.032	0.147
Agre	0.015	0.074	0.839	-0.002	0.038	0.965
Cons	-0.071	0.064	0.266	0.045	0.032	0.165
Open	0.109	0.058	0.064	0.077	0.030	0.011
IVE2	0.150	0.102	0.142	-0.124	0.052	0.018
IVE3	0.261	0.184	0.158	-0.102	0.094	0.279
IVE4	0.071	0.350	0.840	-0.338	0.178	0.060

The p-values show that indeed there are some HEXACO personality dimensions that obviously have a statistically significant impact on the self-reported risky cybersecurity behaviour and attitudes. On a 5% significance-level Honesty-Humility is a good predictor for the risky behaviour with people who seem to be fairer and more honest to be less engaged in risky behaviour. With respect to ATC-IB, people with higher scores in the Emotionality dimension are expected to score lower on the ATC-IB scale, thus presenting less favourable attitudes towards cybercrime and cybersecurity in a business and organizational setting. At the

same time, a higher score in the domain Openness is expected to lead to more favourable attitudes. Interestingly, the variable IVE2, which reflects people who report that they unlikely expect individual victimization in the next 12 months, has a statistically significant negative impact on the attitudes score.

The researcher performed further statistical analysis to come up with an increasingly meaningful model. Stepwise bidirectional selection can help to eliminate variables that have no significant dependence on the target quantity. Table 7.6 shows the obtained results of this process with the remaining variables per each dependent variable.

Table 7.6: Results of linear regression model after stepwise bidirectional selection

	RCsB_Mean			ATCIB_Mean		
	Est.	Std.	p	Est.	Std.	p
(Intercept)	1.867	0.281	0.000	2.610	0.174	0.000
Hone	-0.270	0.062	0.000	NA	NA	NA
Open	0.095	0.057	0.095	0.083	0.029	0.005
Emot	NA	NA	NA	-0.107	0.035	0.003
Cons	NA	NA	NA	0.063	0.030	0.039
IVE2	NA	NA	NA	-0.122	0.052	0.020
IVE3	NA	NA	NA	-0.121	0.092	0.192
IVE4	NA	NA	NA	-0.308	0.177	0.083

The table shows that for the RCsB dependent variable only two HEXACO dimensions remain in the model, but when using a 5% significance-level only the dimension Honest-Humility remains. This confirms the previous model. The dimension Honesty-Humility has a highly statistically significant negative impact on the self-reported risky cybersecurity behaviour. For the model where ATC-IB is the dependent variable, there remain four highly statistically significant variables on a 5% significance-level in the model. The dimensions Openness and Conscientiousness seem to have a weak positive impact on the self-reported attitudes, whereas Emotionality and IVE2 seem to have a negative impact.

Finally, an F test confirms the significance of the reduced model with only the selected variables and in a second step shows that the excluded variables do not contribute significantly to the estimation of the target quantities.

Table 7.7: Results of F-Test

name	Res.Df	RSS	Df	Sum of Sq	F	Pr(>F)	R²	Adj. R²
RCsB_Mean	179	46.749	NA	NA	NA	NA	0.000	0.000
RCsB_Mean	177	41.760	2.000	4.989	10.499	0.000	0.107	0.097
RCsB_Mean	173	41.101	4.000	0.660	0.694	0.597	0.121	0.090
ATCIB_Mean	179	13.191	NA	NA	NA	NA	0.000	0.000
ATCIB_Mean	176	11.201	3.000	1.990	10.406	0.000	0.151	0.136
ATCIB_Mean	173	11.028	3.000	0.173	0.903	0.441	0.164	0.135

The internal consistency of the questionnaires is also of importance when conducting survey research. The questionnaires HEXACO, RCsB and ATC-IB were analysed for their internal consistency with Cronbach's alpha tests. Table 7.8 shows the results of the tests.

Table 7.8: Internal consistency of the test instruments

	alpha	Booststrap CI
HEXACO	0.749	[0.691,0.797]
ATC-IB	0.716	[0.65, 0.768]
RCsB	0.595	[0.497,0.671]

The results for the HEXACO (0.749) and for the ATC-IB (0.716) are in an acceptable range. Values above 0.70 are reflect a good internal consistency for a survey instrument (Bland & Altman, 1997), although other authors consider a reliability of 0.60 and higher adequate too (Field, 2000). Cronbach's alpha for the ATC-IB was on 0.70 to 0.80 range in the original and in replication studies where the instrument was used (Hadlington, 2017; Aivazpour, 2019; Nunes et al., 2021). Cronbach's alpha is lower for the RCsB with 0.595 in the study at hand. Previous studies measured values above 0.70 for the RCsB (Hadlington, 2017; Aivazpour, 2019; Nunes et al., 2020).

The research hypotheses shall be evaluated in the following paragraph. Table 7.9 illustrates the evaluation result.

Table 7.9: Research hypotheses evaluation

RCsB_Mean		ATCIB_Mean	
<i>H0</i>		<i>H0</i>	
H II.1	reject	H III.1	not reject
H II.2	not reject	H III.2	not reject
H II.3	not reject	H III.3	not reject
H II.4	not reject	H III.4	not reject
H II.5	not reject	H III.5	reject
H II.6	not reject	H III.6	not reject

Honesty-Humility has a statistically significant negative impact on the self-reported risky cybersecurity behaviour. Reserve soldiers scoring high are therefore expected to show less risky behaviour. The null-hypothesis of *H II.1* can thus be rejected on a 5% significance-level. Openness seems to have a weak positive impact on risky cybersecurity behaviour, which confirms *H II.6*. However, on a 5% significance-level the null-hypothesis of *H II.6* cannot be rejected by a very small degree. The remaining four HEXACO variables do not show to have any statistically significant impact on the self-reported RCsB and null hypotheses cannot be rejected. It looks differently in terms of statistical significance for the role of HEXACO personality traits in predicting self-reported scores on the ATC-IB scale. The direction of the effects does however only in one out of three cases correspond to the constructed hypothetical considerations. The null-hypothesis of *H III.5* can be rejected at a 5% significance-level. Reserve soldiers who score high on the Conscientiousness dimension are expected to show more favourable attitudes towards cybercrime and cybersecurity as measured by the ATC-IB. The results for the dimensions Openness and Emotionality are highly statistically significant too but do not correspond to the hypothesized effect. The results suggest that the higher one scores in the dimension Openness the more favourable the attitudes towards cybercrime and cybersecurity will be. On the contrary, higher scores in Emotionality are expected to result in less favourable attitudes. Only the null hypothesis of *H III.5* can thus be rejected.

7.3 Serious Gaming for Social Engineering Resilience

Research question IV deals with the effect of the serious gaming training on experimental group participants' proneness towards phishing email compared to the performance of the control group. The effect of the training can be observed in the two post-tests. The null-hypothesis and the alternative hypothesis are denoted as follows:

H IV. 1₀: Participation in the SG does not affect individual proneness towards SE deception rationales.

and

H IV. 1₁: Participation in the SG affects individual proneness towards SE deception rationales.

Classical statistical tests on just the post-tests can be used treating them like a cross-sectional study. Observing just the effects of the SG on the experimental groups treats the experiment as a longitudinal study. Both dimensions, pre versus post as well as participant versus control, can be combined in a difference-in-differences analysis to look for combined insights. In an even more in-depth analysis, the error terms of mixed effects among each participant can be taken into account with generalized linear mixed effects analysis. Finally, the test improvement of either group from pre-test results is analysed.

Cross-Sectional Analysis

The chi-squared contingency test relies on contingency tables to test for dependence of variables, in this case the indicator of having participated in serious gaming training and the indicator of having failed the test.

Table 7.10: Contingency table with pre- and post-test results per study group

	Link						Info					
	pre		Post-test 1		Post-test 2		pre		Post-test 1		Post-test 2	
	pass	fail	pass	fail	pass	fail	pass	fail	pass	fail	pass	fail
PSG												
contr	59	79	114	24	102	36	69	69	131	7	124	14
exp	18	24	36	6	32	10	20	22	41	1	36	6

Neither the results for the link assessment level nor the ones for the info assessment level show significant indications of a dependence between the two variables. It is worth to note, however, that the chi-squared test may not give accurate results with certain entries in the contingency table being below 10. For these cases Fisher's exact test is conducted simultaneously giving better results since it tests for the one-sided alternative hypothesis of odds ratios being below

1. However, there is still no statistically significant indication to be found for the impact of the participation in the training.

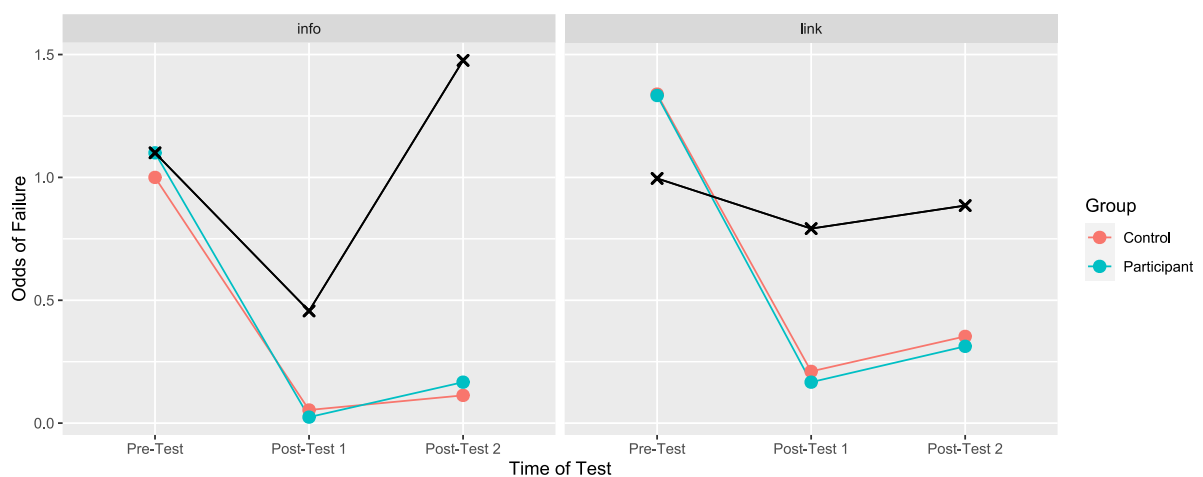
Table 7.11: Test results per type and pre-/post-test point in time

Type	Time	X-squared	P-value
info	pre	0.009	0.925
info	1post	0.098	0.754
info	2post	0.218	0.640
link	pre	0.000	1.000
link	1post	0.056	0.813
link	2post	0.009	0.925

Longitudinal Analysis

Longitudinal analysis focuses on the odds ratios and risk ratios of the two groups over time. If the hypothesis is correct that the serious gaming training helps in reducing the odds or the risk of failure, then significant differences from the pre-test to the post-test should be observable in the experimental group, but not in the control group. However, it looks as though both groups significantly improve due to an unknown effect. The black line illustrates the odds ratios of the respective tests, namely the odds of failure of the participant group in relation to the control group.

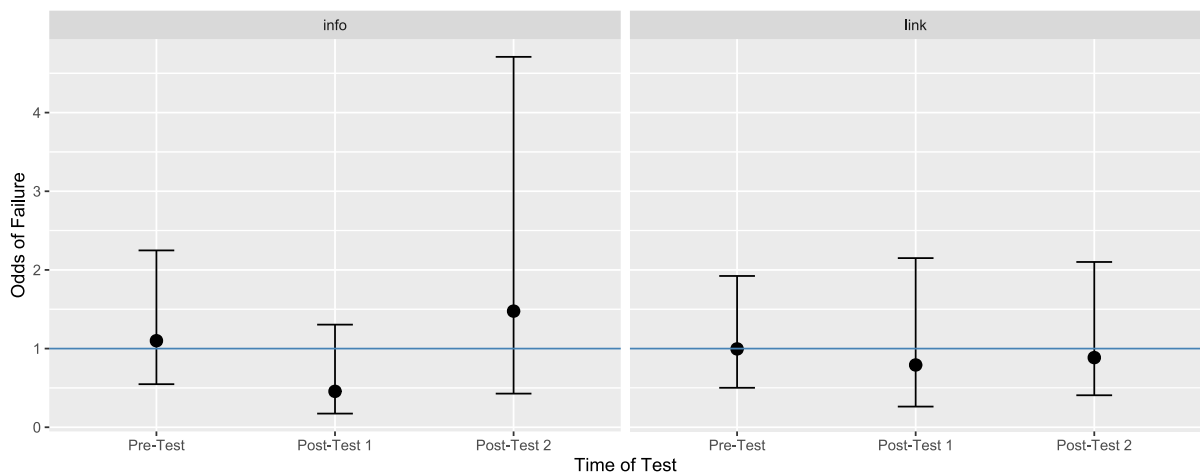
Figure 7.3: Longitudinal illustration of pre- and post-test results



Bootstrapped odds ratios

Non-parametric bootstrap samples can be used to test the statistical variation of the measured odds ratios. The individual participants are sampled independently at random, and a bias-corrected accelerated bootstrap confidence interval is constructed. Since all the confidence intervals well include the value 1, one can conclude that the measured odds ratios are the product of statistical variation and cannot be used to make a definitive statement about the relationship of the odds of failing the tests and participation in the serious gaming training.

Figure 7.4: Statistical variation of bootstrapped measured odds ratios



McNemar Test

The McNemar test allows for a pre-post analysis of the experimental group. The paired results tables are shown for the link assessment level for the improvement at both the first and second post-test compared to pre-test results. Clearly a lot of participants experience no change as can be seen by the high numbers in the diagonal, but for those that do experience change they often times go from failing the pre-test to passing the post-test.

Table 7.12: Contingency table – link clicked in pre and 1st post-test

	pass	fail	Sum
pass	17	1	18
fail	19	5	24
Sum	36	6	42

Table 7.13: Contingency table – link clicked in pre and 2nd post-test

	pass	fail	Sum
pass	16	2	18
fail	16	8	24
Sum	32	10	42

A very similar picture shows itself for the info assessment level as well.

Table 7.14: Contingency table – information inputted in pre and 1st post-test

	pass	fail	Sum
pass	20	0	20
fail	21	1	22
Sum	41	1	42

Table 7.15: Contingency table – information inputted in pre and 2nd post-test

	pass	fail	Sum
pass	19	1	20
fail	17	5	22
Sum	36	6	42

The p-values turn out to be fairly significant for both the participant and the control group. The only possible conclusion is thus that everybody improved significantly from the pre-test to both post-tests, but this does not necessarily have to do with the training.

Table 7.16: McNemar's test results

	Post-Test 1		Post-Test 2	
	Link	Info	Link	Info
contr	0.00000	0.00000	0.00000	0.00000
exp	0.00014	0.00001	0.00218	0.00041

Difference-in-Differences Analysis

Next, the combined information about test results and allocation to either study group are analysed. The easiest way of incorporating both the pre- and post-tests as well as the information about the control and experimental group is to do difference-in-differences estimation. This works by constructing a linear model which can be estimated by a similar procedure as is done for linear regression.

Table 7.17: Difference-in-differences estimation results

	Link		Info	
	Est.	p	Est.	p
(Intercept)	1.339	0.016	1.000	1.000
time1post	0.157	0.000	0.053	0.000
time2post	0.264	0.000	0.113	0.000
PSGpart	0.996	0.987	1.100	0.702
time1post:PSGpart	0.795	0.680	0.415	0.429
time2post:PSGpart	0.889	0.807	1.342	0.612

The difference-in-differences parameters present no significant effect and the model including them fails to be significant in a likelihood ratio test over the null-hypothesis.

Table 7.18: Likelihood ratio test results

type	Resid. Df	Resid. Dev	Df	Deviance	Pr(>Chi)
link	536	858.216	NA	NA	NA
link	534	858.020	2	0.196	0.907
info	536	689.863	NA	NA	NA
info	534	688.753	2	1.11	0.574

The model confirms that there is a statistically significant influence of the time component on the test results. However, neither participation in the training nor the combined effect of time and participation seem to have a relevant effect on participants' test performance. Thus, $H_{IV.1_0}$ cannot be rejected.

Generalized Linear Mixed Effects

Mixed-effects models include an error term for each participant in addition to the standard error term of fixed-effects models, which accounts for the error in each experiment. They thus consider the correlation between the results of each participant. The measurement for each of the fixed-effects will have lower power since this correlation is respected in the model, but comparing models is more accurate. In the following, only likelihood ratio tests are performed to see if the inclusion of the difference-in-differences parameters is significant or not:

Table 7.19: Likelihood ratio test of mixed effects

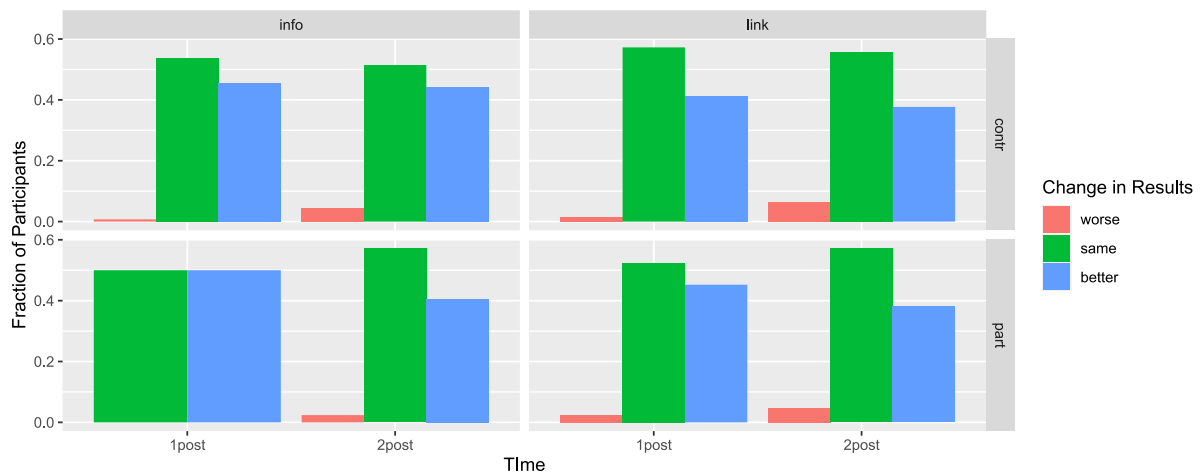
type	npar	AIC	BIC	logLik	deviance	Chisq	Df	Pr(>Chisq)
link	4	719.385	736.551	-355.693	711.385	NA	NA	NA
link	5	721.342	742.799	-355.671	711.342	0.044	1	0.835
link	7	725.027	755.068	-355.513	711.027	0.315	2	0.854
info	4	578.067	595.233	-285.033	570.067	NA	NA	NA
info	5	579.993	601.451	-284.997	569.993	0.074	1	0.786
info	7	581.229	611.27	-283.614	567.229	2.764	2	0.251

Again, there seems to be no statistically significant indication that the inclusion of the difference-in-differences parameters improves the model in a way that the null-hypothesis can be rejected. Only slight indications for the support of $H_{IV.1_1}$ can be seen for the info assessment stage with a statistic of 0.251 being obviously lower than for the remaining scenarios.

Improvement from Pre-Test

In a similar fashion to McNemar's test, the pre-test results can be included in the regression model to extract the participants improvement in the post-tests compared to the pre-test instead of raw performances. To be able to include this variable in the model, the random-effects are dropped. Figure 7.7 shows the change in test results of either study group for each post-test compared to the pre-test.

Figure 7.5: Change in test results per study group and post-test



The results of the pre-test are simply added as a predictor, to construct a linear model. The joint distribution of pre- and post-test results can be shown in a table of probabilities. For each table the marginal odds ratio of failing the post-test with the given pre-test result is added. Since this odds ratio is quite a bit lower for those participants that passed the pre-test than for those who did not, this could be a valuable predictor for post-test results.

Table 7.20: Contingency table for pre- and post-tests with odds ratios

Pre-Test	Post-Test 1			Post-Test 2		
	pass	fail	OR	pass	fail	OR
pass	0.450	0.011	0.025	0.411	0.050	0.122
fail	0.444	0.094	0.212	0.406	0.133	0.329

The linear model now has one modifier for time being the second post-test and one for participation in serious gaming training as before and then one additional modifier for passing the pre-test.

Indeed, the effect for the pre-test result has a significant p-value for both the first and the second post-test.

Table 7.21: Linear model estimation results

	Link		Info	
	Est.	p	Est.	p
(Intercept)	0.075	0.000	0.025	0.000
time2post	1.783	0.034	2.726	0.021
PSGpart	0.837	0.585	1.083	0.863
prefail	4.385	0.000	2.659	0.025

The likelihood ratio tests show again that the pre-test result is certainly a good predictor for the later results. Including the indicator of the training in a second step remains, however, still insignificant.

Table 7.22: Likelihood ratio test results

type	Resid. Df	Resid. Dev	Df	Deviance	Pr(>Chi)
link	358	366.81	NA	NA	NA
link	357	341.247	1	25.563	0.000
link	356	340.943	1	0.304	0.581
info	358	191.035	NA	NA	NA
info	357	185.489	1	5.546	0.019
info	356	185.459	1	0.03	0.864

This section provided different analyses to investigate on the hypothesis that the participation in the SG training statistically significantly reduces the proneness of experimental group participants in falling victim for SE fraud, measured in the response behaviour in three phishing email settings. The detailed analysis provided no indications to reject $H_{IV.1_0}$ and thus conclude that the SG helped to decrease the likelihood of failing the post-tests for experimental group participants. Indeed, an improvement of both groups, the experimental and the control, was observed. The results show that there must be other effects that are responsible for this improvement. Additionally, the results also show that one possible explanatory variable is time or put differently: previous victimization is a good predictor for future victimization.

7.4 General Classification Model

In a further step, the data were analysed with a general classification model method. General classification models can be used to derive insights from the whole dataset at once. First, it includes once again a logistic regression estimation by using all measured variables in the estimation and applying a variable selection method to sort out the most important variables for the model. Second, further classification techniques are applied by using decision trees and random forests.

Logistic Regression

A logistic regression model can be built that incorporates all variables for both the link and info assessment levels. It can be seen that the time variable is obviously most predictive of test failure due to the unknown reasons already discussed above. Additionally, the individual victimization expectation seems to be quite indicative of test failure although one has to take into account the fact that not many participants fall into the high value bins there. The effect estimates are transformed from log scale to linear scale to represent ratios here.

Table 7.23: Logistic regression model estimation results

	Link		Info	
	Est.	p	Est.	p
(Intercept)	3.216	0.519	0.188	0.447
PSGpart	0.962	0.882	1.178	0.597
time1post	0.129	0.000	0.037	0.000
time2post	0.229	0.000	0.104	0.000
Hone	1.093	0.655	1.637	0.047
Emot	0.787	0.246	0.838	0.480
Extr	0.951	0.783	1.080	0.727
Agre	0.860	0.472	1.095	0.719
Cons	1.027	0.884	0.788	0.295
Open	1.053	0.764	0.811	0.320
PIST_pitrue	0.704	0.275	0.914	0.811
PIST_piOTtrue	1.024	0.965	1.012	0.985
PIST_mitrue	0.467	0.296	0.660	0.601
PIST_miOTtrue	0.982	0.981	0.754	0.740
PIV_receivetrue	0.540	0.005	0.509	0.012
IVE2	1.635	0.089	1.653	0.151
IVE3	4.494	0.003	5.219	0.005
IVE4	1.113	0.914	0.652	0.737
RCsB_Mean	1.199	0.412	1.247	0.412
ATCIB_Mean	1.040	0.931	1.678	0.340

Stepwise selection in both directions can now be used to exclude all variables that are not significantly contributing to the predictions. One is then left with the time variables again, previous participation in security training, which are all very correlated values, previous victimization and victimization expectation. Table 7.24 shows that among these remaining variables it is the individual victimization expectation (IVE3) that seems to have the highest estimated impact (4.280 for Link stage and 4.454 for Info stage) on the eventual victimization in the phishing test. Thus, study participants who reported that they consider themselves neither likely nor unlikely to fall for such a scam in the next 12 months are – based on the results – almost four times more likely to eventually fall for it than those who said that they consider themselves likely to fall for such a scam (IVE4). Additionally, for the info assessment level the Honesty-Humility personality trait seems to indicate higher failure chance somewhat significantly on a 10% significance level, meaning that people scoring higher on the dimension thus are considered to be more honest and fairer in social contexts are expected to have a higher proneness in this research setting. Previous completion of a security training concerning military related information (PIST_mittrue), as well as self-reported previous individual victimization (PIV_receive_true) seem to somehow halves the chance of falling for the phishing scam.

Table 7.24: Final model after bidirectional variable selection

	Link		Info	
	Est.	p	Est.	p
(Intercept)	2.048	0.001	0.348	0.204
time1post	0.131	0.000	0.039	0.000
time2post	0.232	0.000	0.107	0.000
PIST_mittrue	0.429	0.003	0.505	0.044
PIV_receivetrue	0.530	0.003	0.519	0.011
IVE2	1.635	0.075	1.653	0.132
IVE3	4.280	0.002	4.454	0.007
IVE4	0.954	0.961	0.574	0.655
Hone	NA	NA	1.496	0.068

For completeness's sake, a chi-square test confirms that the estimates of the model are in fact significant and adding the variables that were left out by the selection does not change the estimates significantly anymore.

Table 7.25: Chi-square test results

type	Resid. Df	Resid. Dev	Df	Deviance	Pr(>Chi)
link	539	686.041	NA	NA	NA
link	532	580.866	7	105.175	0.000
link	520	576.963	12	3.903	0.985
info	539	569.566	NA	NA	NA
info	531	419.126	8	150.440	0.000
info	520	413.949	11	5.177	0.922

Decision Trees

Further, we use decision trees to analyse the data more in-depth and have a closer look at interaction effects. This provides the possibility to discover how the test results are clustered with respect to the measured variables. The tree sizes are selected using cost complexity pruning. For both assessment levels, the click and the info level respectively, the first split is always on time, which is the pre-test outcome, and all post-test results are then estimated as passing the test. Next the evaluation of risky cyber security behaviour seems to be indicative of failure for the participants during the pre-test at the link assessment level, only. For the info assessment level, there is a broader nested split. The personality domain Conscientiousness, risky cybersecurity behaviour, attitudes towards cybercrime and the personality trait Honesty-Humility seem to be a meaningful split and seem to be indicative for failure in the pre-test stage.

Figure 7.6: Decision tree split for link assessment level

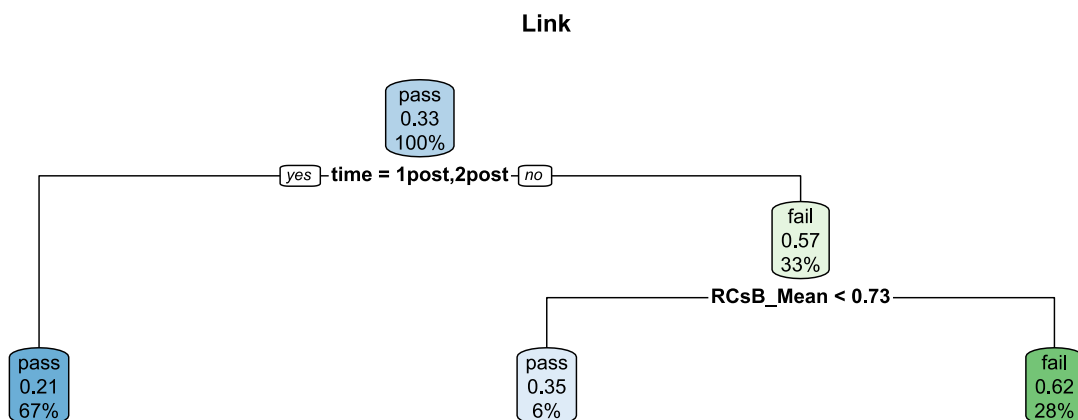
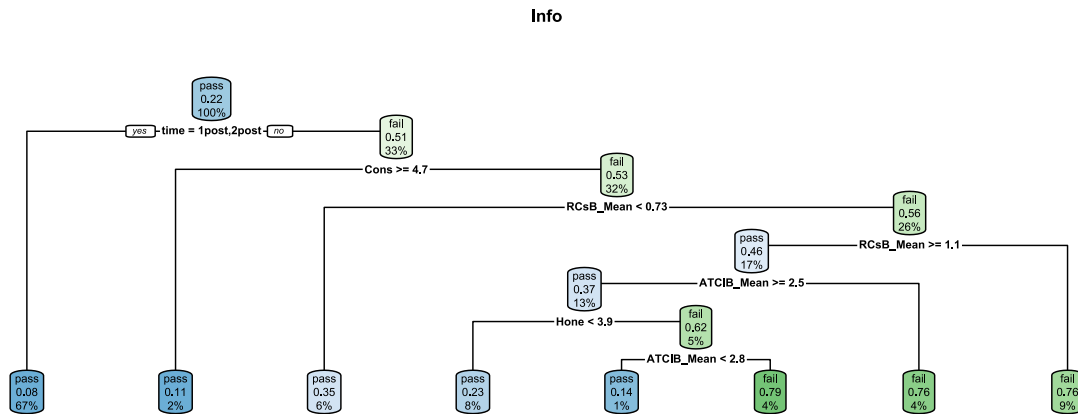


Figure 7.7: Decision tree split for info assessment level



Random Forests

Finally, we can use random forests to come up with increasingly effective predictive models. Random forests use bootstrap aggregation of decision trees and can use the individual trees to derive importance scores for each variable by using mean decrease measures upon permutation.

For the accuracy measure it seems like time is the only relevant predictor although for the link assessment level most variables except participation in serious gaming and previous security training could be contributors. For measuring clustering capabilities again time is most important, but the personality traits as well as risky cyber security behaviour and attitude towards cyber security form a group of somewhat important variables.

Figure 7.8: Random Forest results for clicking link in the pre-test

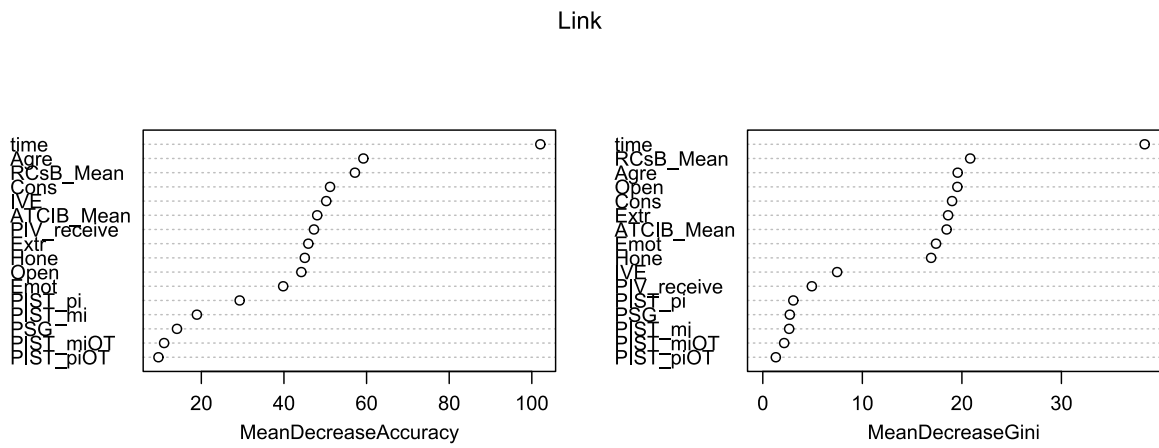
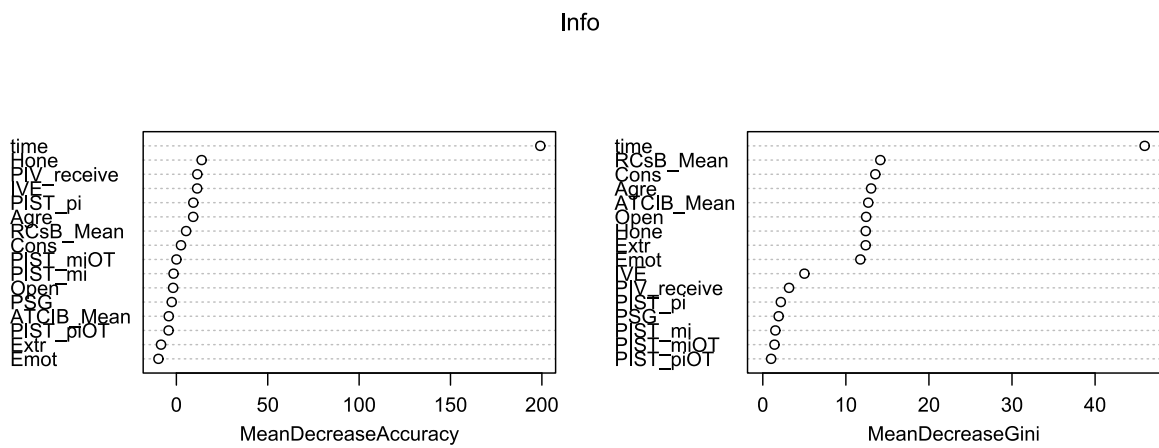


Figure 7.9: Random Forest results for inputting info in the pre-test

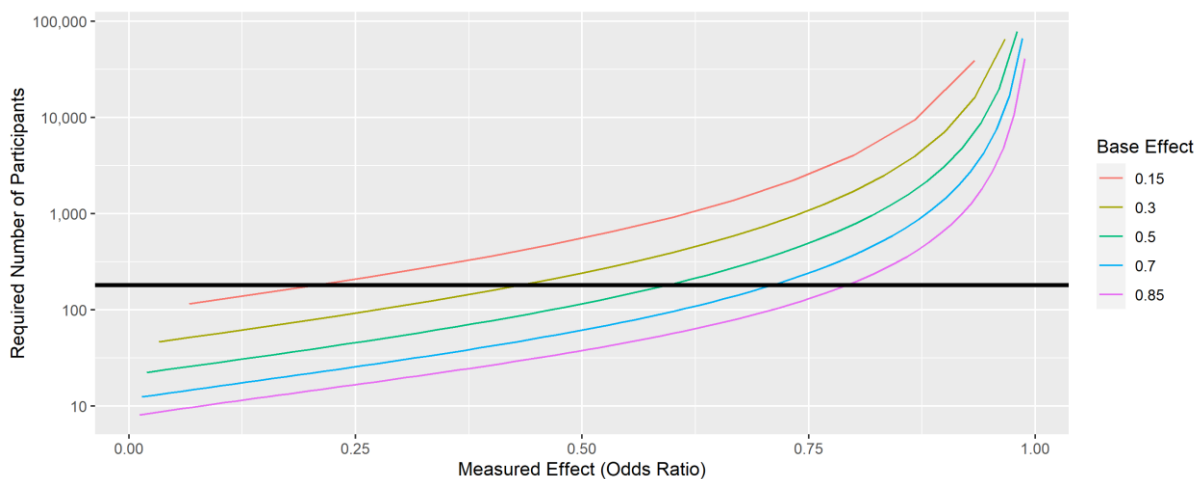


7.5 Power Analysis

The data were further analysed by using power analysis. Power analysis is a hypothetical way of looking at research questions regarding data that give insight into the chances of detecting statistically significant effects in different scenarios. The analysis is conducted at a power level of 80%, which is the chance of detecting an effect at statistical significance level 5%.

First, we can look at the power of the chi-squared test that is conducted on the post-tests and checks dependence of the indicator of having taken part in SG training with the test results. The required number of participants depends on the base level, which is the probability that a member of the control group passes the post-test independent of training. The desired effect to be measured is expressed as the odds ratio of failing the test when having participated in the SG training.

Figure 7.10: Required number of participants per base effect



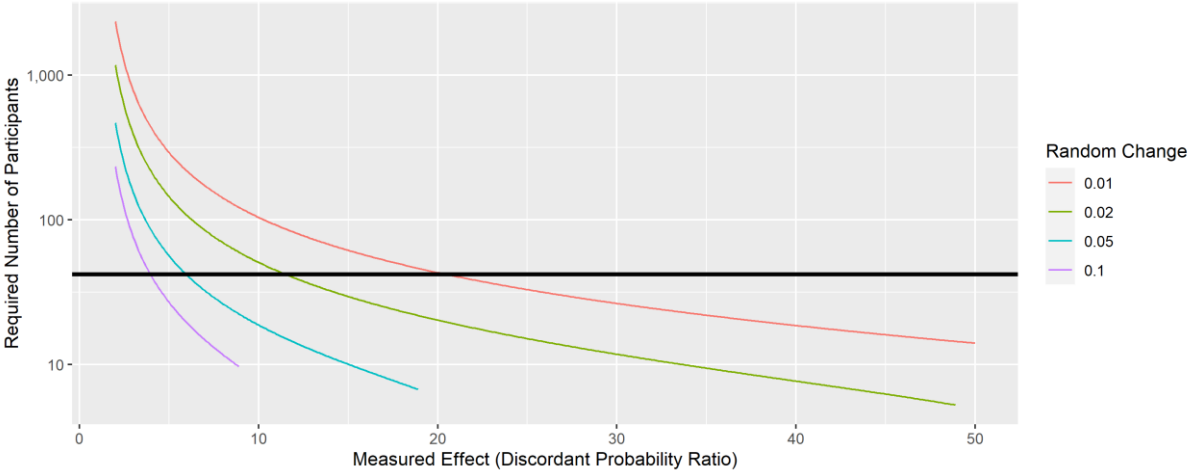
A very generous assumption is that the training leads to a measurable odds ratio of 0.5, meaning that once the training is completed, it will lead to a chance of 50% of the respective participant to pass the post-test. We can then see that, since the post-tests have base effects even lower than 15%, more than 500 participants would have been needed to get a significant result on even such a low odds ratio. We can also see that if the post-tests had a base effect of around 50%, such as the pre-tests had, the number of participants would have been sufficient to measure an odds ratio of up to 0.6.

The same analysis or a McNemar's test can also be performed with the results of experimental group participants. The base effect here is the chance of a participant to change their result in either direction at random. Thus, changing from failing the pre-test to passing the

post-tests or from passing the pre-test to failing the post-tests randomly. The measured effect here is the discordant probability ratio, which is the ratio between the participants that went from failing to passing due to the training and the participants changing in the other direction.

Figure 7.11 shows that with a probability level of 1% the size of the training participant group (the black line) was sufficient to return a measured effect of 20 times more people improving from pre-test to post-test than the other way around. Thus, there is statistically significant evidence that the number of participants in the experimental group was sufficient.

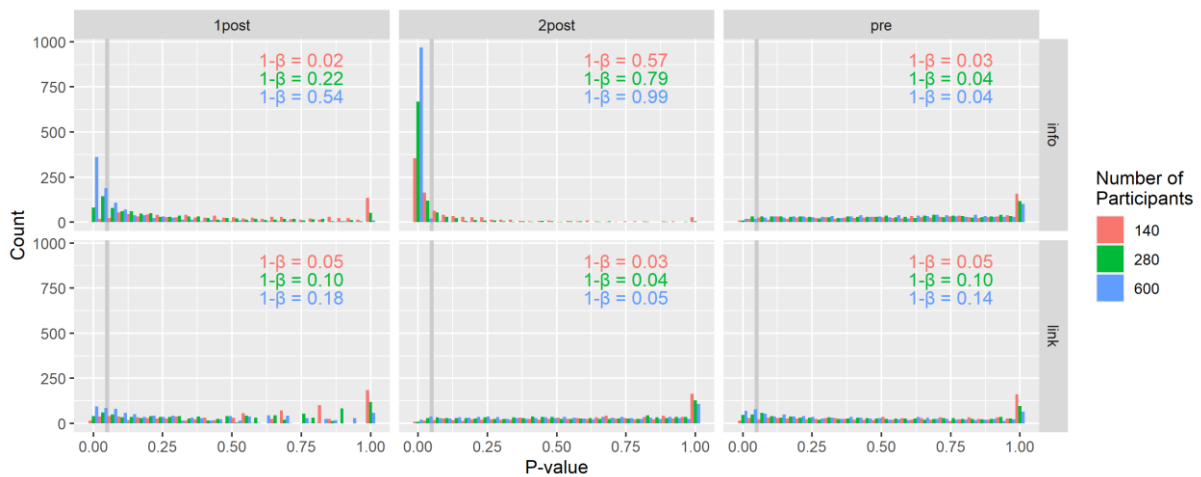
Figure 7.11: Required number of participants per discordant probability ratio



7.6 «What-If» Analysis

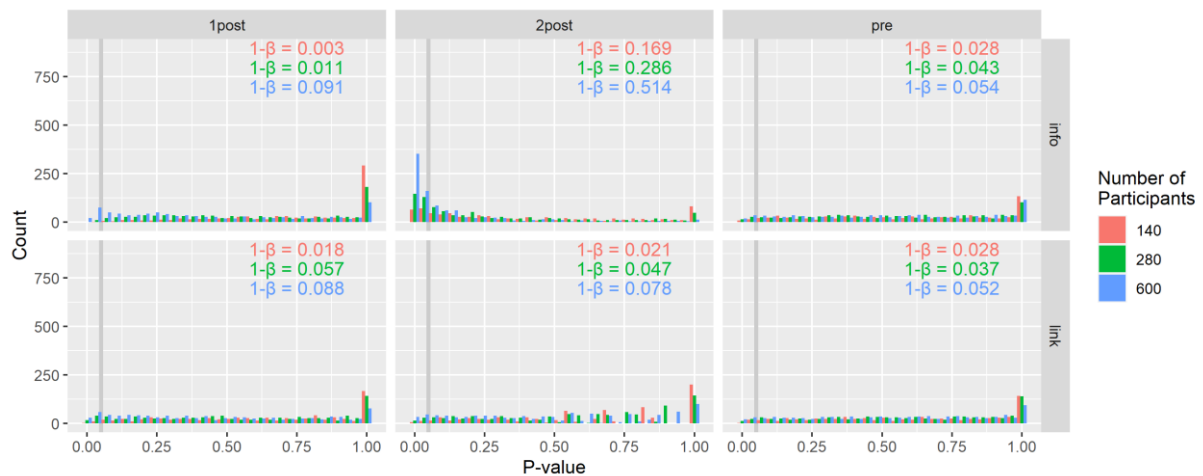
In an ultimate analysis, the data was used to look at even more hypothetical scenarios. Those synthetic approaches can be checked by «What-If» analysis which uses resampling to derive results for synthetic data. A very interesting problem is the fact that all participants of the post-tests improved and had a very low probability of failing them. This results in weak power of the chi-squared test, as could be seen in the section above with the null-hypothesis that post-test results of experimental and control group are different due to the training could not be rejected. There can be various explanations for this stemming from variables that were not measured or as an ultimate conclusion that the game itself is indeed not effective as a means to change behaviour towards SE phishing email resilience. A synthetic dataset can be created where the participants are resampled such that an equal number of them pass and fail the first link post-test. Additionally, the number of participants is also oversampled to exaggerate any measured effects and study the result of the chi-square test if more participants were used.

Figure 7.12: «What-If» analysis results with synthetic dataset



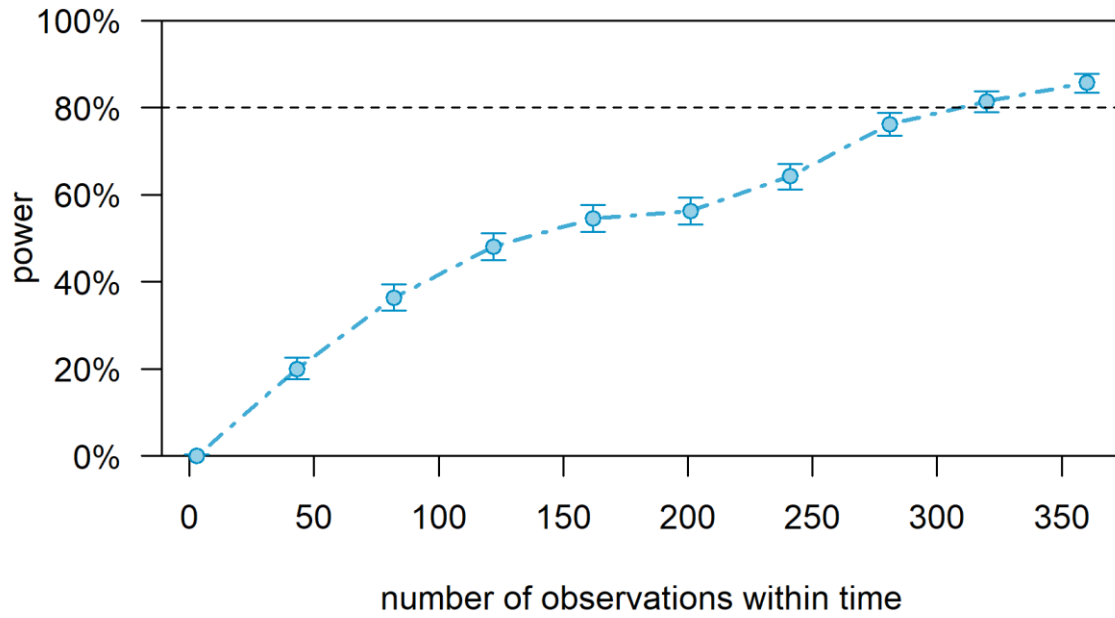
The numbers in the plot refer to the estimated power of the test and indeed the two info post-tests now give significant results for the dependence of participating in serious gaming training and passing the info assessment level. It shows that indeed there are statistically significant results observed at least for the two info post-tests with large statistical power, as can be seen by the numbers for $1 - \beta$ in the plot. It is clearly visible that the synthetic dataset in these cases used a sample size that is double to four times as large, as the effective sample size in the experiment. However, this is evidence that with a larger sample size a statistically significant dependence between participating in the serious game and passing the info post-test were to be observed. One needs to be careful though since the significant results indicate only dependence and not whether the effect was positive or negative. The same resampling method and analysis is repeated by synthetically sampling the participants such that the results in the second link post-test are equal. This gives similar but somewhat weaker results.

Figure 7.13: «What-If» analysis results with synthetic dataset



Finally, the «What-If» analysis can also look at the difference-in-differences test and analyse it for its power. To incorporate the above assumption, the effect of the time variable, which refers to past victimization in the pre-test, is set to 0, such that the post-test results are assumed to have the same base failure chance as the pre-test, which is around 50%. Next, we assume that the difference-in-differences effect of SG training leads to an odds ratio of 0.4, which is a generous assumption, but it was at least observed for the first info post-test. One can now see that there is not enough power with the current number of participants and around 350 would have been needed to derive statistically significant results regarding the participation in the SG training in relation to the test performances among the two study groups without guarantee of the desired direction of observed effect being met.

Figure 7.14: Required number of participants for a statistical power of 80%



7.7 Subjective Effects of Serious Gaming

Experimental group participants took a short survey after the SG training in the experimental intervention phase. Besides insights about participants' satisfaction with the training and the administration of the training, they were also asked to provide their self-perceived opinions about the usefulness of the game and other self-perception dimensions. Detailed descriptive statistics about the data set can be found in chapter 6.2. Hypotheses $H_{IV.2}$ – $H_{IV.4}$ were constructed to derive inferences about the power of the SG based on participants' perception. The null-hypotheses are the following:

$H_{IV.2_0}$: *Participants' perceived knowledge gain about SE does not positively depend on their perceived usefulness of the SG.*

$H_{IV.3_0}$: *Participants' perceived gain in awareness about SE threats does not positively depend on their perceived usefulness of the SG.*

$H_{IV.4_0}$: *Participants' perceived likelihood of the training helping them to avoid future SE victimization does not positively depend on their perceived usefulness of the SG.*

Linear regression analysis quickly return the estimated parameters and the related p -values for each of the three regressions. Tables 7.26 -7.28 show the respective results.

Table 7.26: Perceived knowledge gain about SE and perceived usefulness of SG

	Est.	Std.	p
(Intercept)	2.500	0.674	0.000
U_SG	0.417	0.175	0.022

One can see that participants' perceived usefulness of the SG indeed has a positive impact on the perceived knowledge gain about SE with a statistically significant p -value at a 5% significance level.

Table 7.27: Perceived gain in awareness about SE threats and perceived usefulness of SG

	Est.	Std.	p
(Intercept)	1.652	0.692	0.021
U_SG	0.623	0.180	0.001

The perceived usefulness of the SG does even better perform the variable defining the self-perceived gain in awareness about SE threats. One can see that indeed it has a positive impact with a statistically significant p -value at a 1% significance level.

Table 7.28: Perceived likelihood of future SE victimization and perceived usefulness of SG

	Est.	Std.	p
(Intercept)	2.772	0.602	0.000
U_SG	0.190	0.157	0.231

The variable U_SG also has a slight positive impact on the participants' confidence that they will not become victim of SE in the future. However, this is only a weak indication of the positive dependence, as it is not statistically significant.

Based on the results, hypotheses *H IV.2 – H IV.4* can be evaluated as follows:

Table 7.29: Research hypotheses evaluation

	<i>H0</i>
H IV.2	reject
H IV.3	reject
H IV.4	not reject

The null-hypotheses of *H IV.2* and *H IV.3* can be rejected. Participants' perceived usefulness of the SG indeed has a statistically significant positive impact on both the perceived knowledge gain about SE through the game and the perceived increase in awareness about SE threats through the game. Results indicate that there is also a positive effect of the perceived usefulness on participants' confidence in the game making one less prone to SE threats. The statistical evidence is however not significant and the null-hypothesis of *H IV.4* cannot be rejected.

7.8 Summary

This chapter provided the results to the empirical part of this dissertation. A statistical analysis was performed to look at the effects that the participation in the SG training had on the individual proneness of study participants towards SE fraud that was tested in two post-test settings where they received multilevel phishing emails that tested their behaviour of clicking a link or not and if so whether they provided requested information on a simulated landing page afterwards. Post-test phishing results were analysed for their difference among a control and an

experimental group and in comparison, to a pre-test. Different statistical tests were performed to evaluate and verify the obtained results. The participation in serious gaming training was analysed in particular with difference-in-differences estimation that found no significant result. Although there seems to be an effect of participating in the serious game reduces the chances of falling victim to SE phishing fraud there were no statistically significant evidence that would support a decision to accept the research hypothesis.

The second research question of this dissertation asked whether individual differences in terms of HEXACO personality traits do have a statistically significant impact on the proneness towards SE fraud. Logistic regression was used to investigate on this research question. No evidence could be found for the HEXACO personality traits of having any statistically significant influence on the individual proneness towards SE fraud. Although it was possible to compare the research hypotheses with the estimated coefficient of the HEXACO variables that would make it possible to draw hypothetical conclusions, the data of the sample provided not enough evidence that the estimated model contained any statistically relevant HEXACO variable. It was therefore not possible to accept either of the research hypotheses *H II.1 – H II.6*. Other measured quantities were also tested for their effect for the sake of completeness and to look for other explanatory variables. Only participation in previous security training had a weakly significant effect, reducing the odds of failing by about half.

In a further step, the dataset as a whole was analysed at once to construct a general classification model that eventually led to a predictive model with a couple of statistically significant predictors. Most importantly, longitudinal victimization indicators are a strong predictor. Not only does past victimization predict future victimization, but in this regard somewhat logically does current victimization, as measured by the post-test, also indicate past victimization. Similarly, self-reported past victimization is a good predictor too. On the contrary, prior participation in an information security training that dealt with military related information has a statistically significant somewhat positive impact on the victimization in the pre-test. Interestingly, the strongest predictors in terms of estimated coefficient refer to the self-reported individual victimization expectation. An indifference towards the likely future victimization seems to be the predictor with the strongest impact on future victimization, followed by the indicator that reflects a self-reported unlikely future victimization. This is evidence that self-perceived resilience does not predict resilient future desired behaviour. On the contrary, it predicts future undesired behaviour resulting in victimization. Lastly, there is somewhat statistically significant evidence that the personality dimension Honest-Humility is

a good predictor for the proneness towards SE phishing, at least for providing information on a landing page in the second stage of the pre-test phishing email. People who score high on this dimension, thus having a more pro-social altruistic mindset, have a higher chance of failing. Further analysis with decision trees showed that extreme values for the assessment of risky cyber security behaviour can also be an indicator for failing respectively passing the tests. A random forest analysis further showed that time, measured as past and current victimization, is the most important predictor. HEXACO personality traits as well as RCsB and ATC-IB variables form a cluster of somewhat important predictive variables. Variables that reflect participation previous security trainings or in the SG seem to not provide any contribution as predictor.

In the last two sections, the required number of participants for the expected effect of the serious gaming training were discussed with the most probable conclusion that the conducted experiment had not enough participants, not enough randomization in the experimental design or possibly an insufficient effect size for the variable PSG to provide any statistically significant impact. The results of these analyses suggest that three to five times or about 350 to 500 participants would have been necessary.

Finally, this chapter presented the results of the statistical analysis of data collected with the post-serious game survey. Hypotheses *H IV.2 – H IV.4* were tested and the results showed that there is a statistically significant positive relationship of participants' perceived usefulness of the SG on both the perceived knowledge gain through the SG and the perceived increase in awareness about SE threats due to the SG. However, perceived usefulness of the SG was not a statistically significant predictor for the perceived likelihood of future SE victimization resilience.

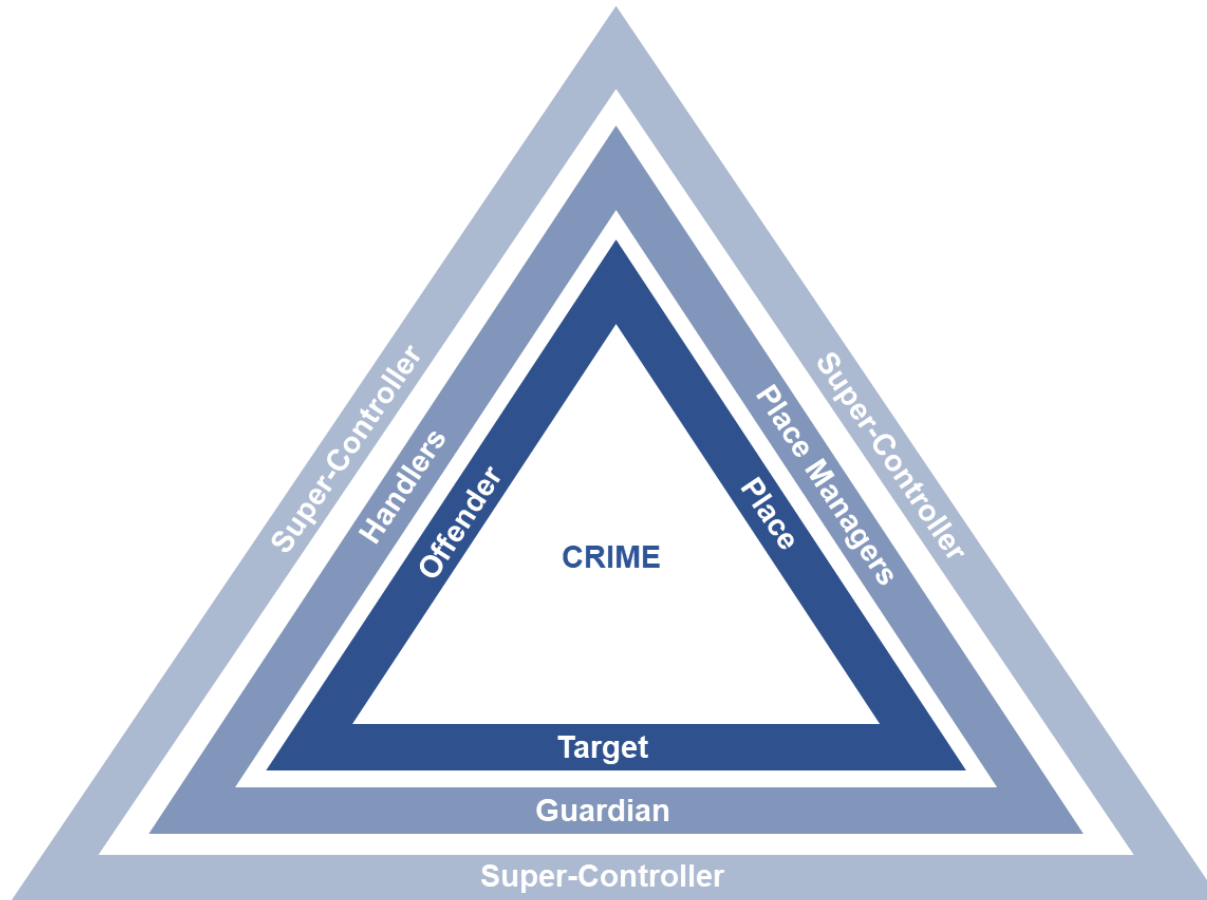
8. A Routine Activity Framework for Social Engineering

This thesis studied the behaviour of Swiss military reserve soldiers in SE situations, while phishing was used to test the behaviour. Phishing is a successful scam – and it was successful in the regard of this study too – as it relies on the psychological deception of individuals that perform routine activities, namely opening emails, looking at the content of the email, sometimes reading the email in detail and not seldomly clicking an attached link. People are used to receive emails with private or work-related content and most of the time they are original, authentic and not supposed to defraud them. Checking and opening emails has become a natural habit for the modern individual. In the course of this dissertation and further to the empirical results, there developed thoughts to look at this phenomenon of routine activity from a rather theoretical point of view with a criminological focus. The following sections will provide these considerations while developing a theoretical framework for SE with a Routine Activity Theoretical approach.

The Routine Activity Theory (RAT) is a criminological theory that aims to explain the occurrence of crimes, criminal victimisation, and offending patterns. Introduced by Cohen and Felson (1979), it consists of the assumption that for a crime to occur, three elements must be present: motivated and capable offenders, suitable targets, and the absence of a capable guardian. The theory has become very useful in explaining dynamics of crimes, patterns in victimisation and the risks towards victimisation, such that it has become “*one of the most influential and policy relevant theories in criminology*” (Tewksbury & Mustaine, 2010). Cohen and Felson (1979) in their original RAT model define the occurrence of crime as a situation where likely offenders, suitable targets and the absence of capable guardian converge in space and time. Over time the theory has developed, and different aspects have been added. Thus, the concept of the guardians as crime preventive power has been defined in more detail under a collective term, as controllers (Tillyer & Eck, 2011). Whereas guardians focus on the victim dimension and protect them, actors that are supposed to control for the place are defined as (place) managers (Eck, 1994). Lastly, handlers control the offender dimension (Felson, 1986). This advanced view of the RAT triangle comprises the elements that are required to be absent for a crime to occur and can be seen as an overlay triangle on the original theory. Sampson et al. (2010) have taken that model yet to another level with the introduction of a third layer, introducing super-controllers. They discuss why controllers are effective only in some cases and in others they do not effectively prevent crime to occur. They conclude that controllers are driven by incentives to prevent crime from happening and that without the appearance of those

specific incentives, controllers are not motivated enough to prevent crimes from happening. Thus, means that control the controllers are required to induce these motivations. Super-controllers, defined as people, organizations, or institutions, provide these incentives and therefore control the controllers. Super-controllers do therefore have only an indirect effect on the prevention of crime through inciting the controllers (Sampson et al., 2010). Figure 8.1 illustrates the RAT and its different layers graphically:

Figure 8.1: The Routine Activity Theory triangles (Sampson et al., 2010)



This short introduction to the RAT approach suggests that it seems reasonable to apply this theoretical framework to crimes determined by deceptive SE techniques as well. SE related crimes specifically make use of human interactions that require a motivated and capable offender and a suitable target to meet in place and time, while a guardian is absent or not capable of deterring the crime. It makes sense for this thesis to look at the RAT approach as a theoretical framework to explain SE related crime and its components. Other researchers already used RAT considerations to look at SE fraud (Hutchings & Hayes, 2009; Leukfeldt, 2014; Glasser et al., 2015; Jansen van Rensburg, 2018; Danquah et al., 2020; Steinmetz, 2021). It is especially useful in looking at patterns of victimisation and the risk of victimisation (Tewksbury & Mustaine, 2010), which lies within the objectives of this research study. Nevertheless, for the sense of adaptability of the theory to SE related crime under a victimization umbrella, the theoretical model particularly looks at the target dimension of the triangle proposed by Sampson et al. (2010) in an adapted configuration of the approach to this specific kind of crime. Thus, this thesis particularly researches the interrelation among the offender and the target dimension of the triangle, namely the target, the guardian and the super-controller. Considerations towards the other components of the different layers of the theory were not reflected in the empirical part of this dissertation. Under the theoretical umbrella of RAT, a SE crime could be termed as a crime where a motivated and capable offender uses deceptive manipulation methods to deceive a victim for acquiring precious information in an online or offline environment with or without the use of technology while a capable guardian is absent or not capable to prevent the crime to occur and a super-controller lacks the capability to incite the guardian for better surveillance.

A motivated and capable offender in this regard is a social engineer, which can be a cybercriminal, a white-collar criminal or other types of offenders possessing the intentions and skills to conduct manipulative offences. Both, “*criminal inclinations and the ability to carry out those inclinations*” are the minimum requirements for an offender to possess (Felson & Cohen, 1980). Whereas the skills of social engineers in general are assumed to be centred around the art of deception, as well as basic technical and information acquisition skills, their motivations can vary broadly, meaning that social engineers have different typologies. Quite often SEA are performed out of pure monetary incentives.¹³ Manipulative phishing mails or

¹³ The 2020 attack on Twitter accounts of US-politicians and VIPs showed that social engineers were taking over the accounts by deceiving Twitter employees. The offenders then tried to deceive the followers of those people to transfer amounts to a bitcoin account in order to receive a doubled reimbursement (Iyengar, 2020; Tidy, 2020).

fraudulent calls where people are tricked to release payments in order to help supposed friends or relatives in emergency are other examples where financially motivated social engineers used this kind of deceptive offence (BKA, 2020; KAPO Zürich, 2020). However, other cases show that the deceptive art of SE is also motivated by the acquisition of valuable information for companies for competitive advantages or even by state-sponsored operations (Winkler, 1996; Hinson, 2008; Conteh & Schmick, 2016). Motivated and capable social engineers, thus, may be characterized as ranging from purely financially motivated criminals or criminal groups on the one hand to white-collar criminals and state-sponsored perpetrators on the other hand.

A suitable target who could be exploited by a social engineer might be generally everything. However, Cohen and Felson (1979 & 1980) define the suitability of a target as “VIVA” (also see Table 8.1). Targets are suitable when they reflect the components *value*, *inertia*, *visibility* and *access*. Thus, the higher the monetary or symbolic value, the less movable or capable of defending oneself and the more easily a target can be discovered and approached, the higher the target’s suitability and risk of victimisation.

Table 8.1: Characteristics of a suitable target (Cohen and Felson, 1979 & 1980)

Characteristic	Definition
Value	Monetary or symbolic value of the target.
Inertia	Degree of movability of the target; self-defending degree of the target.
Visibility	Degree of the target to be discovered as a target.
Access	Degree of easiness to approaching the target.

In a more evolved version of target suitability definition, Clarke (1999) introduces the “CRAVED” characteristics of “hot products”. Objects that are most attractive to offenders are *concealable*, *removable*, *available*, *valuable*, *enjoyable* and *disposable*.

Table 8.2: Characteristics of hot products (Cohen and Felson, 1979 & 1980)

Characteristic	Definition
Concealable	The degree of a product being visible to the potential offenders.
Removable	The degree of a product being easily taken away from its location.
Available	The degree of existence, accessibility and visibility of (new) products.
Valuable	The monetary or symbolic value of the target.
Enjoyable	The degree of the subjective usefulness and pleasure of the product.
Disposable	The degree of being able to re-sell the product.

In the light of SE, the suitable target dimension, as well as the VIVA and CRAVED characterizations deserve some deeper thoughts. Most importantly, it is beneficial to think about the exact definition of the suitable target. Felson himself (2020) says that a suitable target is not automatically the victim. Target and victim need to be separated unambiguously. Offenders usually target property or money while the victim is the holder and/or the owner. There are occasions where the holder and/or owner also is the target, but these are rather exceptions. Moreover, the victim dimension is not unidimensional. The victim of a car theft is the holder of the car at that specific point in time and place but also the owner of the car, which is not always concurring. These considerations are important implications for the routine activity theoretical model of SE offences. Social engineers are usually interested in exploiting information for monetary gain or for the sake of the information itself, like in espionage or other information operations. The target of SEA is therefore the information itself, which than can be exploited by the social engineer subsequently. The victim of such offences is the holder and/or owner of the information. The information holder is the person in possession of the information at a specific point in time and place. While often the information holder is simultaneously the owner of it, this is not a given fact. Social engineers that in direct communication target personal information of people victimize the information holder and owner at the same time. Differently, social engineers that acquire target information through the deception of, for instance, employees, can victimize the employee as information holder and the organization as the owner of the information. There is even a third victimization dimension, depending on the targeted type of information. In case the social engineer exploits customer or citizen information from an organization, the victims are the information holder, namely the employees and the organization, whereas the information owner, which is the customer, or the citizen, is also

victimized indirectly. Following these considerations and the approaches by Cohen and Felson (1980) and Clarke (1999), it derives the fact that a suitable target for SEA are information. They are characterized as being Accessible, Valuable and Exploitable – AVE. Target information are accessible through the deception of the information holder and/or owner. They have a specific value to the offender for either financial use or for the sake of the information itself. It has to be exploitable in the way that the offender can use it to derive advantages in financial or informational terms.

Table 8.3: Characteristics of information as a suitable target (own elaboration)

Characteristic	Definition
Accessible	The degree of acquiring the information through the information holder.
Valuable	The monetary or implicit value of the information.
Exploitable	The degree of making use of the information for financial or informational advantages.

The second layer of the triangle proposes the existence of controllers that have a crime preventive power. Controllers in the target dimension are guardians who can protect targets of being subject to an offence. The deceptive techniques of SE related offences imply a direct or indirect human interaction by the offender with the person possessing or owning the targeted information. The person who holds the information should either have a personal responsibility to protect the information under possession for the sake of information confidentiality in the interest of the information owner or should have a self-interest to protect the information, once her or she is also the owner of the information. The person that interacts with the social engineer either directly or indirectly, with or without the use of technology is therefore the person who guards the targeted information. Persons in possession of exploitable information are their guardians. This implies that a guardian is a human. Another basic characteristic that a guardian should reflect is that he or she is not deceivable, meaning resilient towards the manipulation by the social engineer. With the emergence of the internet and the feasible interconnection of everything and everybody, there actually does not exist any significant limitation in the geographical and temporal dimension for a motivated and capable social engineer to find persons in possession of exploitable information. The accessibility of those persons remains an important characteristic too, but rather has broadened with the online space. Capable guardians

are able to show a certain degree of inaccessibility. The manipulative deception techniques applied by social engineers use rationales of human psychology. Those rationales are so strong that once you are not aware of their existence, it is extremely difficult to not fall prey for them. Cialdini (1984) wrote a whole book about those techniques and how they are applied successfully to sell people goods without really thinking about the supposedly attractive offer. Guardians that are capable in protecting the target information reflect a certain degree of knowledge about those strategies and always look out for their application while safeguarding the information. They reflect a certain degree of susceptibility towards everybody and everything while acting deliberately and trust in themselves. Hence, in the regard of these theoretical considerations and in the course of this research study, capable guardians who prevent a SEA from being successful are **H**umans who are **I**naccessible to the social engineer, **K**nowledgeable about the threats of SE deception techniques, **A**ttentive in the communication with other people, **S**uspicious towards unusual requests by people they assumably know and people they do not know and finally they act with **C**onscientiousness and **C**onfidence – **HIKASc²**.

Table 8.4.: Characteristics of the guardian (own elaboration)

Characteristic	Definition
Human	The guardian is a human being
Inaccessible	The inability of a social engineer to access or approach the guardian.
Knowledgeable	The degree of knowledge of the guardian about SE and SE techniques.
Attentive	The ability to rightfully evaluate to whom and to whom not which kind of information can be communicated.
Suspicious	The ability to question the originality of requests from assumably known or unknown people.
Conscientiousness and confidence	The ability to work diligently and self-confident in handling information and in appearance.

The third layer of the proposed adapted RAT-model of Sampson et al. (2010) includes the existence of super-controllers. Super-controllers are supposed to apply incentives that motivate the controllers to fulfil their obligation of protecting the target. They therefore provide additional mechanisms to prevent crimes from happening. A capable super-controller who could effectively fulfil this role can be the government, by putting in place specific laws or regulations that would take in the duty of the guardians to protect the information. The law

enforcement that would provide effective criminal prosecution and deterrence of those guardians who do not comply. Obviously, those incentives would rather be misleading, as they would punish the guardian in his or her role for non-compliance. More effective super-controllers comprise in organizations and institutions that provide frameworks which enable the guardian to be more effective and reliable in his or her role as information guardian. Those frameworks can be of technological or human nature. Organizations and institutions can provide technological tools that help the guardian to better keep safe potential target information. Basic appliances could be VPN, encryption or simply a safe. However, they also can provide human tools that encourage guardians in their capability of protecting information. Organizations and institutions can provide security trainings or run awareness campaigns. However, even friends and relatives can act as super-controllers by providing human preventive measures, such as explaining to their loved ones the rationales of SE and highlight the significance of protecting important and confidential personal or organizational information from exploitative threats of social engineers. Both dimensions of super-controllers, the organizational and private dimension, obtain an important role in creating awareness and providing solutions among controllers that increase their capability and motivation in protecting information from the risks of SE related crimes.

Although this thesis mainly focuses on the components and dimensions described before, some considerations shall be given towards the remaining components, namely the place, the handler and manager, as well as their super-controllers.

The online sphere is an attractive spatiality for the offender and a highly likely place where the offender and the guardian could meet. This basically holds true, due to the fact that the online environment can easily be used as a means to approach guardians with its limitlessness in terms of geographical and temporal dimension, thus, increasing the scalability of fraudulent motivations. The offline environment does nevertheless reflect an attractive place to deceive people for the sake of monetary or informational purposes. False recruiting is sometimes used to gather intelligence on competitors or to scam innocent people and cases of fake police officers approaching citizens for financial gains are also part of the social engineer's tool kit and are reported (Stajano & Wilson, 2009; Krause, 2015; Doyle, 2020; KAPO Zürich, 2020; Tarun, 2020).

The handler dimension can have a direct impact on the social engineer in his or her doing when being motivated and capable as well. Typically, handlers are defined as people with whom the offender has an emotional attachment (Sampson et al., 2010). Thus, people that could

take on the position of refraining social engineers from their fraudulent activity could be, amongst others, parents, siblings, friends or supervisors, while latter might not always have an interest in deterring the social engineer, like in information operations of intelligence agencies.

Social engineers might also be deterred in their doing indirectly by managers. Managers are responsible for places and are their owners, or the owner's representative (Sampson et al., 2010). When considering an online or digital spatiality as crime place, then managers would consist of people or institutions controlling the environment, like telephone or internet provider, or companies of internet appliances. For the offline, analogous environment things are not that clear cut, as a place manager would be required to provide an intact environment that leaves no opportunity for a social engineer to communicate with a potential victim. This is difficult and probably only possible in sanitary crisis like the CoVid-19 pandemic, what leads us to the relevance of handler and manager super-controllers.

Super-controllers of handlers and managers in the regard of a SE crime would be institutions that provide the necessary conditions for them to act in accordance with the preferred status-quo. A status-quo where personal information, confidential and critical information of organisations, institutions, the providers of critical infrastructures or the government are safeguarded by supporting regulations and technologies. Super-controllers of handlers and managers therefore provide laws and technologies that assist them to either deter a social engineer from his or her doing or keep places in a condition that mitigate SE crimes.

In summary, this theoretical framework defines the components of the RAT-model presented by Sampson et al. (2010) applied to SE fraud. Each dimension and its components consist of a specific type and characteristic. The remainder of this thesis focuses on the interrelation among the offender, the target and the crime preventive components of the guardian and super-controller. Table 8.5 illustrates the different dimensions and its components, whereas the highlighted terms were subject to the empirical part of this dissertation.

Table 8.5: Components of RAT for SE fraud and definitions

Layer 1	Definition	Layer 2	Definition	Layer 3	Definition
Offender	Social engineer	Handler	Parents, friends, siblings, etc.	Super-controller	Government
Target	Information	Guardian	Information holder/owner	Super-controller	Friends, relatives, organizations, institutions
Place	Online/offline	Manager	Internet or telephone provider, internet companies, etc.	Super-controller	Government

The triangle also reflects the substantial considerations by Cohen and Felson that for the criminal act to occur, it is not only necessary to have this convergence in space and time, but also the particular importance that the actors reflect the specific characteristics discussed above. First, for a criminal act to occur, an offender is required to be motivated, thus having some pronounced intention, to look for a victim and perform an offence. The motivation to look for SE opportunities and identifying potential victims could be defined by the combination of seeking situational and individual factors presented by the potential victim, which then can be exploited in the course of a SEA. A motivated offender is on the search for situations, induced by the behaviour of the potential victim, and individual characteristics of the potential victim that reflect an attractiveness for carrying out the criminal act and that are exploitable in a way that the act will have a promising likelihood of success. In the case of financially motivated SE, however, the sole existence of intentions and the search for exploitable situational as well as individual factors does not put the criminal in a position to eventually commit a crime. For a SE related crime, it is of essential importance for a motivated offender to possess deceptive skills. Being capable of deceiving and manipulating a person psychologically in a way that the victim discloses the targeted valuable information or assets, is the main capability of a social engineer (Mitnick & Simon, 2002). Along with this come other skills that are necessary to

perform or support his/her SEA. A motivated social engineer additionally needs to have research and analysis skills for preparing the attack and gathering intelligence on the victim. Amongst others, the offender must have good IT skills and be capable to operate technical applications.

Second, to be of interest for a motivated and capable social engineer, a targeted information must be suitable and has to promise the expected added value for the offender in terms of financial reward or for the informational value of the target information itself. This is an important feature of the RAT for SE, as the target and victim dimension are not the same in this case. Whereas the victim is a person, the eventual target is an information. However, both have to reflect a certain degree of suitability to the offender for an offence to eventually take place.

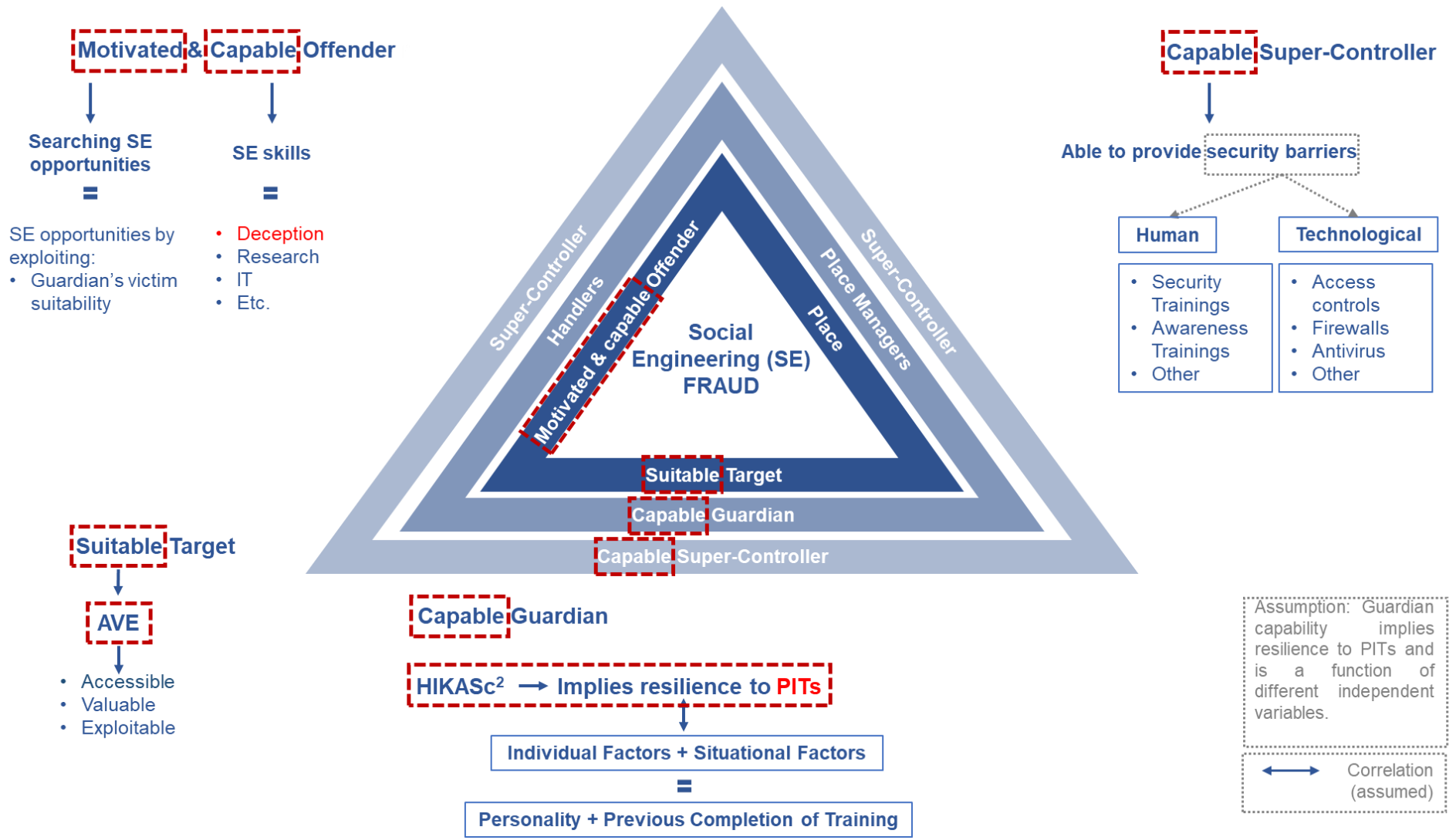
Third, to become victimised for a SE related criminal act, I assume that one must reflect a respective degree of not being able to guard relevant information in terms of the characteristics defined by the derived HIKASc² rationale above. This victim suitability of a guardian for a SEA is defined by specific individual patterns of personality that make him/her prone to such types of offence including specific attitudes, behaviours or routines on the one hand. Individual personality patterns drive the degree of proneness or acceptance towards the PIT and therefore are assumed to make the potential victim more or less prone to the offence of the motivated and capable social engineer. On the other hand, the guardian's suitability as a victim is also defined by situational or environmental factors, such as whether the respective person received specific trainings or whether in this specific situation security controls are in place that would make it harder for the social engineer to perform a successful attack and simultaneously would decrease the guardian's suitability. According to the literature, SE generally relies on the victim being successfully deceived by the application of the PIT (Ferreira et al., 2015; Bullée & Junger, 2020). I argue that the proneness to PIT is not the only driver that defines the guardian's suitability as victim. Victim suitability is rather defined by the set of different aspects mentioned above. Although someone might be dispositioned to PIT to a greater extent than someone else, the person could nonetheless be less suitable and hence less prone to a SEA, as the person finds him-/herself in a situation where the previous individual personality disposition that would make the person more suitable to be victimised, is counteracted by security barriers. Those can be technological providing a more secure environment or they can be human based in the form of specific trainings that would elevate the person's awareness in a SE fraud scenario. Thus, someone who is more easily psychologically influenced, but who received tailored and focused

training, should presumably be less prone to PIT and less suitable to be victimised by social engineers. Therefore, the likelihood of becoming a suitable victim is not uniquely dependent on individual personality compositions, but also on factors that could change the outcome in a specific way, such as security barriers like the previous completion of focused security trainings. This consideration reflects the fact that the occurrence of a crime does not only rely solely on specific psychological conditions in either the offender or victim dimension but are also dependent on given situational factors (McGuire, 2004, p. 62 ff.).

Lastly, a super-controller will not be present to avoid the crime to occur or is not sufficiently capable to deter the crime. As SE is centred around the successful application of deception techniques by the offender, the capability of the super-controller to prevent a SE induced crime from happening can therefore be defined as being deception preventive and taking away the effectiveness from the deception technique. The super-controller will provide security barriers to perform this task. Those are twofold, as already stated above. Security barriers can be human or technological interventions. The super-controller can enable guardians to better protect themselves and their information by imposing security trainings or awareness campaigns or by formulating sanctions in case of stolen data, amongst others. Additionally, or in exchange the super-controller provides security barriers on the technological dimension, such as solutions of access control, firewalls, antivirus or other effective solutions, such as VPN, encryption or physical safes that would animate the guardian to protect valuable information. Ideally, defences against SE take on both dimensions of barriers in a multilevel approach to be as holistic as possible (Gragg, 2003; Saleem & Hammoudeh, 2020).

Figure 8.2 illustrates those considerations and shows the further induction process of the SE perspective implementation in the RAT framework:

Figure 8.2: The Routine Activity Theory triangle for social engineering (1/2)



The illustration of the RAT triangle and its application towards SE related crime already hints on the importance for this research study and the connecting points. But where is the connection made up, exactly? The terms highlighted in red provide a partial answer to this question. First, motivated and capable social engineers, with the use of deceptive techniques to perform their criminal act, exploit the victim's proneness, which itself is defined by individual and situational conditions reflected by the guardian. Deception techniques have been termed as compliance principles, influencing tactics or briefly PIT in the previous chapters. It is obvious that one factor for the likelihood of success in the offender's deceptive criminal act is the extent of a target's proneness to those PIT. What is interesting to know is whether there are individual patterns of personality traits that are more or less correlated with the proneness of the guardian. How do the different personality dimensions discussed earlier in this dissertation interfere with the proneness towards PIT? Moreover, are the impacts of personality traits stable with or without the application of trainings and is the extent of personality impact before and after the training the same? Hence, defining someone's victim suitability in terms of individual personality characteristics and appearance of a situational factor is of great importance for the possibility of SE risk mitigation while standing up to motivated and capable offenders.

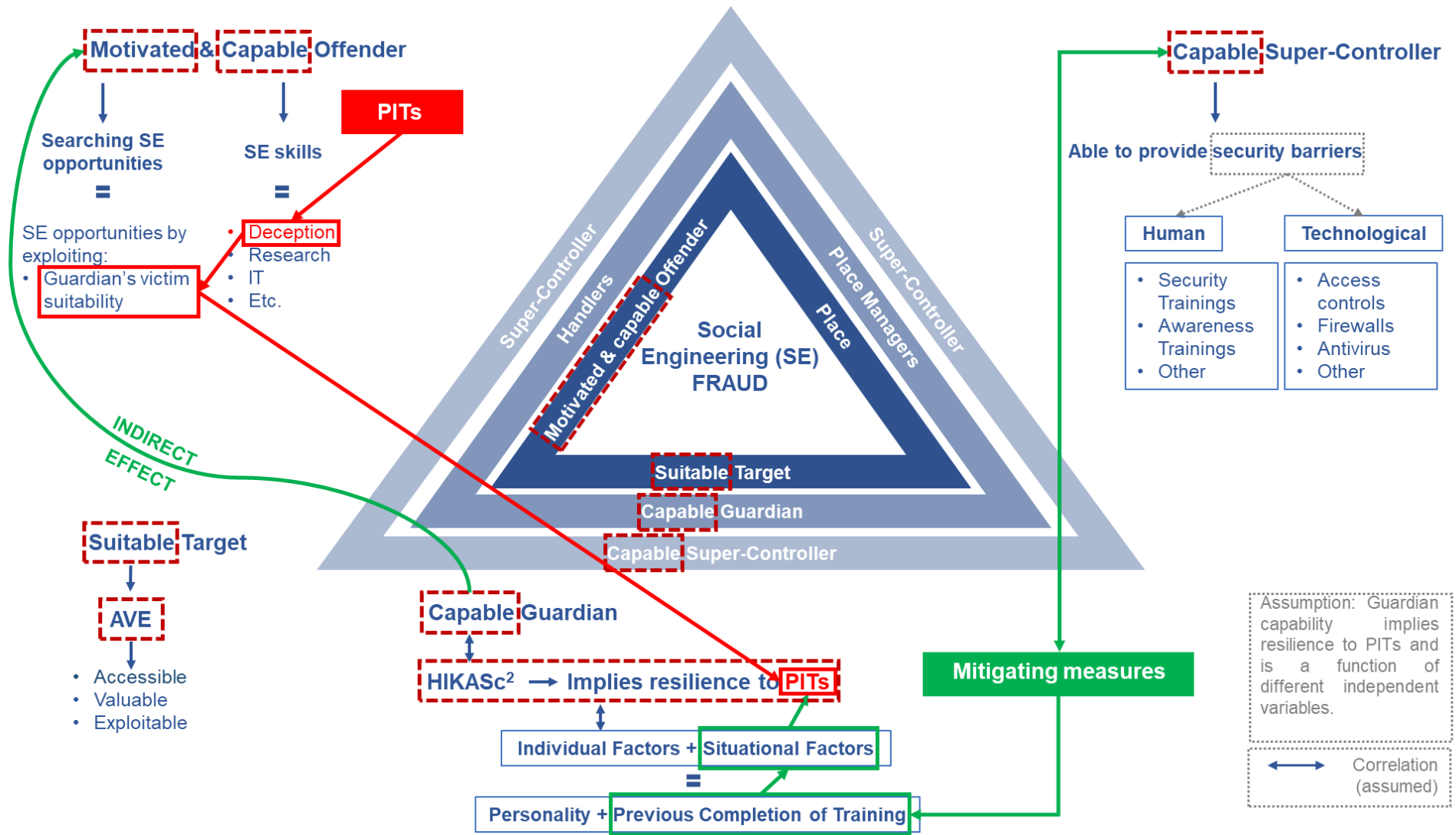
Second, the RAT triangle applied to the concept of SE related crime also provides the opportunity to derive and locate potential SE mitigation measures. Based on the proposed triangle for SE related crime, it seems obvious that there are three main connecting points to address possible SE mitigation measures. First, independent from specific measures taken at the offender or victim level, the pure absence of a capable super-controller provides a fruitful area to implement measures decreasing the likelihood of deceptive offences. In general, as defined earlier, super-controllers that are capable to prevent SE crimes can be organizations or institutions that induce barriers or incentivize the guardians. Similarly, employers do also possess the opportunity and, considering self-protection, the obligation to sensitise their employees about the threats. Thus, adding a layer of security to the human dimension. Nevertheless, companies can add a technological layer of security by developing, providing and applying technologies that are capable in preventing specific technology centred deceptive attacks. A super-controller in its capability to mitigate SE crimes either addresses the human dimension by awareness creation and knowledge transfer, both, the human and technological dimension (e.g. employees) by providing trainings to employees and applying security technology (access control, firewalls, antivirus, etc.) or the technological dimension only by developing technology that can be distributed and applied afterwards. This would not only

create positive effects on combatting SE related incidents in the company but would also have spill-over effects on the employee's handling of security issues in private life. Second, risk mitigation measures could be implemented in the offender-guardian interaction dimension. The triangle quite clearly proposes that the interaction between offender and guardian is driven by the guardian's proneness. Whereas the guardian makes him-/herself attractive to the offender, due to reflecting specific individual and situational patterns that drive their exploitable proneness, the offender him-/herself relies on those patterns that present to the offender potential opportunities to commit the SEA. Although the capability of forming and committing an attack is necessary, it is not sufficient in the absence of an appropriate opportunity. It is therefore indispensable to address these proneness patterns that arise from the guardian's individual and situational factors in order to mitigate SE crimes. Thus, taking away exploitable SE opportunities from the motivated offender. Moreover, addressing mitigating measures at the capability level of the offender seems to be much more difficult, if not impossible. Deterring individuals from using open sources to educate oneself about deceptive and malicious techniques or to perform research and gather intelligence about potential victims, is a defiance that would bear several restrictions. It would not only restrict all peaceful people in their legitimate freedoms or rights to self-determination, which in a democratic society is neither a preferred status-quo nor is it even possible, but it would also come in at tremendous economic costs to be borne. Handlers would be required to prohibit the potential social engineers from educating themselves in the respective techniques, what would come in with a tremendous effort in surveillance. The government as super-controller would need to restrict all people from using open-source material to educate oneself. The capability or SE skills of offenders is therefore not the right place to address SE mitigation measures. The place where such mitigation measures should be located instead is where the offender exploits the proneness of a victim. Shrinking the appearance of proneness patterns and thus decreasing the quantity of opportunities for motivated offenders to exploit situational and individual factors could be a promising approach for such a strategy. By finding ways to make a guardian less suitable for becoming a victim and more capable of being a guardian will also implicitly address the motivational dimension of the offender, as it will be harder for the social engineer to obtain the targeted information. Overall, different components of the triangle can be addressed with mitigating measures. On the offender dimension this happens rather indirectly by directly addressing mitigation measures on the guardian side for decreasing their proneness and thus negatively impacting the offender's motivation, as guardians become less suitable and more

capable, and it is more difficult for the offenders to succeed with their attack. On the super-controller side, SE mitigating measures would focus on the direct provision of human and technological tools to decrease the likelihood of a SE crime to occur. On the guardian dimension, mitigating measure obviously address either individual factors or situational factors or ideally both. For the individual dimension, namely the personality factors, that influence suitability, the identification of specific personality patterns that are more likely to reflect a risk of PIT proneness need to be identified. Once this is done, mitigating measures that address the specific risky personality expressions could be generated. The situational dimension is approached through the super-controller channel. Capable super-controllers provide the opportunity to impose trainings and inform guardians as potential victims about SE and provide specific regulations that could have a crime preventive effect. This can be the government, educational institutions, the law enforcement. Latter institutions are especially appropriate to provide a human security barrier in the form of trainings due to their institutional design and the hopefully preventive self-interest. The research study at hand pursued the approach to address the guardian and the super-controller side for mitigating measures with the beforementioned rationales.

Figure 8.3 illustrates the final considerations for the induction process of the SE perspective implementation in the RAT framework:

Figure 8.3: The Routine Activity Theory triangle for social engineering (2/2)



9. Discussion

9.1 Research findings

The empirical part of this dissertation had two main goals. First, it was of scientific interest whether individual personality traits impact the proneness towards SE fraud as well as victimization behaviour and attitudes. Second, the effectiveness of an interactive SG for SE was tested experimentally, as well.

First, the role of personality traits for falling prey to SE fraud was of specific interest to the researcher. Researchers looked at the importance of personality traits for predicting cybercrime victimization too (Alsedoon et al., 2015; Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017) Personality domains such as Extraversion and Openness are considered positively correlated with cybercrime victimization (Alsedoon et al., 2015; Van de Weijer & Leukfeldt, 2017). Other researchers also looked for the importance of personality traits in cybersecurity behaviour (Bossler & Holt, 2010; Uebelacker & Quiel, 2014; Shappie et al., 2019; Hadlington & Murphy, 2018). The research at hand did not directly find any strong statistically significant effect of personality traits on phishing test performances. Only the personality dimension Honesty-Humility showed to have a somewhat statistically significant positive impact on pre-test performance in a general classification model. People high on this personality dimension seem to be more likely to disclose information requested on a dedicated landing page after having clicked a link in a phishing email. This result follows other victimology research about the Honesty-Humility dimension that also found positive relationships. Moreover, random forest analysis indicates that personality traits form a group of observed variables that have an impact on the phishing performance that is more pronounced than the impact of other observed variables. Although this research cannot provide unambiguous insights on the definitive importance of personality traits, it does however indicate that there are interdependencies that might be worth studying in further research.

To the best of my knowledge, this is the first study that investigated on the role of HEXACO personality traits in relation to self-reported risky cybersecurity behaviour and self-reported attitudes towards cybercrime and cybersecurity, as measured by the RCsB and an adapted ATC-IB inventory first introduced by Hadlington (2017). However, there have been several other studies that researched the role of personality traits for cybersecurity behaviour and cybercrime victimization. Norris et al. (2019) performed a systematic review to take account of studies that dealt with the role of psychology and internet fraud victimization. Shappie et al. (2019) used

the Big5 inventory and a questionnaire to measure online security behaviour. They found that Conscientiousness, Openness and Agreeableness are statistically significant associated with self-reported cybersecurity behaviours. Similarly, Alseadoon (2015) found evidence of Extraversion being a valid predictor for compliance in phishing scams. Other researchers also found relevant evidence of an interdependence between cybercrime victimization and personality traits (Van de Weijer & Leukfeldt, 2017; Albladi & Weir, 2017). None of the presented studies used the HEXACO personality inventory to research possible interdependencies with risky cybersecurity behaviours. As the results of this research showed, the dimension Honesty-Humility does, however, seem to have a statistically significant impact on the self-reported cybersecurity behaviour of the study participants. Results suggest that reserve soldiers with a more honest and fairer personality and who have little temptation to break rules seems to show less risky behaviours in relation to cybersecurity, though with a relatively small impact. This finding is new and does broaden the knowledge about the H-dimension of the HEXACO personality traits and their importance for cybersecurity behaviour. Interestingly, the results of the experimental study showed that the H-dimension is a somewhat important predictor for study participants' failure in phishing scams, which is counterintuitive to the findings derived in the regard of the analysis with respect to RCsB but underlines that actual behaviour does not always go hand in hand with stated likely behaviour.

Additionally, this study used an adapted ATC-IB scale (Hadlington, 2017) with questions amended to reflect a military framework to investigate soldier self-reported attitudes towards cybercrime and cybersecurity and to evaluate the appropriateness of HEXACO personality traits as predictors for the scores on the inventory. The scale is relatively new and available literature respectively thin. Scholars used the inventory to investigate research questions about cybersecurity in different domains such as healthcare, education or water sector (Nunes et al., 2021; Antunes et al., 2021; Mufor et al., 2022), used it in a replication study (Aivazpour, 2019) or to look at relationships between cybersecurity knowledge and the ATC-IB (Roberts, 2021). Discussions about the results of this study in relation to other published literature can, at the point of writing, therefore not be performed. Linking HEXACO personality traits with the ATC-IB seems to be new. The results suggest that there is a statistically significant association among the Openness, Emotionality and Conscientiousness dimension of the inventory with reserve soldiers' attitudes towards cybercrime and cybersecurity. However, the expected effects seem to be weak. Reserve soldiers with higher self-control and lower impulsivity are expected to show a more favourable attitude towards cybercrime and

cybersecurity, which is in line with the hypothesized relationship. Openness is positively associated with the ATC-IB scale, meaning that more open reserve soldiers tend to show more favourable attitudes, which is contrary to the research hypothesis. This is similar to the results achieved for the dimension Emotionality, which shows a statistically significant association with the ATC-IB, but with direction of impact contrary to the one hypothesized. More empathetic people who have a pronounced fear of dangers are said to score high on this dimension, which would result in more compliant and favourable attitudes to security. Obviously, this view is not supported by the results of the research.

With respect to the second research goal, there were clear indications that – with the study design at hand, the respective sample of reserve soldiers and the experiment’s execution – the SG did not have any statistically significant effect on the proneness towards SE fraud victimization of experimental group participants compared to participants of the control group. Both study groups showed an improvement in the victimization rate from pre- to post-test scenarios that did not allow to draw conclusions about the effectiveness of the SG. Further statistical analysis showed that the overall sample size of the study might have been too small to derive valid conclusions about the effectiveness and that for a sample of three times the size, significant effects may have been observable. Apart from the sample size, other considerations could also explain the nonexistence of a measurable effect, such as methodological shortcomings or eventually an actual ineffectiveness of the game. As this study is the first that uses this specific SG approach with phishing test instruments, there is no possibility to directly compare the results with other studies for their reasonability and validity. There are however other studies that used phishing test instruments and other kinds of training interventions to test their appropriateness in reducing victimization. Bullée and Junger (2020) provide a meta-analysis of studies that used experimental designs to study the effect of SE interventions. There are indications that some of these trainings did somehow have an impact on the victimization rate of study participants, but others did not. Generally, laboratory studies reported larger statistically significant effects than field studies did. Moreover, randomization of participant and study group allocation did not have any statistically significant effect on the reduction of victimization. There is therefore some indication that effective training strategies exist. However, study environment, used test instruments and intervention approaches are however not comparable to the set-up of this dissertation. One should therefore be careful in drawing ultimate conclusions about the effectiveness of the SG used in this experimental research.

Next, the results suggest that variables that measure past victimization are a good indicator for predicting future victimization. Self-reported past victimization in terms of receiving phishing emails, as well as effective performance in phishing emails seems to be indicative for future victimization in the regard of this research. This follows research of other authors (Lauritsen & Davis Quinet, 1995; Schreck et al., 2006; Abdulai, 2020) who found that past victimization is an essential variable in predicting future victimization. Another interesting aspect of this research is the overall decreasing rate in victimization from pre- to post-test scenarios. Failing the second post-test did happen more often than failing the first post-test in the study group, but it was nevertheless lower compared to the pre-test. Learning effects concerning the way in which the tests were administered could be one possible explanation for this. Another explanation for the drastically decreasing victimization rate could be spill over effects within the study population. The study population is a community of reserve soldiers of the same battalion. Interpersonal communication upon receipt of the phishing email could have impacted the victimization rate. Those effects might not be favourable for creating and measuring any effect an intervention has on an experimental group. These spill-over effects could lead to a bias and could confound effects that the SG had on the experimental group but not on the control group. From an organizational perspective, a decreasing overall victimization rate is nevertheless a desired outcome. Finally, this thesis found that self-perception measured as a neutral self-perception towards individual victimization expectation in a phishing scam is a highly statistically significant and strong predictor for victimization. Indications of overconfidence were also found. Study participants who stated that they will unlikely become victims of a phishing scam show a weak statistically significant positive relation with actual victimization. Previous research has found ambiguous results in this regard. Different researchers (Kumaraguru, et al., 2007; Fischer et al., 2013; Hong et al., 2013) report that overconfidence is an essential risk factor for scam compliance and that awareness does not guarantee resilient behaviour. On the contrary, Cheng et al. (2020) even found positive relationship between overconfidence and susceptibility to phishing. The results of this thesis extend the literature in this regard with profound but weak evidence for the overconfidence phenomenon. Additionally, the results show strong and highly statistically significant indications for a – may we call it – indifferent phenomenon. People who perceive themselves neither likely nor unlikely to fall for a phishing scam reflect the group that is most likely at risk of becoming victim.

9.2 Obstacles and limitations

It took intensive and extensive planning to perform the experimental research of this study that took the researcher some nerves from preparation until finalization of the study. This is normal in empirical research and in particular in research involving other parties and human participants. It was therefore quite likely that the research at hand would – despite accurate and thorough planning – come along with administrative and methodological challenges that might be able to overcome or not or to be traded off. From an administrative perspective, the main challenges refer to ethical considerations, participant recruitment and availability throughout the study. Particular in research that involves human participants and the intended deception of the same, requires accurate planning and mutual agreements prior to conducting the research. For the study at hand, this was achieved by mutually discussing the conditions for the experiment with the legal department of the Swiss Armed Forces that resulted in an agreement among the parties. Other researchers report these necessary conditions too (Bullée, 2017). An essential condition for the experiment to take place was, however, the voluntary participation of the study participants. The hierarchical and commanding organizational structure of armed forces would in theory make it possible to order participation but was not pursued and granted for the study at hand. Participation was voluntary and opting-out possible. The resulting sample size was clearly impacted by this, as the theoretical sample size potential was unambiguously larger than the effective size of 180. As the results showed, this relatively small sample size might have been insufficient to derive more and better conclusions from the data. Moreover, the availability of the study participants throughout the experiment was limited by the organizational and administrative conditions any military environment presents. A major concern in this regard relates to the selection of experimental group participants by the commander of the battalion for the defined date of SG intervention. Selection criteria was the effective availability of the respective reserve soldier at the mutually defined intervention date. The size of the experimental group as well as its composition was therefore dependent on availability not on any random allocation strategy. It must be mentioned though that experimental group participants comprised soldiers of all different battalion troops that possess different functions. The variety of skill sets and personal characteristics that are required to fulfil these functions was therefore nevertheless given. Further, the battalion commander did not possess any insights on the pre-test results that could have led to a biased selection. Insights in pre-test results and experimental group participant selection was separated strictly. To put it differently, any impact a biased group allocation by the researcher could have had was

eliminated by the impossibility of the researcher to have any influence in this regard. Considering the research results by Bullée and Junger (2020), insufficient participant randomization does not reflect serious problems in terms of validity in experimental SE intervention research. Lastly, the probably most severe methodological limitation refers to the usage of the test instruments. There was no randomization of tests in the pre- and post-test stages. All study participants received the same phishing emails each of the pre- and post-test stages. Three different phishing scenarios were created by the researcher and sent to the responsible persons of the Swiss Armed Forces in the legal department and battalion before sending them for implementation to the vendor that administered the tests. The potential scenarios were limited and restricted by specific requirements, such as a chronological order that would make sense. Otherwise, study participants might have become suspicious right from the beginning. One crucial condition that is worth mentioning is the fact that the battalion, despite its size, is nevertheless a community of people that more or less know each other and communicate with each other. A scenario where the members of this community receive at the same time emails with different topics from the same organization, might have led to suspicion right at the beginning. Comrades would have had the possibility to question the authenticity of the mail and discuss it with one another. Sending the same scenario to each of the study participants at each test stage reflected therefore a congruent and more credible picture than a random assignment of the test scenarios. Credibility was thus traded against randomization. It is nevertheless needless to say that this impacts the validity of the test results, and it goes without saying that future studies should take account of this methodological shortcoming. However, Bullée and Junger (2020) also note that randomization did not play any statistically significant role in the analysis of other intervention studies of SE experiments. Whether the study was randomized, quasi-randomized or not randomized at all resulted in no statistically significant difference of intervention effects among the observed studies. The missing randomization in this study is a shortcoming but based on these findings, it is a limitation of lesser importance.

This study provided several insights on relationships of unexplored territory and although it broadens the literature, there are nevertheless key limitations. In particular, the results must not be taken as granted for a more heterogenous population. The generalizability is not only limited by the size of the sample, but also by its characteristics. It consisted of 100% male participants mainly in their 20s. Not only is this insufficient to draw any valid conclusions outside of a military setting, but it is also limited in its internal meaningfulness. Even in the

armed forces divisions and battalions perform diverse functions and that particularly consist of military personnel that was specifically recruited for either function. Moreover, IS does comprise diverse behaviours across diverse contexts that make other variables apart from personality traits important as well. Situational factors put another toll on the validity of the study. Not only might the situation in which study participants took the survey - that was taking place before their military service period - had an impact on their responses, but also does effective SE fraud and victimization behaviour depend on the specific situation and context as well. These factors might not have been fully and extensively respected in the study at hand.

9.3 Novelties and achievements

Despite the above-mentioned obstacles and methodological shortcomings, this dissertation did however present certain novelties and does add to the literature by providing a couple of considerations and insights that are new. First of all, it provides a discussion and a summary of different psychological rationales that are supposed to be essential requirements to deceive people for conducting SE fraud. Moreover, different tactics of how one possibly can protect against such manipulation techniques together with application examples are presented. Other researchers also discuss the importance of PIT for the success of SE fraud (Atkins, 2013; Ferreira et al., 2015; Bullée, 2017) in particular the Cialdini compliance principles. To the best of my knowledge, Ferreira (2015) is the only one that takes a similar approach but discusses different stances of psychological techniques that are meant to drive the success of SEA. The author analysed them and created a synopsis to come up with a summary of unique principles. In a similar vein, this dissertation also looked at the different approaches but comes up with a different summary as some of the rationales were analysed to be redundant or partly overlapping in addition to what Ferreira (2015) found. Moreover, this dissertation is, at the point of writing and to the best of my knowledge, the first that takes account of the seventh Cialdini compliance principle in the analysis for its application in SE fraud settings. The *Unity* principle is the newest achievement in Cialdini's (2021) research and presents a valid consideration for its application in SE fraud settings as well.

Second, this thesis presented a SG for SE as the operational framework for its empirical part. This approach was first introduced by German researchers Beckers and Pape (2016). In its original approach, they used a tabletop game to educate players about SE and its rationales. Further studies and researchers used this approach to test it or alter it for the application as a general cybersecurity training tool (Hart et al., 2020). In the regard of this dissertation, the initial game design of Beckers and Pape (2016) was used to be tested for improvements regarding its

content and structure. In qualitative research, Muhly et al. (2021) used field observations in a sample of totally 97 participants to derive improvement potentials in these dimensions. With these improvements the game stands out from the ones previously discussed. Eventually, the derived approach was applied in the empirical part of this dissertation.

Third, this dissertation reported about applied experimental field research. In a four staged experimental design, the SG approach was tested for its effectiveness to decrease individual proneness towards SE fraud, measured by email phishing behaviour. There are several aspects of this experimental research that make it novel and reflect, despite some methodological limitations, a thoughtful approach. First of all, it is the first experimental approach, to the best of my knowledge, that tests the SG for its effectiveness in a real-world setting with phishing tests. Aladawy et al. (2018) use the SG approach and test its usefulness to increase knowledge about SE of 27 university employees with pre and post surveys. Hart et al. (2020) used an alternate version of the game to test with 54 study participants the appropriateness of the game to transfer cybersecurity knowledge by using questionnaires. However, there does not exist so far, any research that eventually test the game's impact of players' effective behaviour in SE situations. Moreover, the field experiment of this dissertation was performed with a relatively large sample size. Whereas previous studies incorporated 27 participants (Aladawy et al., 2018) or 54 participants (Hart et al., 2020), the research at hand successfully recruited 180 participants. Nevertheless, this was quite likely too less to derive more reliable conclusions, as has been discussed before. Another achievement refers to the study's environment. A military setting for field research is on the one hand highly attractive for researching peoples' proneness towards SE due the military's system relevance and importance for national security but on the other hand is also an environment where it is difficult to recruit study participants and to implement specific research designs, while respecting regulations, procedures, and hierarchies. Finally, one major achievement of the research design at hand was its ability to track participants and their performances in the respective research stages throughout the whole experiment. Upon mutual agreement with the legal department of the Swiss Armed Forces, participant tracking by the researcher and by him alone was possible. This was a key accomplishment that not only allowed to allocate participants to either control or experimental group and to track their longitudinal performance in the phishing tests, but also to look for individual differences in terms of personality traits. The possibility of longitudinal, as well as inter- and intra-group comparison presents a major achievement from a methodological and research design perspective.

Fourth, the findings of the present study suggest that personality traits as measured by the HEXACO personality inventory are partly associated with risky cybersecurity behaviours and attitudes towards cybercrime and cybersecurity, as measured by the RCsB and ATC-IB inventories, in a sample of Swiss reserve soldiers. In particular, the Honesty-Humility dimensions seems to possess predictive relevance for participants' risky cybersecurity behaviour. Conscientiousness, Emotionality and Openness are statistically significant associated with participants' attitudes towards cybercrime and cybersecurity too. These findings are important to the Swiss Armed Forces for their internal cybersecurity training approaches, in the evaluation of future soldiers in the recruitment stage and for the military command for their organizational aspirations. This research is, to the best of my knowledge, the first that combined the HEXACO personality inventory with the RCsB and ATC-IB inventories to look for evidence that personality traits might predict cybersecurity behaviour and attitudes. Additionally, it is the first that does so in a military set-up at the time of writing, which is a significant achievement. On the one hand, field research in organization outside the university environment is challenging and on the other hand, it comes along with issues of confidentiality. This said, the mere willingness of cooperation and completion of the study might be considered a success. However, it also comes along with limitations to validity. Military personnel possess huge responsibility for national security in times of peace and in particular in times of war. The digitalization of society also bears severe challenges for the security of military information and operability. Soldiers that demonstrate desired behaviour and attitudes towards cybersecurity and cybercrime are therefore a key to maintain national security and organizational information security likewise. This research provided indications on what type of soldiers are more dispositioned to do so. However, the limited sample size and its rather homogenous characteristics in terms of demographics restrict the generalizability of the findings to a wider public. Future research should therefore aim to generate larger insights into the relationship between HEXACO personality traits and cybersecurity behaviours and attitudes.

Fifth, this dissertation built a theoretical framework for SE fraud. The RAT framework and its advancement over time (Cohen & Felson, 1979) was presented and its application as a theoretical framework for SE fraud was discussed. Based on the most current RAT framework with three layers (Sampson et al., 2010), a theory for its application in SE fraud settings was elaborated and presented in chapter 8 of this dissertation. There are different researchers that discuss the RAT framework for fraud and for SE (Hutchings & Hayes, 2009; Leukfedt, 2014;

Glasser et al., 2015; Jansen van Rensburg, 2018; Danquah et al., 2020; Steinmetz, 2021). Further to these studies, the approach presented in this dissertation largens the still sparse literature on the topic and provides additional fresh thoughts. This is clearly an achievement of this dissertation at the point of writing.

Lastly, this thesis found that self-perception measured as the individual victimization expectation in a phishing scam is a highly statistically significant and strong predictor for victimization. The experimental part of this dissertation has found that study participants who reported that they themselves find it neither likely nor unlikely to fall for a scam within the next 12 months were the ones with the highest probability to eventually fall for it. They were about four times as vulnerable, as those who said that they will likely become victim of a scam in the next 12 months. Self-confident people often lack a critical self-reflection and possess a self-concept that lacks to correctly align self-perceived future likely behaviour with actual future behaviour. This is an important finding that was beyond the researcher's radar, but that might path the way for future research aspirations. An observed U-shaped relationship among one's own capability of spotting and resisting phishing scams and eventual victimization is a key finding that is worth looking at in future studies. Approaches that put the spotlight on personality characteristics like self-confidence could be helpful in tackling human proneness to social engineering fraud. Such considerations might even be more promising than looking at specific training approaches. In case we can separate people in terms of their degree of confidence in their own capabilities as indicator of proneness to fraud prior to conducting information security trainings, this would provide an efficient way in achieving resilience against this kind of attacks. People could be categorized by their degree of confidence as indicator for their proneness towards social engineering fraud. This would help practitioners to focus their information security trainings on the people who need it most.

9.4 The Way Ahead

There are different open research directions stemming from this dissertation that future research could address. First, future research should follow-up the experimental design of this study with larger sample sizes and minor improvements in the methodological approach in order to look for more evidence of SG effectiveness and whether personality traits play a significant role in SE victimization. This said, a pronounced focus shall be on the recruitment of a sufficient number of study participants. Future research should aim to generate larger insights into the usefulness of the SG as driving resilient behaviour against SE fraud. Another interesting question that at this point is out of the scope of this thesis, is the question of whether different methods of conveying content and knowledge to people impacts their proneness towards SE deception rationales. Does an online administered training tool, like a webinar or an online presentation, have the same, better or worse impact on an individual's proneness towards SE deception rationales than an offline administered tool, such as a SG? The CoVid-19 pandemic has forced not only corporations to more virtual communication, but also education organizations to transfer their programmes from the classroom to the virtual screen. Answering the question above in future research might also give answers on the performance of an online tool in conveying concepts and rationales compared to an offline tool like the serious game subject to this thesis. Second, the results of this research suggest that it is worth to investigate more on the role of self-perceived victimization likelihood in relation to eventual victimization. It seems that people with a pronounced self-confidence for not falling for a scam are the ones most at risk to eventually fall for a phishing scam. More research should look at this relationship to confirm these results in a broader and more diverse study population. Third, phishing victimization presents only an excerpt of SE fraud variety. Other types of SE fraud, such as telephone or personal based approaches are worth to be tested in this regard too. Fourth, future research could pick up the considerations derived in the theoretical framework of this thesis and further discuss the application of the controller and super-controller layer triangles of the offender and place dimensions and its interrelations. Fifth, the relationship between HEXACO personality traits and cybersecurity behaviours and attitudes is worth studying more extensively. Finally, we should take account of the conscious bias. A critical mass of people overestimates their resilience and underestimates their victimization likelihood.

10. Conclusion

More than three thousand years have passed since Trojans have been successfully lured into giving their opponents access to their most valuable assets and belongings by falling prey to the principle of reciprocity. Desirable values, belongings and assets, as well as the means of war – some would say – have changed since then. What has not changed though is human psychology and its rationales in social encounters. Principles that are deeply rooted within history of society and influenced by one's growing up and parenting drive behaviour in certain situations. From supposedly well-thought through decisions when purchasing highly attractive goods to clicking supposedly harmless links in emails that were sent by someone you think you know or met some time in the past, the rationales behind those strategies that let you open your pocket, or your virtual front door are the same. For sure, the accompanying tools and means to propose you these decision-making situations vary in scope, scale and technical intensity. But in the end, it is you that takes a decision based on rationales that are deeply rooted in you as a human being.

Whereas in the previous examples the former one refers to intelligent marketing, the latter one is considered as social engineering fraud. This thesis and the associated research aimed to shed more light on the interplay between SE and factors that make people more resilient against those malicious threats. SE victimization is something highly important for today's society. According to Verizon (2022), almost 82% of successful cyberattack incorporate a human element that in one way or the other can be classified as manipulating humans with psychological means. In the course of this thesis, you got to know the different psychological rationales that make SE so successful. In an analysis of available approaches that are said to be used as manipulation strategies in SE, commonalities and differences were analysed and a summary of 13 unique principles proposed.

The thesis took on this direction and you were presented a serious gaming approach to educate people about the threats and rationales of SE. Although SG exist since a couple of decades, the one presented in this thesis specifically focuses on SE. An original approach of German researchers Beckers and Pape (2016) was evaluated and improved in several aspects of its content and proceeding before being empirically tested for its effectiveness in a sample of 180 Swiss reserve soldiers in an experimental research design. With pre- and post-test phishing email the effect of the participation in the SG was measured. There was no evidence that would support a decision to accept the research hypothesis that a participation in the

interactive SE serious game reduces the proneness towards phishing SE fraud. However, an additional analysis showed that previous victimization, measured by failing the pre-test, is a good and statistically significant predictor of future victimization, which is the performance in the two post-test scenarios. The research at hand did not directly find any strong statistically significant effect of personality traits on phishing test performances. Only the personality dimension Honesty-Humility showed to have a somewhat statistically significant positive impact on pre-test performance in a general classification model. Further, only participation in previous security training had a weakly significant effect, reducing the odds of failing by about half. However, there were other interesting results derived in the analysis. Most importantly, longitudinal victimization indicators are a strong predictor. Not only does past victimization predict future victimization, but in this regard somewhat logically does current victimization, as measured by the post-test, also indicate past victimization. Similarly, self-reported past victimization is a good predictor too. On the contrary, prior participation in an information security training that dealt with military related information has a statistically significant somewhat positive impact on the victimization in the pre-test. Interestingly, the strongest predictors in terms of estimated coefficient refer to the self-reported individual victimization expectation. An indifference towards the likely future victimization seems to be the predictor with the strongest impact on future victimization, followed by the indicator that reflects a self-reported unlikely future victimization. This is evidence that self-perceived resilience does not predict resilient future desired behaviour. On the contrary, it predicts future undesired behaviour resulting in victimization. Among the 180 study participants, 170 stated that they will not become victim within the next 12 months, whereas of them almost 56% eventually fell for such a scam only about four weeks later. Lastly, there is somewhat statistically significant evidence that the personality dimension Honest-Humility is a good predictor for the proneness towards SE phishing, at least for providing information on a landing page in the second stage of the pre-test phishing email. People who score high on this dimension, thus having a more pro-social altruistic mindset, have a higher chance of failing. Further analysis with decision trees showed that extreme values for the assessment of risky cyber security behaviour can also be an indicator for failing respectively passing the tests. A random forest analysis further showed that time, measured as past and current victimization, is the most important predictor. HEXACO personality traits as well as RCsB and ATC-IB variables form a cluster of somewhat important predictive variables. Variables that reflect participation previous security trainings or in the SG seem to not provide any contribution as predictor. One of the most important findings for this

but also for future research dealing with the instruments that were used in this study relates to the size of the sample. The results of these analyses suggest that three to five times or about 350 to 500 participants would have been necessary for the study to report significant findings about the effect of participation in the SG. Given the organizational and administrative constraints that came along with a field experiment in the armed forces, this was unfortunately not possible at the time when the study was conducted.

You were presented results of research that put HEXACO personality traits in relation with risky cybersecurity behaviour and attitudes towards cybercrime and cybersecurity of the reserve soldiers in the research sample. The findings of the present study suggest that there is a significant association among several of these variables. In particular, the Honesty-Humility dimensions seems to possess predictive relevance for participants' risky cybersecurity behaviour. Conscientiousness, Emotionality and Openness are statistically significant associated with participants' attitudes towards cybercrime and cybersecurity too. These findings are important to the Swiss Armed Forces for their internal cybersecurity training approaches, in the evaluation of future soldiers in the recruitment stage and for the military command for their organizational aspirations.

Further, you were introduced theoretical considerations that applied a routine activity theory approach to SE fraud. In this novel approach, proceedings of a typical SEA were analysed and the different layers of the RAT triangle were mapped with the actors that typically would be present in such an attack. The novelty of this approach is that potential mitigating measures and necessary conditions against SE fraud were catalysed in the course of the theory construction. It is the guardian who is the possessor of information that are evaluated suitable by the offender to satisfy his or her malicious motivations. It is therefore the guardian that is likely to be victimized by offenders during their malicious campaign. Apart from specific individual factors, such as personality, there are situational factors that drive resilience towards SE. Specific security trainings can act as a risk mitigation measure that prepare guardians for being resilient.

This research is, to the best of my knowledge, the first that combined the HEXACO personality inventory with the RCsB and ATC-IB inventories to look for evidence that personality traits might predict cybersecurity behaviour and attitudes. Additionally, it is the first that does so in a military set-up at the time of writing, which is a significant achievement. On the one hand, field research in organization outside the university environment is challenging

and on the other hand, it comes along with issues of confidentiality. This said, the mere willingness of cooperation and completion of the study might be considered a success. Moreover, it is the first that used a four staged experimental design to test the effectiveness of a SG against SE in a field experiment with soldiers. Although there was no direct evidence of the appropriateness of the SG to decrease participants' proneness towards SE fraud in phishing emails, it should nevertheless encourage other researchers to pursue similar approaches with a larger population size and with some essential improvements in the methodology if possible, considering the potential constraints in experimental field research with third or fourth parties involved.

Military personnel possess huge responsibility for national security in times of peace and in particular in times of war. The digitalization of society also bears severe challenges for the security of military information and the organization's operability. Soldiers that demonstrate desired behaviour and attitudes towards cybersecurity and cybercrime are therefore a key to maintain national security and organizational information security likewise. This research provided indications on what type of soldiers are more dispositioned to do so. Moreover, this research also provided a proposal of a training to educate soldiers about the threats and rationales of SE and evaluated it for its possible effectiveness in initiating resilient behaviour towards SE fraud approaches. Whereas some relevant results for the role of personality traits in SE and cyber victimization were found, future research needs to further address the effectiveness of the SG training.

So what is the final conclusion then? Let us hope that the nonexistence of a desired positive statistically significant effect of a participation in the SG is just stationary and limited to the findings of this study. It might be a sorrowful consideration when these findings would be universal. The three-thousand-year lasting history of Trojan horses does however show that – at least for certain people and with maybe specific characteristics – there will not be the ultimate saviour.

In this sense, I would like to close this dissertation with a citation of a Nobel laureate that might bring some hope, if one finds the magic wand:

«What would I eliminate if I had a magic wand? Overconfidence!»

Daniel Kahnemann
Psychologist, Nobel Laureate in Economics

11. Reference List

- Abdulai, M. A. (2020). *Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud*. *International Journal of Cyber Criminology*, 14(1), 157-174.
- Abraham, S., & Chengalur-Smith, I. (2010). *An overview of social engineering malware: Trends, tactics, and implications*. *Technology in Society*, 32(3), 183-196.
- Abt Associates (2020). *Biography of Clark C. Abt*. Retrieved January 6, 2020, from <https://www.abtassociates.com/who-we-are/our-people/clark-c-abt-phd>.
- Abt, C.C. (1970). *Serious Games*. University Press of America.
- Aburrous, M., Hossain, M.A., Dahal, K., & Thabtah, F. (2010). *Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies*. Springer Science+Business Media, LLC 2010: *Cogn Comput* (2010) 2:242–253; DOI 10.1007/s12559-010-9042-7.
- Adams, M., & Makramalla, M. (2015). *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach*. *Technology Innovation Management Review* January 2015.
- Adler A. (1930) *Individual Psychology*. In: Murchison, C. (Ed.). (1930). *International university series in psychology. Psychologies of 1930*. Clark University Press. <https://doi.org/10.1037/11017-000>.
- Adler, A. (1961) *The practice and Theory of Individual Psychology*. In: Shipley, T. (Ed.). (1961). *Classics in psychology*. Philosophical Library.
- Agresti, A. (2003). *Categorical data analysis*. John Wiley & Sons. 2nd edition, 410-411.
- Aitkenhead, M. J. (2008). *A co-evolving decision tree classification method*. *Expert Systems with Applications*, 34(1), 18-25.
- Akhgar, B., Redhead, A., Davey, S., & Saunders, J. (2019). *Introduction: Serious Games for Law Enforcement Agencies*. In: Akhgar B. (eds) *Serious Games for Enhancing Law Enforcement Agencies*. Security Informatics and Law Enforcement. Springer, Cham.
- Aladawy, D., Beckers, K., & Pape, S. (2018). *PERSUADED: Fighting Social Engineering Attacks with a Serious Game*. In: Furnell S., Mouratidis H., Pernul G. (eds) *Trust, Privacy and Security in Digital Business*. TrustBus 2018. *Lecture Notes in Computer Science*, vol 11033. Springer, Cham.
- Alalehto, T., & Azarian, R. (2018). *When white collar criminals turn to fatal violence: The impact of narcissism and psychopathy*. *Journal of investigative psychology and offender profiling*, 15(2), 215-226.
- Albladi, S. M., & Weir, G. R. (2017). *Personality traits and cyber-attack victimisation: Multiple mediation analysis*. In 2017 *Internet of Things Business Models, Users, and Networks* (pp. 1-6). IEEE.

- Aldawood, H., & Skinner, G. (2018). *Educating and raising awareness on cyber security social engineering: A literature review*. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) (pp. 62-68). IEEE.
- Algarni, A., Xu, Y., & Chan, T. (2014). *Social engineering in social networking sites: The art of impersonation*. In 2014 IEEE International Conference on Services Computing (pp. 797-804). IEEE.
- Allport, G. W., & Odbert, H. S. (1936). *Trait names: A psycholexical study*. Psychological Monographs, 47, 211.
- Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). *What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?* In Advanced Computer and Communication Engineering Technology (pp. 949-962). Springer, Cham.
- Altaher, A. (2017). *Phishing websites classification using hybrid SVM and KNN approach*. International Journal of Advanced Computer Science and Applications, 8(6), 90-95.
- Amin, R., Ryan, J., & van Dorp, J. (2011). *Detecting targeted malicious email*. IEEE Security & Privacy, 10(3), 64-71.
- Amineddoleh, L. A. (2016). *Are you faux real: An examination of art forgery and the legal tools protecting art collectors*. Cardozo Arts & Ent. LJ, 34, 59.
- Amir, M. (1971). *Patterns in forcible rape*. Chicago, IL: University of Chicago Press.
- Anderson, E. (1999). *Code of the street: Decency, violence, and the moral life of the inner city*. New York, NY: WW Norton & Company.
- Annisette, L. E., & Lafreniere, K. D. (2017). *Social media, texting, and personality: A test of the shallowing hypothesis*. Personality and Individual Differences, 115, 154-158.
- Antunes, M., Silva, C., & Marques, F. (2021). *An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context*. Applied Sciences, 11(23), 11269.
- Arcos, R., & Lahnemann, W.J. (2019). *The Art of Intelligence. More Simulations, Exercises and Games*. Security and Professional Intelligence Education Series (SPIES). Series Editor: Jan Goldman. The Rowman & Littlefield Publishing Group, Inc.
- Ares, C. E., Rankin, A., & Sturz, H. (1963). *The manhattan bail project: An interim report on the use of pre-trial parole*. New York University Law Review, 38(1), 67-95.
- Ariel, B. (2012). *Deterrence and moral persuasion effects on corporate tax compliance: findings from a randomized controlled trial*. Criminology, 50(1), 27-69.
- Armerding, T. (2018). *Lance Spitzner: How To Secure The Human Operating System*. In: FORBES, 18. October 2018. <https://www.forbes.com/sites/taylorarmerding/2018/10/16/lance-spitzner-how-to-secure-the-human-operating-system/#d91d79fed599>.
- Ashton, M. C., & Lee, K. (2007). *Empirical, theoretical, and practical advantages of the HEXACO model of personality structure*. Personality and Social Psychological Review, 11, 150-166.
- Ashton, M. C., & Lee, K. (2009). *The HEXACO-60: A short measure of the major dimensions of personality*. Journal of personality assessment, 91(4), 340-345.

- Atkins, B., & Huang, W. (2013). *A Study of Social Engineering in Online Frauds*. Open Journal of Social Sciences 2013. Vol.1, No.3, 23-32. Published Online August 2013 in SciRes (<http://www.scirp.org/journal/jss>).
- Aviv, S. S. (2019). *An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals*.
- Bailey, C. D. (2017). *Psychopathy and accounting students' attitudes towards unethical professional practices*. Journal of Accounting Education, 41, 15-32.
- Barber, R. (2001). *Social engineering: A People Problem?* Network Security, 2001, Vol.2001(7), pp.9-11.
- Barker, K. J., D'amato, J., & Sheridan, P. (2008). *Credit card fraud: awareness and prevention*. Journal of financial crime.
- Barnes, D. S. (2006). *A defense-in-depth approach to phishing*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.
- Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). *Fraud detection in telecommunications: History and lessons learned*. Technometrics, 52(1), 20-33.
- Beckers, K., & Pape, S. (2016). *A Serious Game for Eliciting Social Engineering Security Requirements*. 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, 2016, pp. 16-25.
- Ben Simon, O. (2009). *Demystifying the advance-fee fraud criminal network*. African Security Studies, 18(4), 5-18.
- Berg, M. T., Stewart, E. A., Schreck, C. J., & Simons, R. L. (2012). *The victim-offender overlap in context: Examining the role of neighbourhood street culture*. Criminology, 50, 359–390.
- Bergmann, J. D. (1969). *The Original Confidence Man*. American Quarterly, 21(3), 560–577. <https://doi.org/10.2307/2711934>.
- Bertrand, M., Duflo, E., & Mullainathan, S. (2004). *How much should we trust differences-in-differences estimates?* The Quarterly journal of economics, 119(1), 249-275.
- BinSubaih, A., Maddock, S., & Romano, D. (2009). *Serious games for the police: Opportunities and challenges*. Dubai, UAE: Dubai Police Academy Research & Studies Center.
- BKA (2020). *Enkeltrick: Betrug am Telefon mit neuer Masche*. Bundeskriminalamt, BKA, 17th March 2020. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200317_CoronaEnkeltrick.html.
- BKA (2020). *Achtung: Bundesweite Phishing-Welle im Zusammenhang mit der COVID19-Pandemie*. Bundeskriminalamt, BKA, 7th May 2020. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200507_Coronaphishing.html.
- Blass, B. (2017). *Bei Anruf Geld weg*. DFZ 61, 54–55 (2017). <https://doi.org/10.1007/s12614-017-7097-5>.
- Boehm, J., Kaplan, J., & Sportsman, N. (2020). *Cybersecurity's dual mission during the coronavirus crisis*. McKinsey Insights.

- Bossler, A. M., & Holt, T. J. (2010). *The effect of self-control on victimization in the cyberworld*. *Journal of Criminal Justice*, 38(3), 227-236. DOI: <https://doi.org/10.1016/j.jcrimjus.2010.03.001>.
- Böck, B., Klemen, M.D. and Weippl, E.R. (2007). *Social Engineering*. In Handbook of Computer Networks, H. Bidgoli (Ed.). <https://doi.org/10.1002/9781118256107.ch25>.
- Brownmiller, S. (1975). *Against our will: Men, women and rape*. New York, NY: Open Road Media.
- Breiman, L. (2001). *Random forests*. *Machine Learning*, 45 (1), 5–32.
- Britt, C.L., Weisburd, D. (2010). *Statistical Power*. In: Piquero, A., Weisburd, D. (eds) *Handbook of Quantitative Criminology*. Springer, New York, NY. https://doi.org/10.1007/978-0-387-77650-7_16
- Bruzzone, A., Tremori, A., & Massei, M. (2009). *Serious games for training and education on defense against terrorism*. Italy: Defense Technical Information Center.
- Buchanan T, Whitty MT (2014). *The online dating romance scam: causes and consequences of victimhood*. *Psychol Crime Law* 20(3):261–283.
- Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). *Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK*. *European Societies*, 23(sup1), S47-S59.
- Bullée, J.W.H., Montoya, L., Pieters, W., Junger, M., & Hartel, P.H. (2015). *The persuasion and security awareness experiment: reducing the success of social engineering attacks*. Springer Science+Business Media Dordrecht 2015. *J Exp Criminol*: DOI 10.1007/s11292-014-9222-7.
- Bullée, J.W.H., Montoya, L., Junger, M., & Hartel, P. (2016). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention*. *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016 A*. Mathur and A. Roychoudhury (Eds.).
- Bullée, J.W.H., Montoya, L., Junger, M., & Hartel, P. (2017). *Spear phishing in organisations explained*. *Information & Computer Security*, Vol. 25 Issue: 5, pp.593-613, <https://doi.org/10.1108/ICS-03-2017-0009>.
- Bullée, J.W.H. (2017). *Experimental Social Engineering Investigation & Prevention*. University of Twente.
- Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P.H. (2017). *On the anatomy of social engineering attacks - A literature-based dissection of successful attacks*. *Journal of Investigative Psychology and Offender Profiling*, 2018, pp.urn:issn:1544-4759.
- Bullée, J. W., & Junger, M. (2020). *Social Engineering*. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 849-875.
- Bullee, J. W., & Junger, M. (2020). *How effective are social engineering interventions? A meta-analysis*. *Information & Computer Security*.
- Burger, J. M. (2008). *Personality (7th ed.)*. Belmont, CA: Wadsworth Cengage.
- Burkett, R. (2013). *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*.

- Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). *Breaching the human firewall: Social engineering in phishing and spear-phishing emails*. arXiv preprint arXiv:1606.00887.
- Carré, J. R., Jones, D. N., & Mueller, S. M. (2020). *Perceiving opportunities for legal and illegal profit: Machiavellianism and the Dark Triad*. *Personality and Individual Differences*, 162, 109942.
- Cattell, R. B. (1946). *Description and measurement of personality*. World Book Company.
- Cattell, R. B. (1957). *Personality and motivation structure and measurement*. World Book Co..
- Cendrowski, H. & Petro, L.W. (2012). *History of Fraud Deterrence*. In *The Handbook of Fraud Deterrence* (eds H. Cendrowski, J. Martin and L. Petro). <https://doi.org/10.1002/9781119202165.ch3>
- Chen, G., Zhou, G., Mao, Z., Liu, Q., Zheng, Z., Chen, G., & Qin, P. (2015). *Research of Social Engineering Attacks in Telecommunications Fraud*. In 2015 International Conference on Social Science, Education Management and Sports Education (pp. 1869-1872). Atlantis Press.
- CHEN, G., DING, L., CHEN, G., ZHOU, G., & LIU, Q. (2016). *Research on the Vital Non-Technical Factor in Telecommunications Fraud: Social Engineering*. DEStech Transactions on Social Science, Education and Human Science, (hsc).
- Cheng, C., Chan, L., & Chaur, C.I. (2020). *Individual differences in susceptibility to cybercrime victimization and its psychological aftermath*. *Computers in Human Behavior* 108 (2020) 106311.
- Chihara, L. M., & Hesterberg, T. C. (2022). *Mathematical statistics with resampling and R*. John Wiley & Sons.
- Cho, J.H., Cam, H., & Oltramari, A. (2016). *Effect of personality traits on trust and risk to phishing vulnerability: modeling and analysis*. Presented at the Proceedings of the IEEE CogSIMA 2016 International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, San Diego, CA, (pp. 7–13).
- Choi, K., Leeb, J-l., & Chunb, Y-t. (2015). *Voice phishing fraud and its modus operandi*. *Security Journal* (2017) 30, 454–466. doi:10.1057/sj.2014.49.
- Choo, X.M., Chiew, Kang Leng, Ibrahim, D.H.A., Musa, N., Sze, S.N. & Tiong, W.K.. (2016). *Feature-based phishing detection technique*. 91. 101-106.
- Chuchuen, C., & Chanvarasuth, P. (2015). *Relationship between phishing techniques and user personality model of Bangkok Internet users*. *Kasetsart Journal Social Sciences* 36(2):322–334.
- Chung, T.S. (2013). *Table-top role playing game and creativity*. *Thinking Skills and Creativity*, 8 (2013), pp. 56-71.
- Chung, H., Seo, H., Forbes, S., & Birkett, H. (2020). *Working from home during the COVID-19 lockdown: Changing preferences and the future of work*.
- Cialdini, R.B. (1984). *INFLUENCE The Psychology of Persuasion*.
- Cialdini, R.B. (2021). *Influence, new and expanded: The psychology of persuasion*. HarperCollins.

- Clarke, R.V. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods* (Paper 112), B.Webb (Ed.). London: Home Office, Research Development and Statistics Directorate.
- Clark, L. A., & Watson, D. (2008). *Temperament: An organizing paradigm for trait psychology*. In O. P. John, R. W. Robins, & L. A. Pervin (Eds.), *Handbook of personality: Theory and research* (p. 265–286). The Guilford Press.
- Cohen, L.E., & Felson, M. (1979). *Social Change and Crime Rate Trends: A Routine Activity Approach*. *American Sociological Review*, Vol. 44, No. 4 (Aug., 1979), pp. 588-608. American Sociological Association. Stable URL: <https://www.jstor.org/stable/2094589>.
- Cohen, L. E. Klugel, J. R. & Land, K. C. (1981). *Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory*. *American Sociological Review* 46: 505-524.
- Cohen, G. (2005). *For you, half price*. *The New York Times*, 27.
- Conteh, N. Y., & Schmick, P. J. (2016). *Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks*. *International Journal of Advanced Computer Research*, 6(23), 31.
- Cozens, P., McLeod, S., & Matthews, J. (2018). *Visual representations in crime prevention: exploring the use of building information modelling (BIM) to investigate burglary and crime prevention through environmental design (CPTED)*. *Crime Prevention and Community Safety*. 20. 10.1057/s41300-018-0039-6.
- Craig, J. M., & Piquero, N. L. (2016). *The effects of low self-control and desire-for-control on white-collar offending: A replication*. *Deviant Behavior*, 37(11), 1308-1324.
- Cropsey, A. S. (2018). *The Relationship of Extrinsic and Intrinsic Motivation to Honesty-Humility in University Accounting Majors* (Doctoral dissertation, Northcentral University).
- Cross, C. (2014). *Love hurts: the costly reality of online romance fraud*. *The Conversation*.
- Cross, C., & Gillett, R. (2020). *Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud*. *Journal of Financial Crime*.
- Cross, C. (2020). *Theorising the impact of COVID-19 on the fraud victimisation of older persons*. *The Journal of Adult Protection*.
- Danquah, P., Longe, O. B., Lartey, J. D., & Tobbin, P. E. (2020). *Towards a Theory for Explaining Socially-Engineered Cyber Deception and Theft*. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 44-58). IGI Global.
- Davinson, N., & Sillence, E. (2010). *It won't happen to me: Promoting secure behaviour among internet users*. *Computers in Human Behavior*, 26(6), 1739-1747.
- DeKeseredy, W., & Schwartz, M. (2009). *Dangerous exits: Escaping abusive relationships in rural America*. Piscataway, NJ: Rutgers University Press.
- Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). *Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education*. *CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 915–928. doi:10.1145/2508859.2516753.

- Desilver, D. (2020). *Working from home was a luxury for the relatively affluent before coronavirus - not anymore.* World Economic Forum. <https://www.weforum.org/agenda/2020/03/working-from-home-coronavirus-workers-future-of-work/>.
- Diener, E., Lucas R. E. & Cummings, J. A. (2019). *Personality Traits*. In: Cummings, J. A. and Sanders, L. (2019). Introduction to Psychology. Page 871. Saskatoon, SK: University of Saskatchewan Open Press. <https://openpress.usask.ca/psy120121>.
- Dillenburger, K. (2007). *A Behavior Analytic Perspective on Victimology*. International Journal of Behavioral Consultation and Therapy, Volume 3, No. 3, 2007.
- Djaouti, D., Alvarez, J., & Jessel, J.-P. (2011). *Classifying Serious Games: the G/P/S model*. Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches.
- Djaouti, D., Alvarez, J., Jessel, J. P., & Rampnoux, O. (2011). *Origins of serious games*. Serious games and edutainment applications (pp. 25–43). London: Springer.
- DoJ (2020). *Three Individuals Charged For Alleged Roles In Twitter Hack*. U.S. Department of Justice, DoJ, 31st July 2020. <https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack>.
- Dorr, B., Bhatia, A., Dalton, A., Mather, B., Hebenstreit, B., Santhanam, S., ... & Strzalkowski, T. (2020, April). *Detecting asks in social engineering attacks: Impact of linguistic and structural knowledge*. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 34, No. 05, pp. 7675-7682).
- Doyle, A. (2020). How to Detect and Avoid Fake Recruiter Scams. The balance careers, 12th June 2020. <https://www.thebalancecareers.com/fake-recruiter-scams-and-how-to-avoid-them-2062178>.
- Dumper, K., Jenkins, W., Lacombe A., Lovett, M. & Perimutter, M. (2019) *Learning Approaches to Personality*. In: Swindell, S. (Ed.) (2019). Introductory Psychology.
- Dwan, B. (2004). *Identity theft*. Computer Fraud & Security, 2004(4), 14-17.
- Dyson, S.B., Chang, Y.-L., Chen, H.-C., Hsiung, H.-Y., Tseng, C.-C., & Chang, J.-H. (2015). *The effect of tabletop role-playing games on the creative potential and emotional creativity of Taiwanese college students*. Thinking Skills and Creativity 19 (2016) 88–96.
- Ebbinghaus, H. (1885/1913). *Memory: A contribution to experimental psychology* (H. A. Ruger & C. E. Bussenius, Trans.). New York: Columbia University, Teacher's College. (Reprinted 1964, New York: Dover).
- Eck, J. E. (1994). *Drug markets and drug places: A case-control study of the spatial structure of illicit drug dealing*. PhD dissertation, University of Maryland, College Park.
- Einarsen, K. M. O., & Jack, L. (2019). *Collective action and UK wine investment fraud*. Qualitative Research in Financial Markets.
- Erikson, E. H. (1958). *Young man Luther: A study in psychoanalysis and history*. New York: Norton.
- Erikson, E. H. (1963). *Youth: Change and challenge*. New York: Basic books.

- EUROPOL (2020). *COVID-19: Fraud*. 04 02. <https://www.europol.europa.eu/covid-19/covid-19-fraud>
- Eysenck, H. J. (1947). *Dimensions of personality*. Kegan Paul.
- Eysenck, H. J. (2006). *The Biological Basis of Personality*. First Edition. Routledge. <https://doi.org/10.4324/9781351305280>.
- Eysenck, H. J. (2009). *The biological basis of personality* (3rd ed.). New Brunswick, NJ: Transaction Publishers.
- Fan, W., Lwakatare, K., & Rong, R. (2017). *Social engineering: IE based model of human weakness for attack and defense investigations*. International Journal of Computer Network & Information Security, 9(1).
- Farrington, D.P., & Welsh, B.C. (2005). *Randomized experiments in criminology: What have we learned in the last two decades?* Journal of Experimental Criminology (2005) 1: 9–38.
- Farrington, D.P., Ohlin, L.E., & Wilson, J.Q. (1986). *Understanding and controlling Crime*. New York: Springer Verlag.
- Farrington, D. P., & Loeber, R. (2000). *Some benefits of dichotomization in psychiatric and criminological research*. Criminal behaviour and mental health, 10(2), 100-122.
- Fattah, E.A. (1991). *Understanding Criminal Victimization*. Scarborough, Ont.: Prentice Hall Canada.
- Fattah, E.A. (2000). *Victimology: Past, Present and Future*. Criminologie, Printemps 2000, Vol. 33, No. 1, La Victimologie: Quelques Enjeux (Printemps 2000), pp. 17-46.
- Fattah, E.A. (2010). *The Evolution of a Young, Promising Discipline Sixty Years of Victimology, a Retrospective and Prospective Look*. In Shoham, S.G., Knepper, P., Kett, M. (Ed.), International Handbook of Victimology (Chapter 3, pp. 43-86).
- Fazeli, S.H. (2012). *The Exploring Nature of the Assessment Instrument of Five Factors of Personality Traits in the Current Studies of Personality*. Asian Social Science, 8, 264.
- FBI (2020). *FBI and Secret Service Working Against COVID-19 Threats*. Federal Bureau of Investigation, FBI, 15th April 2020. <https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats>.
- Felson, M., & Cohen, L.E. (1980). *Human Ecology and Crime: A Routine Activity Approach*. Human Ecology, Vol. 8, No. 4, 1980.
- Felson, M. (1986). *Linking criminal choices, routine activities, informal control, and criminal outcomes*. In: D.B. Cornish and R.V. Clarke (eds.) *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag, pp. 119 – 128.
- Felson, M. (2020). *Reducing Crime podcast episodes 1-20*. #16 Marcus Felson. In: Ratcliffe, J. (ed). *The Reducing Crime podcast*. 2020. Accessed at 04.10.2021. Available at <https://www.reducingcrime.com/podcast-1-20>.
- Ferreira, A., Coventry, L., & Lenzini, G. (2015). *Principles of Persuasion in Social Engineering and Their Use in Phishing*. In: Tryfonas T., Askoxylakis I. (eds) *Human Aspects of Information Security, Privacy, and Trust*. HAS 2015. Lecture Notes in Computer Science, vol 9190. Springer, Cham.

- Field, A., Miles, J. and Field, Z. (2012), *Discovering Statistics Using R*. Sage Publications, London.
- Fisher, R. A. (1922). *On the interpretation of χ^2 from contingency tables, and the calculation of P*. Journal of the Royal Statistical Society. 85 (1): 87–94. doi:10.2307/2340521. JSTOR 2340521.
- Fischer, P., Lea, S. E., & Evans, K. M. (2013). *Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance*. Journal of Applied Social Psychology, 43(10), 2060-2072.
- Fischer, H., Boone, W., & Neumann, K. (2014). *Quantitative Research Designs and Approaches*.
- Fisher, J.S., & Radvansky, G.A. (2018). *Patterns of forgetting*. Journal of Memory and Language 102 (2018) 130–141.
- Freud, S. (1916-1917). *A General Introduction to Psychoanalysis*. Published, 1920, by Horace Liveright, Inc.
- Garrett, E. V. (2014). *Exploring internet users' vulnerability to online dating fraud: Analysis of routine activities theory factors*. The University of Texas at Dallas.
- George, M. S., Teunisse, A. K., & Case, T. I. (2020). *Gotcha! Behavioural validation of the gullibility scale*. Personality and Individual Differences, 162, 110034.
- Georgiadou, A., Mouzakitidis, S. & Askounis, D. (2021). *Working from home during COVID-19 crisis: a cyber security culture assessment survey*. Security Journal (2021). <https://doi.org/10.1057/s41284-021-00286-2>
- Glasser, D., & Taneja, A. (2015). *A routine activity theory-based framework for combating cybercrime*. In *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 398-406). IGI Global.
- Glueck, S., & Glueck, E. (1936). (Eds.) *Preventing Crime: A Symposium*. New York: McGraw-Hill. 1936.
- Goeke, L., Quintanar, A., Beckers K., & Pape, S. (2019). *PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks*. Conference: Computer Security - ESORICS 2019 International Workshops, MSTEC 2019, Luxemburg, September 26-27, 2019.
- Goldberg, L. R. (1990). *An alternative description of personality: The Big Five personality traits*. Journal of Personality and Social Psychology, 59, 1216–1229.
- Gottfredson, M. R., & Hirschi, T. (1990). *A General theory of crime*. Stanford, CA: Stanford University Press.
- Gosling, S.D., Rentfrow, P.J., & Swann, Jr. W.B. (2003). *A very brief measure of the Big-Five personality domains*. Journal of Research in Personality 37 (2003) 504–528. Department of Psychology, University of Texas, Seay Psychology Bldg. Rm. 4.212, Austin, TX 78712, USA.
- Gragg, D. (2003). *A Multi-Level Defense Against Social Engineering*. SANS Institute - InfoSec Reading Room, Tech. Rep.
- Gray, J. (1842). *An efficient remedy for the distress of Nations*. 1842. Edinburgh.

- Greenhalgh, T. (2010). (4th Edition) *How to read a paper: The basics of evidence-based medicine*. BMJ Publishing: London.
- Grossrieder, L., Chopin, J., Jendly, M., Genessay, T., & Baechler, S. (2017). *Nothing is permanent except change: a case study of crime displacement in Switzerland*. *Security Journal*, 30(3), 749-771.
- Gupta, S., Singhal, A., & Kapoor, A. (2016). *A literature survey on social engineering attacks: Phishing attack*. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.
- Gusenbauer, M, Haddaway, NR (2020). *Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources*. *Res Syn Meth*. 2020; 11: 181– 217. <https://doi.org/10.1002/jrsm.1378>.
- Haapasalo, J., & Pulkkinen, L. (1992). *The Psychopathy Checklist and non-violent offender groups*. *Criminal Behaviour and Mental Health*, 2(4), 315-328.
- Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.
- Hadnagy, C., & Schulman, S. (2021). *Human hacking: Win friends, influence people, and leave them better off for having met you* (p. 17). New York: Harper Business.
- Hadlington, L. (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. *Heliyon* 3 (2017) e00346. doi: 10.1016/j.heliyon.2017.e00346.
- Hadlington, L., & Murphy, K. (2018). *Is media multitasking good for cybersecurity? exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors*. *Cyberpsychology, Behavior, and Social Networking*, 21(3), 168-172.
- Hamann, U. (2017). *In der Schokoladenfabrik: IT-Sicherheit spielerisch verbessern*. *Wirtsch Inform Manag* 9, 40–47 (2017). <https://doi.org/10.1007/s35764-017-0088-0>.
- Hansson, S. O. (2006). *A note on social engineering and the public perception of technology*. *Technology in Society*, 28(3), 389-392.
- Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). *Riskio: A Serious Game for Cyber Security Awareness and Education*. *Computers & Security* 95 (2020) 101827.
- Hartshorne, H., & May, M. A. (1928). *Previous efforts to measure deceptive conduct*. In H. Hartshorne, M. A. May, *Character Education Inquiry, & The Institute of Social and Religious Research, Studies in the nature of character, [part] 1: Studies in deceit: book 1, General methods and results; book 2, Statistical methods and results* (p. 28–46). MacMillan Co. <https://doi.org/10.1037/13386-002>
- Heartfield, R., Loukas, G., & Gan, D. (2016). *You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks*. *IEEE Access*. PP. 1-1. 10.1109/ACCESS.2016.2616285.
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

- Hinson, G. (2008) *Social Engineering Techniques, Risks, and Controls*. EDPACS, 37:4-5, 32-46, DOI: 10.1080/07366980801907540.
- Hochstetler, A., & Copes, H. (2016). *Qualitative Criminology's Contributions to Theory*. In: The Handbook of Criminological Theory, First Edition. Edited by Alex R. Piquero. 2016 John Wiley & Sons, Inc. Published 2016 by John Wiley & Sons, Inc.
- Holt, T. J., & Turner, M. G. (2012). *Examining risks and protective factors of on-line identity theft*. Deviant Behavior, 33(4), 308-323.
- Hong, K.W., Kelley, C.M., Tembe, R., Murphy-Hill, E., & Mayhorn, C.B. (2013). *Keeping up with the Joneses: assessing phishing susceptibility in an email task*. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 57, No. 1, pp. 1012–1016). Sage CA: Los Angeles, CA: SAGE Publications, 57, 1012, 1016.
- Hove, L. (2020). *Strategies Used to Mitigate Social Engineering Attacks* (Doctoral dissertation, Walden University).
- Hutchings, A. (2018). *Leaving on a jet plane: the trade in fraudulently obtained airline tickets*. Crime, Law and Social Change; Dordrecht Vol. 70, N° 4, (Nov 2018): 461-487. DOI:10.1007/s10611-018-9777-8.
- Hutchings, A., & Hayes, H. (2009). *Routine activity theory and phishing victimisation: who gets caught in the 'net'?*. Current Issues in Criminal Justice, 20(3), 433-452.
- Iliffe, R. (2009). Newton and the money men. Nature, 462(7269), 39-40.
- Ivan, N., Ahishakiye, E., Omulo, E. O., & Taremwa, D. (2017). *Crime Prediction Using Decision Tree (J48) Classification Algorithm*. International Journal of Computer and Information Technology (ISSN: 2279 – 0764).
- Ivaturi, K., Janczewski, L., & Chua, C. (2014). *Exploring the effects of users' Frame of mind on online deception detection attitude and behaviour*.
- Iyengar, R. (2020). *Twitter accounts of Joe Biden, Barack Obama, Elon Musk, Bill Gates, and others apparently hacked*. CNN Business. Archived from the original on July 16, 2020. Retrieved July 15, 2020. <https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html> .
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). *Social phishing*. Communications of the ACM, 50(10), 94-100.
- Jansen, J., & Leukfeldt, R. (2015). *How people help fraudsters steal their money: An analysis of 600 online banking fraud cases*. In 2015 workshop on socio-technical aspects in security and trust (pp. 24-31). IEEE.
- Jansen van Rensburg, S. (2018). *Contextualising social engineering through criminological theorising*. Acta Criminologica: African Journal of Criminology & Victimology, 31(3), 1-19.
- Jansiewicz, D. R. (1973). *The New Alexandria Simulation: A Serious Game of State and Local Politics*. Canfield Press.
- Jansiewicz, D. R. (2020). *The Game of Politics - Frequently Asked Questions*. Retrieved January 6, 2020, from: http://gameofpolitics.com/f__a__q_.htm.
- Jones, D. N., & de Roos, M. S. (2016). *Validating the four components of Mimicry Deception Theory from the victim's perspective*. Personality and Individual Differences, 95, 37-39.

- Judges, R.A., Gallant, S.N., Yang, L., & Lee, K. (2017). *The role of cognition, personality, and trust in fraud victimisation in older adults*. *FrontPsychol* 8:588.
- Jung, C. G. (1921) *Psychological Types*. Zürich: Rascher 1921. Neu in GW 6. Zürich: Rascher 1960.
- Jung, C.G. (1959) *The archetypes and the collective unconscious*. Originally published in England in 1959 by Routledge & Kegan Paul. 2nd ed., 1968. In 2 parts.
- Junger, M., Montoya, L., & Overink, F. J. (2017). *Priming and warnings are not effective to prevent social engineering attacks*. *Computers in human behavior*, 66, 75-87.
- KAPO Zürich (2020). *Neue Telefonbetrüge mit Vorwand des Corona-Virus*. Kantonspolizei Zürich, KAPO Zürich, 16th March 2020. <https://www.cybercrimepolice.ch/de/fall/neue-telefonbetruege-mit-vorwand-des-corona-virus/>.
- KAPO Zürich (2020). *Meilen: Polizei verhaftet zwei «Falsche Polizisten»*. Kantonspolizei Zürich, KAPO Zürich, 22th July 2020. <https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2020/07/2007221h.html>.
- Kaptein, M. C. (2012). *Personalized persuasion in ambient intelligence*. Eindhoven: Technische Universiteit Eindhoven. <https://doi.org/10.6100/IR729200>
- Karwowski, M., & Soszynski, M. (2008). *How to develop creative imagination? Assumptions, aims and effectiveness of role play training in creativity (RPTC)*. *Thinking Skills and Creativity*, 3 (2008), pp. 163-171.
- Keen, J., & Fitness, J. (2011). *Can employers screen job applicants for potential white collar fraud offenders?*. In *Personality and Individual Differences: Theory, Assessment, and Application* (pp. 265-274). Nova Science Publishers.
- Kent, S. A. (2008). *Narcissistic Fraud in the Ancient World: Lucian's Account of Alexander of Abonuteichos and the Cult of Glycon*. *Cultic Studies Review*, 7(3).
- Kertz, C. L., & Burnette, L. B. (1992). *Telemarketing Tug-of-War: Balancing Telephone Information Technology and the First Amendment with Consumer Protection and Privacy*. *Syracuse L. Rev.*, 43, 1029.
- Killias, M., Kuhn, A., & Aebi, M.F. (2012). *Précis de criminologie*. Troisième édition. © Stämpfli Editions SA Berne · 2012.
- Kilovaty, I. (2019). *Legally Cognizable Manipulation*. *Berkeley Tech. LJ*, 34, 449.
- Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). *Risk factors for social networking site scam victimization among Malaysian students*. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 123-128.
- Kleist, V., Dull, R., & Morris, B. (2012). *Importance of IT Controls for Casino Slot Machines: A Case of Social Engineering and Software Based Fraud*.
- Kondo, M. C., Keene, D., Hohl, B. C., MacDonald, J. M., & Branas, C. C. (2015). *A difference-in-differences study of the effects of a new abandoned building remediation strategy on safety*. *PloS one*, 10(7), e0129582.
- Krause, R. (2015). *Social Engineering Scam: Fake LinkedIn Profiles*. LinkedIn, 14th October 2015. <https://www.linkedin.com/pulse/social-engineering-scam-fake-linkedin-profiles-randall-krause>.

- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). *Advanced social engineering attacks*. *Journal of Information Security and applications*, 22, 113-122.
- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., & Hong, J. (2007). *Protecting people from phishing: The design and evaluation of an embedded training email system*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905-914).
- LaFleur, B. J., & Greevy, R. A. (2009). *Introduction to Permutation and Resampling-Based Hypothesis Tests**. *Journal of Clinical Child & Adolescent Psychology*, 38(2), 286-294.
- Lancaster, M. (2021). *A Quantitative Study on How Personality Affects the Ability to Detect Phishing* (Doctoral dissertation, Capella University).
- Lang, F.R., John, D., Lüdtke, O., Schupp, J., & Wagner, G.G. (2011). *Short assessment of the Big Five: robust across survey methods except telephone interviewing*. *Behav Res* (2011) 43:548–567 DOI 10.3758/s13428-011-0066-z.
- Lauritsen, J. L., & Davis Quinet, K. F. (1995). *Repeat victimization among adolescents and young adults*. *Journal of Quantitative Criminology*, 11(2), 143-166.
- Lee, K., & Ashton, M. C. (2004). *Psychometric properties of the HEXACO personality inventory*. *Multivariate behavioral research*, 39(2), 329-358.
- Leukfeldt, E. R. (2014). *Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization*. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551-555.
- Linehan, C., Lawson, S., & Doughty, M. (2009). *Tabletop Prototyping of Serious Games for 'Soft Skills' Training*. Coventry, UK: 2009 Conference in games and virtual worlds for serious applications.
- Lingnau, V., Fuchs, F., & Dehne-Niemann, T. E. (2017). *The influence of psychopathic traits on the acceptance of white-collar crime: do corporate psychopaths cook the books and misuse the news?* *Journal of Business Economics*, 87(9), 1193-1227.
- Liu, W., & Zhong, S. (2017). *Web malware spread modelling and optimal control strategies*. *Scientific reports*, 7(1), 1-19.
- Long, J. (2008). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Rockland, MA: Syngress Publishing.
- Long, R. M. (2013). *Using phishing to test social engineering awareness of financial employees*. (Doctoral dissertation, Eastern Washington University).
- Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (2010). *Seeing beyond the surface, understanding and tracking fraudulent cyber activities*. arXiv preprint arXiv:1001.1993.
- Lusignan, R. & Marleau, J. (2010). *The Evolution of a Young, Promising Discipline Sixty Years of Victimology, a Retrospective and Prospective Look*. In Shoham, S.G., Knepper, P., Kett, M. (Ed.), *International Handbook of Victimology* (Chapter 11, pp. 303.-318).
- Ma, K. W. F., & McKinnon, T. (2021). *COVID-19 and cyber fraud: emerging threats during the pandemic*. *Journal of Financial Crime*.

- Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. A. (2017). *A systematic literature review: Information security culture*. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 1-6). IEEE.
- Marriott, C. (2018). *Through the Net: Investigating How User Characteristics Influence Susceptibility to Phishing*.
- Mann, I. (2008). *Hacking the human: Social engineering techniques and security measures*. Burlington, VT: Gower Publishing Company.
- Manske, K. (2000). *An introduction to social engineering*. *Inf. Secur. J. A Glob. Perspect.*, 9(5), 1-7.
- Maslow, A. H. (1954). *Motivation and personality*. New York: Harper.
- Matsel, G.W. (1859). *Vocabulum or The Rogue's Lexicon. Confidence Man*. In: The Project Gutenberg EBook of *Vocabulum*, by George W. Matsell. Released on June 13, 2016 by Curnow, C. & Schaal, E. <https://www.gutenberg.org/files/52320/52320-h/52320-h.htm>. Accessed on: 19.05.2022.
- Mawby, R., & Walklate, S. (1994). *Critical victimology: International perspectives*. Thousand Oaks, CA: Sage.
- Maxfield, M., & Babbie, E. (2017). *Research Methods for Criminal Justice and Criminology 8th Edition*. Wadsworth Publishing.
- Mazerolle, L., & Bennett, S. (2011). *Experimental Criminology*. In obo in *Criminology*. 13 Jan. 2020. <<https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0085.xml>>.
- McConnell, J. P. (2020). *UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases*.
- McCord, J. (1992). *The Cambridge-Somerville Study: A pioneering longitudinal-experimental study of delinquency prevention*. In *Preventing Antisocial Behavior*, edited by J. McCord and R. E. Tremblay, 196–206. New York: Guilford.
- McCord, J., & McCord, W. (1959). *A follow-up report on the Cambridge-Somerville youth study*. *The ANNALS*, 322, 89–96.
- McGuire, J. (2004). *Understanding Psychology and Crime: Perspectives on Theory and Action*. McGraw-Hill Education (UK), 01.09.2004.
- McCrae, R. R., & Costa, P. T. (1987). *Validation of the five-factor model of personality across instruments and observers*. *Journal of Personality and Social Psychology*, 52, 81–90.
- McCrae, R. R. & John, O. P. (1992). *An introduction to the five-factor model and its applications*. *Journal of Personality*, 60, 175–215.
- McNemar, Quinn. 1947. *Note on the sampling error of the difference between correlated proportions of percentages*. *Psychometrika* 12:153–7.
- Mendelsohn, B. (1956). *The victimology*. *Etudes Internationales de psycho-sociologie criminelle*, 10, 23–26.

- Mermod, A. Y. (2012). *Fraud in modern banking: Highlights on online internet banking fraud*. In *Emerging Fraud* (pp. 149-161). Springer, Berlin, Heidelberg.
- Meyer, B. D. (1995). *Natural and quasi-experiments in economics*. *Journal of business & economic statistics*, 13(2), 151-161.
- Michael, D., & Chen, S. (2005). *Serious Games: Games That Educate, Train, and Inform (1er ed.)*. Course Technology PTR.
- Miethe, T. D., & McDowall, D. (1993). *Contextual effects in models of criminal victimization*. *Social Forces*, 71(3), 741-759.
- Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*. Albany, NY: Suny Press.
- Mitnick, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley.
- Mischel, W. (1968). *Personality and assessment*. New York: John Wiley.
- Mohebzada, J. G., El Zarka, A., BHOjani, A. H., & Darwish, A. (2012, March). *Phishing in a university community: Two large scale phishing experiments*. In *2012 international conference on innovations in information technology (IIT)* (pp. 249-254). IEEE.
- Mouton, F., Leenen, L., & Venter, H.S. (2016). *Social Engineering Attack Examples, Templates and Scenarios*. *Computers & Security*, Jun 2016, Vol.59, p.186.
- Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). *Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud*. *Computers in Human Behavior*, 69, 421-436.
- Mufor, B. S., Marnewick, A., & von Solms, S. (2022). *The Development of Cybersecurity Awareness Measurement Model in the Water Sector*. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 211-218).
- Muhly, F., Jordan, J., Cialdini, R.B. (2021). *Your Employees Are Your Best Defense Against Cyberattacks*. *Harvard Business Review*, HBR, August 30, 2021. <https://hbr.org/2021/08/your-employees-are-your-best-defense-against-cyberattacks>.
- Muhly, F., Leo, P., & Caneppele, S. (2021). *A Serious Game For Social Engineering Awareness Creation*. *Journal of Cybersecurity Education, Research and Practice*: Vol. 2022 : No. 1 , Article 4. Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/5/>.
- Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. (2017). *The malevolent side of human nature: A meta-analysis and critical review of the literature on the dark triad (narcissism, Machiavellianism, and psychopathy)*. *Perspectives on Psychological Science*, 12(2), 183-204.
- Murre, J.M.J., Dros, J. (2015). *Replication and Analysis of Ebbinghaus' Forgetting Curve*. *PLoS ONE* 10(7): e0120644. doi:10.1371/journal.pone.0120644.
- Müller, R. K. (2010). *History of doping and doping control*. *Doping in sports: Biochemical principles, effects and analysis*, 1-23.
- Myers, D.G. (1994). *Exploring Social Psychology*. McGraw-Hill series in social psychology. New York : McGraw-Hill, c1994.

- Nagy, K., Hale, B., & Strouble, D. (2010). *Verify Then Trust: A new Perspective on Preventing Social Engineering*. In International Conference on Cyber Warfare and Security (p. 259). Academic Conferences International Limited.
- Nettleton, E. (2006). *End of the line for phone scams?* Journal of Database Marketing & Customer Strategy Management, 13(3), 231-235.
- Neuman, L. W. (2003). *Social Research Methods: Qualitative and Quantitative Approaches*. Massachusetts: Allyn & Bacon.
- Newbould, M., & Furnell, S. (2009). *Playing Safe: A Prototype Game For Raising Awareness of Social Engineering*. Proceedings of the 7th Australian Information Security Management Conference.
- Neyroud, Peter. (2007). *Community Policing*. Policing. 1. 10.1093/police/pam032.
- Njenga, K. (2018). *Social media information security threats: Anthropomorphic emoji analysis on social engineering*. In IT Convergence and Security 2017 (pp. 185-192). Springer, Singapore.
- Nohlberg, M. (2009). *Why humans are the weakest link*. In Social and human elements of information security: Emerging trends and countermeasures (pp. 15-26). IGI Global.
- Norris, G., Brookes, A., & Dowell, D. (2019). *The psychology of internet fraud victimisation: A systematic review*. Journal of Police and Criminal Psychology, 34(3), 231-245.
- NCSC (2020). *Cyber experts step in as criminals seek to exploit Coronavirus fears*. National Cyber Security Center, NCSC, 16th March 2020. <https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus>.
- Nunes, P., Antunes, M., & Silva, C. (2021). *Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions*. Procedia Computer Science, 181, 173-181.
- Olanrewaju, A.-S. T., & Zakaria, N.H. (2015). *Social engineering awareness game (SEAG): an empirical evaluation of using game towards improving information security awareness*. Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015 11-13 August 2015 Istanbul, Turkey. Universiti Utara Malaysia (<http://www.uum.edu.my>).
- O'Reilly III, C. A., Doerr, B., & Chatman, J. A. (2018). "See You in Court": How CEO narcissism increases firms' vulnerability to lawsuits. The Leadership Quarterly, 29(3), 365-378.
- Oxford English Dictionary (2019). *Social Engineer*: <https://www.oed.com/view/Entry/272695>.
- Oxford English Dictionary (2019). *Social Engineering*: <https://www.oed.com/view/Entry/272695>.
- Oxford English Dictionary (2022). *Fraud*: <https://www.oed.com/view/Entry/74298?isAdvanced=false&result=1&rskey=iEci4v&>.
- Paris, B. (1994). *Karen Horney: a psychoanalyst's search for self-understanding.*, New Haven, CT: Yale Univ. Press.
- Padayachee, K. (2020). *Understanding the Relationship Between the Dark Triad of Personality Traits and Neutralization Techniques Toward Cybersecurity Behaviour*. International Journal of Cyber Warfare and Terrorism (IJCWT), 10(4), 1-19.

- Parker, J. N. (2019). *Examining the Relationship Between Workplace Victimization, the Dark Triad, and Workplace Behavior*.
- Parno, B., Kuo, C., & Perrig, A. (2006). *Phoolproof phishing prevention*. In International conference on financial cryptography and data security (pp. 1-19). Springer, Berlin, Heidelberg.
- Pattinson, M.R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M.A. (2011). *Managing phishing emails: a scenario-based experiment*. Paper presented at the Proceedings of the Fifth International Symposium on Human Aspects of the Information Security & Assurance HAISA (pp. 74–85).
- Pavlov, I. P. (1927). *Conditional reflexes* (G. V. Anrep, Trans.). New York: Oxford University Press.
- Paulhus, D.L., & Williams, K.M. (2002). *The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy*. *Journal of Research in Personality* Volume 36, Issue 6, December 2002, Pages 556-563.
- Perri, F. S. (2011). *White-collar criminals: The 'kinder, gentler' offender?* *Journal of Investigative Psychology and Offender Profiling*, 8(3), 217-241.
- Pimentel, A., & Steinmetz, K. F. (2022). *Enacting social engineering: the emotional experience of information security deception*. *Crime, Law and Social Change*, 77(3), 341-361.
- Popper, K.R. (1966). *The Open Society and Its Enemies*. (Princeton University Press, Princeton, New Jersey, fifth edition, 1966).
- Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). *Self-control and victimization: A meta-analysis*. *Criminology*, 52, 87–116.
- Proofpoint, Inc. (PFPT) (2022). *2022 State of the Phish. An In-Depth Exploration of User Awareness, Vulnerability and Resilience*. Retrieved March 31, 2022, from: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>.
- Puig-Verges, N., & Schweitzer, M. G. (1996). *Swindlers, swindling and expression of psychopathology*. In *Annales medico-psychologiques* (Vol. 154, No. 2, pp. 132-5).
- Purdioux, L. (2015). *Predicting deception detection ability based on the concept of self-compassionate personality trait, openness personality structure, and agreeableness personality structure* (Doctoral dissertation, Capella University).
- Quisenberry, W. L. (2017). *Ponzi of all Ponzis: critical analysis of the Bernie Madoff scheme*. *International Journal of Econometrics and Financial Management*, 5(1), 1-6.
- Radvansky, G.A., O'Rear, A.E., & Fisher, J.S. (2017). *Event models and the fan effect*. *Mem Cogn* (2017) 45:1028–1044 DOI 10.3758/s13421-017-0713-4.
- Raman, K. (2008). *Ask and you will receive*. *McAfee Security Journal*, 1-12.
- Rammstedt, B., Kemper, C.J., Klein, M.C., Beierlein, C. & Kovaleva, A. (2012). *Eine kurze Skala zur Messung der fünf Dimensionen der Persönlichkeit: Big-Five-Inventory-10 (BFI-10)*. *GESIS-Working Papers 2012|22*. GESIS – Leibniz-Institut für Sozialwissenschaften 2012.
- Reuschke, D., & Felstead, A. (2020). *The effect of the Great Lockdown on homeworking in the United Kingdom*.

- Ribeiro, R., Guedes, I. S., & Cruz, J. N. (2019). *White-collar offenders vs. common offenders: a comparative study on personality traits and self-control*. *Crime, Law and Social Change*, 72(5), 607-622.
- Riniolo, T. C. (1999). *Using a Large Control Group for Statistical Comparison: Evaluation of a Between-Groups Median Test*. *The Journal of Experimental Education*, 68(1), 75–88. <http://www.jstor.org/stable/20152616>.
- Roberts, S. A. (2021). *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors* (Doctoral dissertation, Northcentral University).
- Rogers, C. (1980). *A Way of Being*. Houghton Mifflin; 1st edition (January 1, 1980).
- Rudman, S.A. (2019). *Serious games to study the influence of wildlife devaluation strategies on hunter behaviour*. A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Master of Science. Victoria University of Wellington, 2019.
- Rusch, J. (1999). *The Social Engineering of Internet Fraud*. United States Justice Department – Proceedings of the 1999 Internet Society Conference.
- Ruskov, M., Maestre Celdran, J., Ekblom, P., & Sasse, A. (2012). *Unlocking the Next Level of Crime Prevention: Development of a Game Prototype to Teach the Conjunction of Criminal Opportunity*. *Information Technologies and Control*. 8.
- Ruskov, M.P. (2014). *Employing variation in the object of learning for the design-based development of serious games that support learning of conditional knowledge*.
- Salahdine, F., & Kaabouch, N. (2019). *Social Engineering Attacks: A Survey*. *Future Internet* 2019, 11, 89; doi:10.3390/fi11040089.
- Saleem, J., & Hammoudeh, M. (2018). *Defense Methods Against Social Engineering Attacks*. 10.1007/978-3-319-58424-9_35.
- Salu, A. O. (2004). *Online crimes and advance fee fraud in Nigeria-are available legal remedies adequate?* *Journal of Money Laundering Control*.
- Sampson, R. J., & Lauritsen, J. L. (1990). *Deviant lifestyles, proximity to crime, and the offender-victim link in personal violence*. *Journal of Research in Crime and Delinquency*, 27, 110–139.
- Sampson, R., Eck, J.E., & Dunham, J. (2010). *Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure*. 2010 Macmillan Publishers Ltd. 0955–1662 *Security Journal* Vol. 23, 1, 37–51.
- Sawyer, B., & Rejeski, D. (2002). *Serious Games: Improving Public Policy Through Game-based Learning and Simulation*. Woodrow Wilson International Center for Scholars.
- Schild, C., Moshagen, M., Ścigała, K. A., & Zettler, I. (2020). *May the odds--or your personality--be in your favor: Probability of observing a favorable outcome, Honesty-Humility, and dishonest behavior*. *Judgment & Decision Making*, 15(4).
- Schipke, Rae. (2006). *The Language of Phishing, Pharming, and Other Internet Fraud-Metaphorically Speaking*. 1 - 6. 10.1109/ISTAS.2006.4375897.

- Schneider, M. (2020). *Protection Motivation Theory Factors that Influence Undergraduates to Adopt Smartphone Security Measures* (Doctoral dissertation, Capella University).
- Schreck, C. J. (1999). *Criminal victimization and low self-control: An extension and test of a general theory of crime*. *Justice Quarterly*, 16, 633–654.
- Schreck, C. J., Stewart, E. A., & Fisher, B. S. (2006). *Self-control, victimization, and their influence on risky lifestyles: A longitudinal analysis using panel data*. *Journal of Quantitative Criminology*, 22(4), 319-340.
- Schur, E. M. (1957). *Sociological analysis of confidence swindling*. *The Journal of Criminal Law, Criminology, and Police Science*, 48(3), 296-304.
- Semrad, M., Scott-Parker, B., & Vanags, T. (2020). *DeceIT and Personality: Which HEXACO Traits Make a Convincing Liar?*. *Journal of Police and Criminal Psychology*, 1-8.
- Sengstock, M. (1976). *The Culpable Victim in Mendelsohn's Typology*. Paper presented at the Annual Meeting of the Midwest Sociological Society (St. Louis, Missouri, April 21-24, 1976).
- Shafer, W. E., & Wang, Z. (2018). *Machiavellianism, social norms, and taxpayer compliance*. *Business Ethics: A European Review*, 27(1), 42-55.
- Shane, J. M., Piza, E. L., & Mandala, M. (2015). *Situational crime prevention and worldwide piracy: a cross-continent analysis*. *Crime science*, 4(1), 1-13.
- Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). *Personality as a Predictor of Cybersecurity Behavior*. *Psychology of Popular Media Culture*. Advance online publication. doi: <http://dx.doi.org/10.1037/ppm000024>
- Sharma T., Bashir M. (2020) *An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited*. In: Corradini I., Nardelli E., Ahram T. (eds) *Advances in Human Factors in Cybersecurity*. AHFE 2020. *Advances in Intelligent Systems and Computing*, vol 1219. Springer, Cham. https://doi.org/10.1007/978-3-030-52581-1_7.
- Shaw, C. (2020). *Why Phishing Works and the Detection Needed to Prevent It* (Doctoral dissertation, Utica College).
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish*. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).
- Sherman, L.W., & Berk, R.A. (1984). *The Minneapolis Domestic Violence Experiment*. Police Foundation Reports, April 1984.
- Skinner, B. F. (1953). *Science and Human Behavior*. Macmillan.
- Sorace, S., Quercia, E., La Mattina, E., Charalampos, Z. Patrikakis, L., Bacon, G., & Mackinnon, L. (2018). *Serious Games: An Attractive Approach to Improve Awareness*. *Community-Oriented Policing and Technological Innovations*.
- Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I., et al. (2016). *A serious game empowering the prediction of potential terrorist actions*. *Journal of Policing, Intelligence and Counter Terrorism*, 11(1), 30.
- Speiser, J. L., Miller, M. E., Tooze, J., & Ip, E. (2019). *A comparison of random forest variable selection methods for classification prediction modeling*. *Expert systems with applications*, 134, 93-101.

- Spinelli, L. (2018). *Tabletop Role-Playing Games and Social Skills in Young Adults*. Honors College Theses. 192. https://digitalcommons.pace.edu/honorscollege_theses/192.
- Stajano, F., & Wilson, P. (2009). *Understanding scam victims: seven principles for systems security*. *Commun. ACM* 54(3), 70–75.
- Steinmetz, K. F. (2021). *The Identification of a model victim for social engineering: A qualitative analysis*. *Victims & Offenders*, 16(4), 540-564.
- Stelmack, R. M., & Stalikas, A. (1991). *Galen and the humour theory of temperament*. *Personal Individual Difference*, 12(3), 255–263.
- Stirnemann, S. (2018). *Social Engineering als Modus Operandi*. In *Der Mensch als Risikofaktor bei Wirtschaftskriminalität* (pp. 127-157). Springer Gabler, Wiesbaden.
- Sumar, S., & Ismail, H. (1995). *Adulteration of foods—past and present*. *Nutrition & Food Science*.
- Sun, J. C.-Y. & Yeh, K. (2016). *The effects of attention monitoring with EEG biofeedback on university students' attention and self-efficacy: The case of anti-phishing instructional materials*. *Computers & Education*. 106. 10.1016/j.compedu.2016.12.003.
- Susi, T., Johannesson, M., & Backlund, P. (2007). *Serious Games: An Overview (HS- IKI -TR-07-001)*. Retrieved from <https://www.diva-portal.org/smash/get/diva2:2416/FULLTEXT01.pdf>.
- Tabron, J. L. (2016). *Creating urgency in tech support scam telephone conversations*. Hofstra University.
- Taherdoost, H. (2016). *Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research*. *International Journal of Academic Research in Management (IJARM)* Vol. 5, No. 2, 2016, Page: 18-27, ISSN: 2296-1747.
- Tarun, R. (2020). *COVID-19 Social Engineering Attacks*. CSO, 23rd March 2020. <https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html>
- Tedeschi, J. T., & Felson, R. B. (1994). *Violence, aggression, and coercive actions*. Washington, DC: American Psychological Association.
- Tetri, P., & Vuorinen, J. (2013). *Dissecting social engineering*. *Behaviour & Information Technology*, 32(10), 1014-1023.
- Tewksbury, R. (2009). *Qualitative versus quantitative methods: Understanding why qualitative methods are superior for criminology and criminal justice*. In *Journal of Theoretical and Philosophical Criminology* 1(1): 38-58.
- Tewksbury, R.A., & Mustaine, E.E. (2010). *Encyclopedia of Criminological Theory*. "Cohen, Lawrence E., and Marcus K. Felson: Routine Activity Theory". Pub. Date: 2010. Publishing Company: SAGE Publications, Inc. City: Thousand Oaks. Print ISBN: 9781412959186. Online ISBN: 9781412959193. DOI: <http://dx.doi.org/10.4135/9781412959193.n52>. Print pages: 187-192.
- Thompson, S. (2006). *Helping the hacker? Library information, security, and social engineering*. *Information Technology and Libraries*, 25, 222-225.
- Tidy, J. (2020) *Major US Twitter accounts hacked in Bitcoin scam*. BBC News, 16th July 2020. <https://www.bbc.com/news/technology-53425822>.

- Tillyer, M. S., Fisher, B. S., & Wilcox, P. (2011). *The effects of school crime prevention on students' violent victimization, risk perception, and fear of crime: A multilevel opportunity perspective*. *Justice Quarterly*, 28, 249–277.
- Tillyer Skubak, M., & Eck, J.E. (2011). *Getting a handle on crime: A further extension of routine activities theory*. 2011 Macmillan Publishers Ltd. 0955–1662 *Security Journal* Vol. 24, 2, 179–193.
- Triandis, H.C. & Suh, E. M. (2002). *Cultural Influences on Personality*. *Annual Review of Psychology* 2002 53:1, 133-160.
- Trim, P. R., & Lee, Y. I. (2019). *The role of B2B marketers in increasing cyber security awareness and influencing behavioural change*. *Industrial Marketing Management*, 83, 224-238.
- Townsend, K. (2010). *The art of social engineering*. *Infosecurity*, 7(4), 32-35.
- Uebelacker, S., & Quiel, S. (2014). *The Social Engineering Personality Framework*. Workshop on Socio-Technical Aspects in Security and Trust, 24–30.
- Valuck, R. J., Poirier, S., & Mrtek, R. G. (1992). *Patent medicine muckraking: influences on American pharmacy, social reform, and foreign authors*. *Pharmacy in history*, 34(4), 183-192.
- Van de Weijer, S. G., & Leukfeldt, E. R. (2017). *Big five personality traits of cybercrime victims*. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407-412.
- Van Dijk, J. and Steinmetz, C.H.D. (1982). *A First Step Towards Victimological Risk analysis*. The Hague: Ministry of Justice.
- Van Rensburg, Y. E. J., de Kock, F. S., & Derous, E. (2018). *Narrow facets of honesty-humility predict collegiate cheating*. *Personality and Individual Differences*, 123, 199-204.
- Van Scotter, J. R., & Roglio, K. D. D. (2020). *CEO bright and dark personality: Effects on ethical misconduct*. *Journal of Business Ethics*, 164(3), 451-475.
- Van Wyk, J., & Benson, M. L. (1997). *Fraud victimization: risky business or just bad luck?*. *American Journal of Criminal Justice*, 21(2), 163-179.
- Vermillion, S. D., Malak, R. J., Smallman, R., & Fields, S. (2014). *Linking Normative and Descriptive Research with Serious Gaming*. *Procedia Computer Science*, 28, 204-212.
- Vermillion, S. D., Malak, R. J., Smallman, R., Becker, B., Sferra, M., & Fields, S. (2017). *An investigation on using serious gaming to study human decision-making in engineering contexts*. *Design Science*, 3, e15.
- Verizon (2022). *2022 Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/dbir/>
- Von Hentig, H. (1948). *The Criminal and His Victim*. New Haven: Yale University Press.
- Walker, L. E. (1984). *The battered woman syndrome*. New York, NY: Springer.
- Watson, D. (2019) *Personality Assessment*. In: Cummings, J. A. and Sanders, L. (2019). *Introduction to Psychology*. Page 871. Saskatoon, SK: University of Saskatchewan Open Press. <https://openpress.usask.ca/psy120121>.

- Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). *Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users*. In International Conference on Human-Computer Interaction (pp. 650-668). Springer, Cham.
- Weissburd, D. (2000). *Randomized Experiments in Criminal Justice Policy: Prospects and Problems*. *Crime & Delinquency*, Vol. 46 No. 2, April 2000, 181-193.
- Welsh, B.C., Dill, N.E., & Zane, S.N. (2019). *The first delinquency prevention experiment: a socio-historical review of the origins of the Cambridge-Somerville Youth Study's research design*. *J Exp Criminol* (2019) 15:441–451 <https://doi.org/10.1007/s11292-018-9323-9>.
- Wendorf Muhamad, J., & Yang, F. (2019). *Cross-cultural learning in gameplay: BAFÁ BAFÁ, persuasive technology, and the exploration of intercultural sensitivity*. *Simulation & Gaming*, 50(6), 848-859.
- Wilcox, P. (2010). *Victimology, theories of in Fisher*. In B. S. Fisher (Ed.), *Encyclopedia of victimology and crime prevention* (Vol. 1, pp. 978–986). Thousand Oaks, CA: Sage.
- Wilcox, H., Bhattacharya, M., & Islam, R. (2014). *Social engineering through social media: an investigation on enterprise security*. In International Conference on Applications and Techniques in Information Security (pp. 243-255). Springer, Berlin, Heidelberg.
- Wilcox, H. & Bhattacharya, M. (2015). *Countering social engineering through social media: An enterprise security perspective*. In *Computational Collective Intelligence* (pp. 54-64). Springer, Cham.
- Wiley, A., McCormac, A., & Calic, D. (2020). *More than the individual: Examining the relationship between culture and Information Security Awareness*. *Computers & Security*, 88, 101640.
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). *Individual differences in susceptibility to online influence: A theoretical review*. *Computers in Human Behavior*, 72, 412-421.
- Wilson, D. B. (2001). *Meta-analytic methods for criminology*. *The Annals of the American Academy of Political and Social Science*, 578(1), 71-89.
- Wincup, E. (2017). *Criminological Research Understanding qualitative methods*. Second Edition. SAGE Publications, 2017.
- Winkler, I. S. (1996). *Case study of industrial espionage through social engineering*. In Proceedings of the 19 th Information Systems Security Conference (pp. 1-7).
- Workman, M. (2008). *Wisecracker: A theory-grounded investigation of phishing and pretext social engineering threats to information security*. *Journal of personality and Social Psychology*, 9, 1-27.
- Wolfgang, M. E. (1958). *Patterns in criminal homicide*. Philadelphia, PA: University of Pennsylvania Press.
- Wolfgang, M. E., & Ferracuti, F. (1967). *The subculture of violence: Towards an integrated theory in criminology*. London: Tavistock.
- Wright, J. P., Morgan, M. A., Almeida, P. R., Almosaed, N. F., Moghrabi, S. S., & Bashatah, F. S. (2017). *Malevolent forces: Self-control, the Dark Triad, and crime*. *Youth violence and juvenile justice*, 15(2), 191-215.

Wundt, W. (1874/1886). *Elements du psychologie, physiologique (2ieme tome)*. [Elements of physiological psychology, Vol. 2]. (E. Rouvier, Trans.). Paris: Ancienne Librairie Germer Bailliere et Cie.

Wüest, C. (2010). *The risks of social networking*. Symantec Corporation.

Xing, T., Sun, F., Wang, K., Zhao, J., Wu, M., & Wu, J. (2020). *Vulnerability to fraud among Chinese older adults: do personality traits and loneliness matter?* *Journal of elder abuse & neglect*, 32(1), 46-59.

Yadon, L. J., & Smith, R. B. (2011). *Old West Swindlers*. Arcadia Publishing.

Zaykowski, H. & Campagna, L. (2014). *Teaching Theories of Victimology*. *Journal of Criminal Justice Education*, 25:4, 452-467, DOI: 10.1080/10511253.2014.965410.

Zimba, A. (2017). *Malware-free intrusion: a novel approach to ransomware infection vectors*. *International Journal of Computer Science and Information Security*, 15(2), 317.

Zuckoff, M. (2005). *Ponzi's scheme: The true story of a financial legend*. Random House.

Zyda, M (2005). *From Visual Simulation to Virtual Reality to Games*. *Computer*, September 2005, pp. 25–32.

12. Annex

A. A Serious Game for Social Engineering Awareness Creation

(Published in: Journal of Cybersecurity Education, Research and Practice:
Vol. 2022 : No. 1 , Article 5.)

INTRODUCTION

The method of social engineering (SE) was initially defined as an instrument of politics to steer future social change and societal behavior (Popper, 1966). Nowadays, however, SE is rather connected to the exploitation of the human factor in cybercrime and defined as deceiving targets using psychological manipulation techniques (Rusch, 1999; Mouton, 2016; Bullée, 2017). Proofpoint (2019), in their *Human Factor Report*, highlight that almost 99% of cybercrime incidents that were surveyed among their global customer base in 2018 had exploited the human factor for the attack. Even for advocates of the human security dimension, this number seems to be somewhat propagandistically high. However, in a study that lasted for five years, researchers were physically penetrating the security systems of 1,000 banks, using human psychology to steal confidential data about customers. They were successful in 96.3% of the cases (Robinson, 2008). Verizon's (2021) most recent *Data Breach Investigations Report* also states that the majority of data breaches involve a human element. The 2020 Twitter hack also showed the dimension that social engineering attacks (SEAs) can have. Three cybercriminals used SE to hack around 130 Twitter accounts belonging to various politicians and celebrities for monetary gain (United States Department of Justice [DoJ], 2020). But SEAs not only pose risks to banks, politicians, and celebrities they also pose severe security threats to critical infrastructures, the organizations controlling them (Green et al., 2015; Ghafir et al., 2018), and basically to anybody with information that can be exploited by offenders for a financial gain or espionage purposes. It is therefore needless to say that approaches to the detection of and the protection against SE menaces are beneficial for ordinary people in their private lives, as well as for organizations in the public or private sector to keep critical information safe.

A promising approach for the education of people about the concepts and threats of SE is serious gaming (SG). Serious games are interactive, experiential learning tools that educate people about a specific topic in an entertaining way. The current study used an SG approach to evaluate participants' involvement and instruction compliance in three field observations. The findings of those observations were used to improve the game's administration and process before testing the approach experimentally in future research as a tool for reducing people's proneness to fall for SE.

The remaining paper is structured as follows: The following section reviews the origin of the SG vein in more detail, addressing its application in different domains and as a tool for SE awareness creation. Section 3 presents the purpose of the research. Section 4 describes the game's components and the gaming process used in the study. Sections 5 and 6 present the research data and method, as well as the corresponding results. In sections 7 and 8, the results are discussed and concluded before section 9 presents the limitations of the study and the aspirations for future research on the presented approach.

LITERATURE REVIEW

Serious games and SG are relatively new concepts, with serious games being perceived as *games that do not have entertainment, enjoyment, or fun as their primary purpose* (Michael & Chen, 2005, p. 21). Similarly, Vermillion (2017, p. 1) describes SG as being used *for purposes beyond entertainment*. This definition is widely accepted and is therefore the most current

designation within the evolution of the definition of the term (Djaouti et al., 2011). According to Djaouti et al. (2011), these definitions have all been derived from Sawyer and Rejeski (2002) who, with their white paper, paved the way to the current understanding of applying SG with technology for training and education. Further, the authors made a decisive contribution to the SG industry by inventing the Serious Game Initiative and serious gaming conferences such as the Serious Gaming Summit or Games for Health (Djaouti et al., 2011). The original heritage of the SG definition and the term's first usage dates to the 1970s. In his book *Serious Games*, Clark Abt (1970) describes the use of games for training and educational purposes and how decision makers of different domains in industry, government, education, and personal relations can be trained through those games (Abt Associates, 2020). Nowadays, serious games are commonly perceived to be virtual computer games and assumed to be limited to the digital sphere (Zyda, 2005; Rudman, 2019). Abt's (1970) definition, however, is rather open and does not relate to technology:

Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining. (Abt, 1970 p. 9)

The fact that serious games nowadays are commonly digital does not mean that SG is meant to be purely digital. A serious game presented by Jansiewicz (1973) for educating students about the mechanisms of United States politics provides a good reason why SG should not be seen as purely digital. Games that are played by incorporating human interactions are better suited to teach complex matters (Linehan et al., 2009; Jansiewicz, 2020). Moreover, interactive, experiential learning methods are ideally suited to assist participants in understanding implicit and subtle concepts, such as deception (Arcos & Lahnemann, 2019). Using an offline serious game as an interactive, experiential learning method to confront participants with the deceptive rationales of SE is therefore reasonable.

A Selective Review of Serious Gaming Application Domains

Serious games are applied in a broad range of domains, such as military, education, health care, communications, and politics (Djaouti et al., 2011). The first reported SG applications refer to the training of decision makers in industry, government, or education (Abt, 1970). Abt created different games, digital and nondigital, that were used by schools to educate pupils or by the military to train officers in Cold War simulations (Djaouti et al., 2011). Since then, the fields of application have widened and releases of serious games have accelerated (Djaouti et al., 2011). The continuous improvement in digital or virtual computer capabilities has contributed to this increase as well. The domains in which SG could be applied are almost limitless according to Abt's definition because such games are being built for educational and training purposes, fostering informed decision-making. The scope of application is open to almost every domain or industry where knowledge and awareness creation are needed to support people's understanding of principles, processes, and rationales. Scholars have used gaming to research human behavior in emergency scenarios and disaster communication, anti-terrorism training, engineering and information systems, health care, the military, environmental contexts, and policing contexts as well as to research the effect of gaming approaches in cybersecurity trainings. Table 1 provides a selective overview of literature from those domains with their respective academic contributors who either applied or discussed an SG approach as an educational experiential learning tool. The selection was made based on a contribution's relevance to the discussed topic and the academic fields of the authors. There are highlighted

authors who contributed more than one study. However, only the initial, most relevant study from a given author or group of authors was chosen to keep the selection concise.

Table 1. Selected domains of SG application in the academic literature

Domain	Academic Contributors
Disaster Communication	Haferkamp, 2011; Almeida et al., 2017
Anti-terrorism Training	Bruzzone, 2009; Sormani, 2016
Engineering and Information Systems	Vermillion et al., 2017; Kwak et al., 2019
Military	Garris et al., 2002; Zyda, 2005; Yildirim, 2010
Policing	BinSubaih, 2005; Bosse & Gerritsen, 2017; Sorace et al., 2018; Akhgar et al., 2019
Cybersecurity	Sheng et al., 2007; Cone et al., 2007; Newbould & Furnell, 2009; Arachchilage, 2013; Denning et al., 2013; Olanrewaju & Zakaria, 2015; Hendrix & Sherbaz, 2016; Beckers & Pape, 2016; Aladawy et al., 2018; Chothia et al., 2018; Frey et al., 2018; Goeke et al., 2019; Hart et al., 2020

Serious Gaming and Social Engineering

Serious games for SE are identified among other industrial or commercial training programs as solutions for cybersecurity (Aldawood & Skinner, 2019). The following paragraphs highlight foundational approaches that invented or further developed such gamified approaches. They present innovative means of instruction for the topic under discussion and different degrees of content of the SE rationales.

Anti-Phishing Phil

An early and seminal example of a gamified approach that tries to raise awareness for malicious SE techniques among players is the game Anti-phishing Phil (Sheng et al., 2007) developed at Carnegie Mellon University. It is an online game that teaches players ways to identify phishing

attacks. The researchers tested its effectiveness by evaluating a player's ability to spot fraudulent websites compared to the abilities of study participants who did not play the game. The researchers recruited 42 participants on campus who were split into three study groups. Although phishing is a very prevalent type of SE attack, it is only one attack vector in the malicious repertoire of social engineers.

Playing Safe

Another early gamified approach that made use of SG for awareness creation of SE threats was undertaken by Newbould and Furnell (2009). With a digital board game, they informed and educated players about the dangers of different SEA techniques. The authors performed a prototype test game with 21 players. Based on the players' self-evaluated level of awareness, the authors argue that the game helped to increase awareness of SE.

Social Engineering Awareness Game

In another approach, Olanrewaju and Zakaria (2015) tested their Social Engineering Awareness Game to see whether it improved information security awareness in a controlled laboratory experiment with 20 students. The game was conducted in a paper-based and prototype digital-based form. The players had to complete three levels during the game. A quiz section asked questions about SE. In a second step, players had to match pictures with definitions in a memory card game, and in a third step, real-life applications were tested. The researchers compared the performance of the paper-based game participants with that of the prototype digital-based game participants. Based on players' subjective perceptions, they conclude that the prototype game seems to be beneficial for SE awareness creation. Similar to the game of Newbould and Furnell (2009), however, their game also lacks the component of being interactive on the human level. Still, it is worth noting that SE is a concept of psychological manipulation and entails forms of direct or indirect human interaction.

A Serious Game for Eliciting Social Engineering Security Requirements

Beckers and Pape (2016) describe the invention of a tabletop serious game for SE awareness creation. They validated the approach in practical experiments with 27 university employees, with 3 to 4 players per experiment. The players took on the role of the social engineer and had to apply psychological principles of influence in combination with a suitable SEA technique to formulate an attack based on the playing cards they have drawn from the respective card deck (psychological influences and attack techniques). Those cards are then used to come up with a suitable SEA applied on a target person selected from a pool of different characters presented in a fictitious corporate environment. The fictitious corporate environment consists of an environment map, representing the corporate floor, and shows the offices of the fictitious target persons. The target persons are described using different attributes and skills, therefore leaving room to conduct different kinds of SEAs.

The suitability of the formulated attack is mutually evaluated by the players. The advantage of this approach is the active examination of the SE rationales and principles in a reflective and socially interactive way. A disadvantage of this offline tabletop approach is its scalability. Aladawy et al. (2018) and Goeke et al. (2019) developed an online version of the game and changed the player perspective from being a social engineer to being a SEA defender to train players' resistance against persuasion. Being put into a defending position correlates better with real-world scenarios (generally, most people would rather face situations where they must defend against SEAs than be an attacker themselves). However, research confirms that increased understanding and awareness creation about criminal processes and techniques can

be obtained from putting someone into the criminal's perspective (Wright & Bennett, 1990; Jacques & Bonomo, 2017).

A game that simulates SEAs will create awareness at the player's level, but it will also generate insights on creative SEA techniques invented by the players that could be prevented in future real-life situations. Thus, the game could be preventive through awareness creation and by preventively addressing future SEAs. Similar thoughts apply to the pedagogical layout of the game. Physical social interaction and the exchange of ideas during a tabletop game with a role-playing character provides valuable experiences to the players. Such a game can contribute positively to awareness creation, as well as to the knowledge creation process (Linehan et al., 2009; Jansiewicz, 2020). Offline role-playing games foster creativity and social skills (Karwowski & Soszynski, 2008; Chung, 2013; Dyson et al., 2015; Spinelli, 2018). SE is based on the exploitation of psychological triggers to manipulate victims. The means by which social engineers can manipulate the victims are therefore only limited by their creativity.

RISIKO

Most recently, Hart et al. (2020) further developed the approach of Beckers and Pape (2016). The researchers created a tabletop game that incorporates a more general view of aspects of cybersecurity and a larger variety of attack types. Hence, in their opinion, their game is educational and entails more than SE-related aspects. They proposed a tabletop game for increasing cybersecurity awareness among people in organizations without a technical background. The researchers evaluated the game in four experiments with a total of 54 participants, of whom 29 were students or recent graduates. Using a post-activity questionnaire, they asked participants about the perceived ease of use of the game, perceived usefulness of the game, and their intention to use any lessons learned.

SG approaches that specifically focus on SE rationales and concepts are rare. Different scholars have provided approaches that look only at single attack vectors of SEAs; have mostly applied the approaches in an academic, nonprofessional setting; and have often used online approaches without the possibility of direct human interaction. A tabletop offline gaming approach, however, seems to be reasonable to convey knowledge and rationales that are based on human psychology. Being put in front of a screen externalizes the human component and makes it more intangible again. We, therefore, find it reasonable and beneficial to use an offline tabletop game that lets players directly interact with each other and learn about rationales that are based on social interactions. The SG approach that is used in the study at hand resembled that of Beckers and Pape (2016) because it is a full offline SG tabletop approach, is socially interactive, and specifically focuses on SE.

RESEARCH PURPOSE

The current study explores the application of an SG approach as described in the previous section. The purpose of this study is to observe participants' game involvement and instruction compliance and to derive administrative and procedural improvement potentials before testing the game's effectiveness as an experiential learning tool experimentally in further studies. Moreover, the study seeks to broaden the research field by specifically focusing on a business environment. Prior research, as mentioned in section 2.2, applied such approaches only to a very limited extent in professional settings. The discovery of practical implications for the applicability of an SG approach for SE in the business environment provides added value. Thus, the research objectives that were assessed by this study are as follows:

Observe participants' involvement with the game throughout the playing process.

The first objective of this study was to observe participant engagement throughout the game and whether the game content as well as the game procedure catches their attention.

Observe and evaluate participants' compliance with the instructions given by the game masters and game material.

A second goal of this study was to observe specifically the compliance of players with the instructions given by the game masters and the game material, as these are the direct connecting points in conveying the topic and the rationales of SE to the players.

Observe other relevant findings that could be identified throughout the events.

We wanted to leave room in our research approach to insights that evolve in the course of an interactive SG approach that are beyond the primary focus but would improve the quality of this instructional approach. Based on the research objectives, the research questions that were subject to this study are as follows:

RQ1: Are there game improvement potentials?

With *improvement potentials* we mean any change in the administrative or procedural design of the game that would help to foster participants' engagement, satisfaction, and interpersonal interactions during the game. Prior research suggests that specific introductory material might assist players from a broader background in more easily engaging with the rationales and purpose of the game (Beckers & Pape, 2016). Moreover, interpersonal interaction is a key element of the SG approach (Beckers & Pape, 2016; Hart et al., 2020). Sample sizes that are significantly larger than those in the aforementioned studies might expose improvement potentials in the dimension of interpersonal interaction.

RQ2: Do game masters take on an essential role for participants' performance and their instruction compliance during the game?

Prior research has shown that the role of the game master is relevant to the overall success of a game. Hart et al. (2020) state that game masters have a *focal role* in engaging the participants and making the game fun. Game masters motivate players, guide the game process, and ensure the procedural sequence of the game (Beckers & Pape, 2016). Facts that qualify for an investigation of the role of the game master are also addressed in the study at hand.

GAME DESCRIPTION

The following section provides an overview of the game process and its components as it was applied in the three samples. The approach resembled the one taken by Beckers and Pape (2016).

Game Process

We have chosen to start the game with a short 5-to-10-minute introduction presentation about the topic of SE, as well as about the purpose and rationales of the game, as done by Beckers and Pape (2016). The game then starts and lasts for one or two iterations. The game is led by one game master per game table, and each game table consists of three to four teams with two to three players per team. In each iteration, the teams must create a suitable SEA based on the given game material. It consists of a situation plan for a fictitious company (office); a set of fictitious employee profiles, where each employee is characterized by position, computers

skills, and strengths and weaknesses; and an attack plan sheet that guides the players through the process. Additionally, the game set consists of two stacks of cards. One set covers the principles of influence of social psychology, which are the foundation of SE deception techniques for building trust. The second set incorporates different SE attack vectors. Every card from either stack has a precise description. This process helps players familiarize themselves with the concept of SE.

After an initial familiarization phase of about 10 minutes with the situation plan and the fictitious employees, each team draws three cards from both of the stacks. The teams now receive their attack plan sheets where they have to formulate a reasonable SEA, and they will again have about 10 minutes available. The aim is to formulate an attack that applies a reasonable combination of a compliance principle with an attack vector on a suitable target person to exploit a formulated target asset, for instance, access to the CEO's office or access to specific financial information. Based on the cards they have drawn, there will be more or less suitable attack options that they will have to evaluate themselves. In the next phase, the teams will present their formulated attacks to the other teams at the game table. For the presentation, each team is allotted around 5–7 minutes. Each presenting team is evaluated by the other (evaluating) teams based on a predefined point scale. The evaluating teams have the ability to propose attack improvements to gain bonus points. Thus, the point rating acts as a proofing instrument, showing whether the concepts have been understood, correctly. Once this is completed, another iteration can be played. The team that accumulates the most points over the two rounds will be the winner of the game. Although winning is not the sole purpose of the game, its playful character is meant to engage participants with the concepts.

Game Components

The game material generally consists of a fictitious corporate situation plan, a description of the different target persons (employees), an attack plan sheet, and two stacks of playing cards (see also annex B).

Fictitious corporate situation plan: First, the game contains a fictitious corporate situation plan. In the setting at hand, the situation plan reflects an office environment. The situation plan also accounts for the fact that SE attacks can be executed physically by the means of person-to-person contact or digitally by using technological means.

Target persons: A second crucial component is the set of fictitious target persons. Each person is characterized by a different corporate function and personal characteristics, strengths and weaknesses, interests, and computer skills. The game is meant to help participants understand the characteristics of the fictitious target persons that could be exploited in SEAs.

Attack plan sheet: The attack plan sheet guides the players through the game process. It provides the participants help on how to structure their attack and how to use the game material. Moreover, the attack plan sheet entails examples for each component to foster the familiarization process.

Compliance principles cards: The concept of SE is based on psychological principles of persuasion or influence to deceive targeted persons and make them comply with a request. Those compliance principles can be authority, reciprocity, or social proof, for example (Cialdini, 2021). The playing cards are meant to help the participants understand the different ways that the cards could be used in SE, such that participants can better detect and protect themselves against targeted attacks.

Attack vector cards: Additionally, there are attack vector playing cards. It is important for the participants to understand that SE attacks can take on various forms, for instance, phishing or

tailgating. This knowledge will help participants better detect SE attacks and protect themselves against them.

DATA AND METHODOLOGY

The current study was conducted using a qualitative research approach that included field observations and unstructured field interviews. It was intended to produce ethnographic knowledge about the behaviors and social interactions of the participants during the game. Field observations are well suited for drawing conclusions about specific conditions and behaviors in a natural setting (Maxfield & Babbie, 2017). As Hochstetler and Copes (2016) say, qualitative research provides context to the topics under investigation. Field observations provide the opportunity to generate depth and free-flowing participant responses.

The researchers' positions took on different forms in the study. They were either full participants administering the game as a game master or were full participant observers. Either position had its benefits and limits. Whereas the full participant position provided the researchers the opportunity to interact with the participants and collect firsthand insights, there was a risk that immediate involvement would influence the researchers' assessment of participants' behaviors and perceptions. The position as a full participant observer was better suited to avoid selective perception from the researchers, but it also limited the researchers' direct interaction with the participants. To balance the benefits and limits of those stances, the researchers took on positions that complemented each other in all observations such that both positions were filled in either of the observations. We used the SG approach of Beckers and Pape (2016) to assess the research objectives and research questions. However, in contrast to aforementioned researchers, our approach was administered by game masters who were each in control of a game table with three to four teams and two to three players per team and table. Each of the teams was asked to create a SEA based on the information and game material provided by the game master. The game material consisted of an attack plan sheet that helps the players to navigate through the game, a floor plan of a fictitious company with fictitious employees as target persons, a description sheet that characterizes the target persons, and SE deception principle and SE attack vector playing cards. At the end of a game iteration, the teams mutually evaluated each other's SEAs and in doing so further fostered their reflection on and understanding of the subject in an interactive way. Additionally, game masters were provided a game master instruction cheat sheet in advance of a game (see annex B for an exemplary extract of the game material and game structure, as well as the game master cheat sheet).

Data and Data Collection

Between December 2019 and February 2020, we observed a heterogenous group of 97 professionals in three independent observations. The sample population consisted of practitioners of various industries and professions. The participants represented different Swiss companies or Swiss affiliates of international companies from the telecommunications, technology, and energy industry from Swiss and international advisory firms, law and cybersecurity firms, and information technology (IT) apprentices of a Swiss governmental defense organization. Overall, the sample population reflected a pronounced degree of heterogeneity in terms of the sectors, industries, professions, and life and professional experiences represented. Participants were between 16 and 20 years old for IT apprentices and up to around 55 years old for senior professionals. The gender ratio was 11 female to 86 male participants; they were consultants, finance or marketing specialists, lawyers, key account managers, and management personnel. The sample was recruited by using the researchers'

professional networks, pursuing a purposive sampling path of opportunity. Table 2 provides a summary of the sample characteristics.

Table 2. Summary of general sample characteristics

Sample	Date	Place	Sector	Industry	Sample Size
1	05.12.2019	Zürich, CH	Private	Consumer electronics, telecommunications, and crisis management	9
2	05.12.2019	Zürich, CH	Private	Telecommunications, advisory, technology, energy, law, and cybersecurity	83
3	13.02.2020	Bern, CH	Public	Defense	5

Each sample was exposed to the game independently, at different times and places, to collect the data. The observations were conducted in a workshop-style format on the premises of the respective host organization. The observations lasted for two hours in samples 1 and 2 with one game iteration. The observation in sample 3 lasted for four hours because in sample 3, the researchers decided to conduct a two-iterations game to study the effects that two iterations would have on the considerations stated in the objectives. Sample 1 and sample 2 were conducted in the afternoon, whereas sample 3 was a full morning workshop with a 15-minute break between the iterations. Each of the observations took place in a climatized room with conference tables and chairs organized for the grouping of three to four teams per table and two to four participants per team. Sample 3 was organized into three teams with two participants per team, but one participant had to leave the game during the second iteration due to an urgent professional obligation. For sample 2, the researchers were assisted by voluntary game masters who were briefed on the game and their task as game masters in advance of the observation.

The data produced were collected and recorded through note-taking during the games and by transcribing the content of the unstructured interviews to a Microsoft Excel data bank after the respective observations. The interviews did not follow a predefined structure but were discussions between the researchers and individual participants about their experiences and perception of the game. The researchers nevertheless asked all interviewees about their evaluation of the game's attractiveness and possible improvement proposals for the game. Besides that, free-flowing comments from the interviewees were collected. Note-taking took

place through both the researchers and the participants. Whereas the researchers took notes to directly record anything that related to the research objectives, the participants took notes with respect to the game proceedings on the provided attack plan sheets (see annex B) that were collected by the researchers from the teams after the game's conclusion. The sheets were used to record additional data and insights for the research objectives while representing a standardized reporting tool across the samples. All collected data were recorded in a Microsoft Excel data bank for each sample, with a structure presented in annex A.

Method of Analysis

Data were collected by the means of observing participant behavior, gathering feedback through unstructured interviews, and recording the respective data through note-taking. Additionally, the attack plan sheets that had to be filled out by each team in each sample of the game proceedings were collected. In a deductive process, familiarization with and a first screening of the collected data was performed. Deductive coding processes are categorized by analyzing data with respect to a predefined list of codes (Miles et al., 2013). The predefined categories of interest in the study at hand referred to the research objectives presented earlier and related to participants' game involvement, their instruction compliance, and other relevant findings. Data were allocated in the predefined categories afterward. Moreover, categorizing patterns of data aided in the further identification and coding of subthemes. To illustrate the findings, we present a table of the categories, the identified coded subthemes, and relevant examples (see table 3 in the results section). Further, we have used verbatim quotations from the unstructured interviews to present response categories with the number of an interviewee and the interviewee's industry mentioned in brackets (e.g., (20; defense)). Each theme was analyzed to gain a deeper understanding of participants' perceptions of the game and gaming behaviors to help answer the research questions.

RESULTS

The findings indicate that there are several procedural and content-related improvement potentials to make the approach more participant centric and knowledge conveying so that the game can be a promising instructional tool for SE awareness creation. Table 3 hereafter illustrates the structure of the derived findings.

The analysis of the data shows that there are specific themes that appeared repeatedly among the participants in either the observations or the unstructured interviews that would be categorizable under either of the three research objectives. The coded subthemes have been presented because they represent in a good way what was important for the research, namely whether the observations and unstructured interviews would expose improvement potentials concerning the level of engagement, satisfaction, and interaction among the participants and their compliance with instructions during the game.

Table 3. Categories of interest, coded subthemes, and examples

Category	Subtheme	Example
<p>Game involvement</p>	<p><u>Game material</u></p>	<p>Familiarization ease, language, game material usage, and improvement proposals</p>
	<p><u>Teamwork</u></p>	<p>Within and among teams, directive, authoritative, and cooperative</p>
	<p><u>Active participation</u></p>	<p>Discussion intensity, voluntary comments, and call for participation</p>
	<p><u>Understanding rationales</u></p>	<p>Poorly completed attack plan sheets, messy SEA creation, and usefulness of compliance principles</p>
	<p><u>Environmental factors</u></p>	<p>Room appropriateness, population size, noise, time constraint, and team grouping</p>

<p>Instruction compliance</p>	<p><u>Game material</u></p> <p><u>Game master ability</u></p> <p><u>Presentation of attack</u></p>	<p>Game material usage in way of order and attack plan sheet completion</p> <p>Participants asked for clarifications, discussions out of context, and lack of introduction and control</p> <p>Explaining the situation and used methods, conveying rationales, and attack improvement proposals</p>
<p>Other findings</p>	<p><u>Deviant behavior and thoughts</u></p> <p><u>Information overload</u></p>	<p>Theft of game material and pronounced deviant considerations</p> <p>Not using game material properly, poorly completed attack plan sheets, and attack plan improvement proposals being too demanding in one iteration</p>

Game Involvement

It appeared that participants' involvement with the game differed within the samples and among the samples. Based on the researchers' observations and the feedback gathered from the participants, several findings have been derived. In particular, there are some suggestions to improve the game proceedings and the game material. Interviewees mentioned the following:

This was an interesting and educational event. One suggestion for the game from my side would be an introduction sheet at the beginning of the game to better familiarize the participants with the game's rationale. Moreover, a sociogram that captures exploitable social relationships among the target persons could be a nice extension. (2; crisis management)

In my opinion, a more profound introductory presentation would have been beneficial for a general familiarization with the topic. (5; telecommunications)

The game should be digitized to scale it and make it more accessible. (12; advisory)

The game was really fun, and we could administer it in our company as well. The only problem I had was with the game material, as I am not perfectly fluent in English. (19; energy provider)

The sociocultural behavior of participants within their teams, among teams, and toward the game masters was observed to be heterogenous as was the overall demography of the population in each sample. When there was a diverse demography in terms of gender, age, education, profession, and extent of professional experience, participants with a higher education and participants who seemed to be more open and extraverted dominated the discussions within the teams and among the teams. When the demographic distribution among the participants was rather homogenous, a compliant and cooperative working style within the teams and a more directive, authoritarian working style with less cooperation but a high degree of competitiveness was observed among the teams. Although professional and life experiences seemed to be linked positively with active participation, once younger participants were invited to participate, they provided valuable feedback for the researchers in terms of personal involvement:

This game was fun and educational. I guess, I learned more in this half day than in the last couple of months in vocational school. (20; defense)

Oh, we already have a break? I did not recognize the time passing by. (21; defense)

Another important factor for the effectiveness of the approach is participants' involvement with the underlying rationales. The analysis of the teams' attack plan sheets and the data collected from each team's attack presentation suggest that participants' understanding of the basic principles underlying this SE approach should be guided:

The case study and the presentation of the social engineering principles really helped me to better grasp the game's rationales. (11; technology provider)

Another participant's feedback does, however, show that an introductory presentation is no guarantee for the comprehensibility and the conveyance of the game's underlying principles and rationales:

I did not find the compliance principle cards of psychological manipulation helpful and would abandon them from the game. (24; defense)

For a freer-flowing attack formulation without a scientifically proven framework of psychological principles, this request would be feasible. Psychological principles of interpersonal influence are, however, fundamental for SEAs and therefore should be well integrated within a game that intends to convey awareness about SE rationales.

Lastly, the analysis of the data hints at the fact that specific environmental factors play an important role in participants' involvement with the game. In two of the three samples, the population sizes ranged within 5–9 participants, which was administratively easier to handle than a population size of 83. But this somewhat opposing study condition also revealed limitations to the operability of the approach. An increasing population size not only requires more game masters but also asks for specific logistic prerequisites, such as room size or room climatization for the participants to stay focused. If such conditions are not met, participants may get distracted and annoyed by noises, heat, or a lack of space, which would negatively impact their involvement with the game:

The tight seating and grouping of game tables was not that comfortable, as it was hard to always get what the others at the table were saying with the noise behind my back. (11; technology provider)

The room was almost too small, as it has become too noisy. (13; advisory)

Instruction Compliance

Based on the collected data, the findings suggest that participants enjoyed the game but sometimes had trouble with following the game instructions. The attack plan sheets to be filled out provided a unified measure among each sample and team to review participants' compliance to the overall instruction of using the game material to create a reasonable SEA, respecting the components and rationales of SE. It was intended that participants would familiarize themselves with the concepts and rationales and think through their SEA approach by filling out the sheet. The attack plan sheet contained specific examples per each step and acted as a guide for the participants. In total, we have analyzed 27 attack plan sheets for the participants' instruction compliance in filling them out as demanded. The findings show that most of the teams sporadically completed the sheets in note form and that others did not even complete them:

I did not see any use in completing the attack plan sheet. We rather enjoyed discussing the things. (7; telecommunications)

Although discussing the rationales and principles of the game with the team members is an essential part of the familiarization and awareness creation process, it is vital to follow the structure of the attack plan that replicates the underlying procedural principles of SE. If these structures are not respected, the game reflects an interactive and fun event with discussions about the topic but does not get down to the point that SEAs are accurately planned, as well as precisely and purposefully executed. Building on this, another focal finding in terms of participants' instruction compliance refers to the game master's ability. Discussions out of context, participants asking for clarification, or a game master who was too passive were signs of an ineffectively administered game table. The game master's primary role is to explain to the participants the game material, the goal of the game, and the information they need to process and to effectively guide participants through the structure of the game. In this sense, it was observed that not all game masters possessed this authoritative but permissive nature to effectively guide the participants through the framework of the game while leaving room for nourishing discussions:

Although I generally liked the game, it was not perfectly administered and the introduction to the game material could have been more extensive. (15; technology provider)

I liked the approach, but it was a lot of information, and it would have been beneficial if the game master more strictly guided through the process. (17; telecommunications)

Lastly, a good overall indication of whether the participants stuck to the instructions were the SEA presentations of the teams at the end of each game iteration. In samples 1 and 3, the

researchers witnessed all the presentations personally while in sample 2, the researchers listened to random samples of SEA presentations and also asked the respective game masters about how participants put the instructions into practice. The findings were that most participants grasped the essential idea of the game and its instructions but struggled with the detailed implementation of the rationales and structure of a SEA. The analysis of the attack plan sheets mentioned above supports this finding. Some presentations indeed showcased detailed considerations but not in terms of an in-depth application of SE principles, and not many of the attack plan sheets reflected this either.

Other Findings

The analysis of the data revealed two other important findings besides those that can be directly allocated to either the participant involvement or the instruction compliance category. First, deviant tendencies were observed and recorded for two of the three samples. In sample 2, the game revealed a deviant behavior by one of the participants who purposefully took the property of the researchers. Similarly, in sample 3, one participant exposed deviant thoughts during the game that were unsettling and an expression of a well-thought-through plan rather than the correct application of the game's rationales and principles. During the proceedings of the game, the researchers asked the participants how they were doing with their brainstorming and whether they had already come up with an idea for an attack. One participant answered as follows:

Yes, we could poison the assistant's cat, such that she has to go to the doctor's, and we can take advantage of her not being present in the office... Then we would smash the windows in the office to gather access to her office... These are things I already made up when I was 14 years old... (24; defense)

Second, the analysis of the data revealed that the gaming approach contains a large amount of information to be processed by the participants. Time constraints and a one-iteration game structure seemed to particularly impact participants' satisfaction with and receptivity to the game:

I enjoyed the game and could imagine replicating it in our company. However, I would propose to have different levels of complexity and more time available, as it were a lot of information to be processed. (17; telecommunications)

The game was educational and fun. I wished to have had more time available to play a second iteration. (10; cybersecurity)

DISCUSSION

To the best of our knowledge, this is the first study in criminology that applied SG for SE and looked for improvement potentials to make the serious game more effective as an educational tool based on field observations. However, there have been studies outside criminology that used a similar approach. Beckers and Pape (2016) performed experiments to test the effectiveness of an SG approach for SE awareness creation and further developed the approach to create an online version of the game (Aladawy et al., 2018; Goeke et al., 2019). The initial approach, however, was not further evaluated for improvement potentials. We think that the results of the three field observations support the view that the interactive and interpersonal character of an offline tabletop game approach is well suited to foster knowledge and awareness of the creation process among the participants and that several game improvements are possible to enhance this process. Hart et al. (2020) used an offline tabletop SG approach for cybersecurity awareness and education for people with no technical background. Although their approach does not specifically focus on SE and features other content in terms of game material,

the administrative design resembles the one used in this research study. In accordance with our findings, they conclude that the game master takes on a *focal role in stimulating active learning* and thus fosters the degree of participant involvement with the game. For the overall improvement of the approach in terms of participant involvement, instruction compliance, and consistent pedagogical quality, the importance of the game master should not be underestimated.

Analysis

Based on the findings, we derived two improvement dimensions: the game material and the game process. Each dimension can be improved in the following areas: the briefing, the level of complexity, and other. Eventually, we propose the following adaptations for the game. First, to increase participants' involvement and instruction compliance, it is essential that players are briefed more thoroughly. In the game, we followed the approach of Beckers and Pape (2016), who gave a short introduction to their game. Obviously, this practice is not sufficient. We therefore see a need to prepare the players better at the beginning of the game. This will be achieved by conducting a stimulating SE introductory presentation and by providing an introductory sheet at the beginning of the game. Moreover, game masters need to be more comprehensively briefed because we can confirm that they play a *focal role* in the game (Hart et al., 2020). Second, it seems to be beneficial for the awareness creation process and for the reduction of information overload to apply an increasing level of complexity by adding different levels of difficulty during the game process. This implies that, ideally, the game process should encompass more than one iteration, and in the second iteration, players will be provided a sociogram of the target persons as an additional layer of difficulty. Further, they will only be given the ability to propose attack improvements during the mutual evaluation phase in the second iteration. Table 4 summarizes the key improvements discovered during the field observations.

Table 4. Summary of key improvement potential applications for the serious game

Dimension/Area	Briefing	Complexity Level	Other
Game Material	Provision of introductory sheet	Provision of sociogram for target persons in second iteration	
Game Process	Stimulating introductory presentation	Two iterations approach. Mutual attack improvement proposals only in second iteration.	Comprehensive training of game masters

LIMITATIONS AND FUTURE RESEARCH

The study at hand evaluated the participants' engagement and satisfaction with SG for SE awareness creation in a business environment. The study was a pilot project that seized the opportunity to conduct observations in the business environment, which is hard to achieve and an added value. It provided the opportunity to apply the game in a naturalistic setting in the field and to gather practical knowledge about its purpose, which is to help organizations increase SE awareness among their employees. Although we properly prepared and executed the study, there are methodological limits given the fact that the study was set up in a very short period. We were supposed to implement the insights from this study in the methodological setup of further observations in the field during 2020/2021 with organizations that had confirmed their cooperation for it. Unfortunately, due to the COVID-19 pandemic, these field studies have not taken place so far. We, nevertheless, decided to publish the study at hand because we are convinced that the study bears valuable and shareable results.

The outcome of the study at hand will be used for the improvement of the respective SG approach. It will be applied as an operational framework in a randomized controlled trial research design that tests the serious game's effectiveness as an educational tool to reduce participants' proneness to fall for SE's influencing techniques. Simultaneously, the research design aims to control for personality differences and different methods of instruction.

Further, we will pursue aspirations to adapt the game's content, in particular the target person descriptions and the corporate environment sheet, to a version appropriate for educating intelligence officers. Based on feedback received from the intelligence community, we see a potential to tailor the game to the needs of educating intelligence personnel about the power of social psychology in influencing situations.

Moreover, even though offline interactive educational tools might be the purest form of social interaction, they are not suited for pandemics, as COVID-19 has taught us. The authors therefore aspire to create a technology-assisted gaming approach. However, we still believe that social interaction during such a game is key for the process of SE awareness creation.

CONCLUSION

This article presented an evaluation of an SG approach as an interactive, experiential learning tool for SE awareness creation. Through three field observations with a total of 97 participants, insights on possible improvements for the applied SG approach were derived. Besides pure sociodynamic observations, it was possible to identify valuable insights on how to adapt the layout and the administration of the serious game to make it more accessible, less generic, and hopefully, effective in raising awareness among the participants about the rationales and techniques of SE. Moreover, in two of the three samples, the researchers observed deviant behavior and thoughts. However, this observation does not mean that those people tend to be criminals outside the game setting. Still, this specific observation was nevertheless unsettling to the researchers and thus was worth reporting on. Generally, we have learned that research in the business environment bears challenges that should be respected in the methodological setup. We, nevertheless, gathered valuable insights for future studies. This study does not provide insights on the SG approach's ability in improving responses to SEA. But it does add value to the **ABC** of cybersecurity. The observations and participant feedbacks that were collected during the study do not only help to improve the gaming approach, but they also showed that it

is a reasonable approach to create Awareness for SE. Whether it can help change people's Behavior in real-life SE situations and create a SE resilient Culture is yet to be tested.

This game was fun and educational. I guess, I learned more in this half day than in the last couple of months in vocational school. (20; defense) Although this statement is subjective and should be treated carefully and neither reflects the quality of the school nor of the serious game, it nevertheless indicates that the SG approach was impressive, was fun, involved the participants in the game, and made people aware about SE threats and rationales.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

NOTES

REFERENCES

- Abt Associates (2020). Biography of Clark C. Abt. Retrieved January 6, 2020, from <https://www.abtassociates.com/who-we-are/our-people/clark-c-abt-phd>.
- Abt, C.C. (1970). *Serious Games*. University Press of America.
- Akhgar, B., Redhead, A., Davey, S., & Saunders, J. (2019). Introduction: Serious Games for Law Enforcement Agencies. In: Akhgar B. (eds) *Serious Games for Enhancing Law Enforcement Agencies*. Security Informatics and Law Enforcement. Springer, Cham.
- Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In: Furnell S., Mouratidis H., Pernul G. (eds) *Trust, Privacy and Security in Digital Business*. TrustBus 2018. Lecture Notes in Computer Science, vol 11033. Springer, Cham.
- Aldawood, H., & Skinner, G. (2019). A Taxonomy for Social Engineering Attacks via Personal Devices. *International Journal of Computer Applications* (0975 – 8887) Volume 178 – No. 50, September 2019.
- Almeida, J. E., Rossetti, R. J. F., Jacob, J. T. P. N., Faria, B. M., & Leça Coelho, A. (2017). Serious games for the human behaviour analysis in emergency evacuation scenario. *Cluster Computing*, 20(1), 707-720.
- Arachchilage, N.A.G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706{714.
- Arcos, R., & Lahnemann, W.J. (2019). *The Art of Intelligence. More Simulations, Exercises and Games*. Security and Professional Intelligence Education Series (SPIES). Series Editor: Jan Goldman. The Rowman & Littlefield Publishing Group, Inc.
- Barber, R. (2001). Social engineering: A People Problem? *Network Security*, 2001, Vol.2001(7), pp.9-11.
- Beckers, K., & Pape, S. (2016). A Serious Game for Eliciting Social Engineering Security Requirements. 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, 2016, pp. 16-25.
- BinSubaih, A., Maddock, S., & Romano, D.M. (2005). Comparing the use of a tabletop and a collaborative desktop virtual environment for training police officers to deal with traffic accidents: Case study. *International Conference on Engineering Education*, July 25–29th, Gliwice, Poland, Volume 2, pp. 94–100.
- Bosse, T., & Gerritsen, C. (2017). Towards Serious Gaming for Communication Training - A Pilot Study With Police Academy Students. Paper presented at the 8th International Conference on Intelligent Technologies for Interactive Entertainment, Utrecht, the Netherlands, 28–30 June 2016.
- Bruzzo, A., Tremori, A., & Massei, M. (2009). *Serious games for training and education on defense against terrorism*. Italy: Defense Technical Information Center.
- Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P.H. (2017). On the anatomy of social engineering attacks - A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 2018, pp.urn:issn:1544-4759.
- Chothia, T., Paiu, S. I., & Oultram, M. (2018). Phishing attacks: Learning by doing. In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).
- Chung, T.S. (2013). Table-top role playing game and creativity. *Thinking Skills and Creativity*, 8 (2013), pp. 56-71.
- Cialdini, R.B. (2021). *Influence, New and Expanded: The Psychology of Persuasion*. Harper Business; Expanded ed. Edition (4. Mai 2021).
- Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. *Computers & Security*, 26(1): 63–72.

- Denning, T., Lerner, A., Shostack, A., Kohno, T. (2013). Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. *Proceedings of the ACM Conference on Computer and Communications Security*. 915-928. 10.1145/2508859.2516753.
- Djaouti, D., Alvarez, J., Jessel, J. P., & Rampnoux, O. (2011). Origins of serious games. *Serious games and edutainment applications* (pp. 25–43). London: Springer.
- DoJ (2020). Three Individuals Charged For Alleged Roles In Twitter Hack. United States Department of Justice, DoJ, 31st July 2020. <https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack>.
- Dyson, S.B., Chang, Y.-L., Chen, H.-C., Hsiung, H.-Y., Tseng, C.-C., & Chang, J.-H. (2015). The effect of tabletop role-playing games on the creative potential and emotional creativity of Taiwanese college students. *Thinking Skills and Creativity* 19 (2016) 88–96.
- Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, 45(5), 521-536. [8194898]. <https://doi.org/10.1109/TSE.2017.2782813>
- Garris, R., Ahlers, R. & Driskell, J. E. (2002). Games, Motivation and Learning. Research and Practice Model. In: *Simulation & Gaming*, 33. Jg., H. 4: Newbury Park (USA): Sage Publications, S. 441-467.
- Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, 74(10), pp.4986-5002.
- Goeke, L., Quintanar, A., Beckers K., & Pape, S. (2019). PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. Conference: Computer Security - ESORICS 2019 International Workshops, MSTEC 2019, Luxemburg, September 26-27, 2019.
- Green, B., Prince, D., Busby, J. & Hutchison, D. (2015). The impact of social engineering on Industrial Control System security. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy* (pp. 23-29).
- Haferkamp, N., Kraemer N.C., Linehan C., & Schembri, M. (2011). Training disaster communication by means of serious games in virtual environments. *Entertainment Computing* 2 (2011) 81–88.
- Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security* 95 (2020) 101827.
- Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training? *International Journal of Serious Games*. 3(1).
- Hochstetler A. & Copes H. (2016). Qualitative Criminology's Contributions to Theory. In: *The Handbook of Criminological Theory*, First Edition. Edited by Alex R. Piquero. 2016 John Wiley & Sons, Inc. Published 2016 by John Wiley & Sons, Inc.
- Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' Perspective on Crime Prevention. In: LeClerc B., Savona E. (eds) *Crime Prevention in the 21st Century*. Springer, Cham.
- Jansiewicz, D. R. (1973). *The New Alexandria Simulation: A Serious Game of State and Local Politics*. Canfield Press.
- Jansiewicz, D. R. (2020). The Game of Politics - Frequently Asked Questions. Retrieved January 6, 2020, from: http://gameofpolitics.com/f__a__q_.htm.
- Karwowski, M., & Soszynski, M. (2008). How to develop creative imagination? Assumptions, aims and effectiveness of role play training in creativity (RPTC). *Thinking Skills and Creativity*, 3 (2008), pp. 163-171.
- Kwak, D.-H., Ma, X., Polites, G., Srite, M., Hightower, R., et al. (2019). Cross-Level Moderation of Team Cohesion in Individuals' Utilitarian and Hedonic Information Processing: Evidence in the Context of Team-Based Gamified Training. *Journal of the Association for Information Systems*; Atlanta.
- Linehan, C., Lawson, S., & Doughty, M. (2009). Tabletop Prototyping of Serious Games for 'Soft Skills' Training. Coventry, UK: 2009 Conference in games and virtual worlds for serious applications.
- Maxfield, M., & Babbie, E. (2017). *Research Methods for Criminal Justice and Criminology* 8th Edition. Wadsworth Publishing.
- Michael, D., & Chen, S. (2005). *Serious Games: Games That Educate, Train, and Inform* (1er ed.). Course Technology PTR.
- Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative data analysis: A methods sourcebook*. Thousand Oaks, CA: SAGE Publications, Incorporated.
- Mouton, F., Leenen, L., & Venter, H.S. (2016). Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security*, Jun 2016, Vol.59, p.186.
- Newbould, M., & Furnell, S. (2009). Playing Safe: A Prototype Game For Raising Awareness of Social Engineering. *Proceedings of the 7th Australian Information Security Management Conference*.

- Olanrewaju, A.-S. T., & Zakaria, N.H. (2015). Social Engineering Awareness Game (SEAG): An Empirical Evaluation Of Using Game Towards Improving Information Security Awareness. Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015 11-13 August 2015 Istanbul, Turkey.
- Popper, K.R. (1966). *The Open Society and Its Enemies*. (Princeton University Press, Princeton, New Jersey, fifth edition, 1966).
- Proofpoint, Inc. (PFPT) (2019). Human Factor Report 2019. Retrieved December 16, 2021, from: <https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more>.
- Redpath, S. M., Keane, A., Andrén, H., Baynham-Herd, Z., Bunnefeld, N., Duthie, A. B., & Travers, H. (2018). Games as Tools to Address Conservation Conflicts. *Trends in ecology & evolution*, 33(6), 415-426.
- Robinson, J. (2008, September 9). Researchers dupe banks with heists without holdups. *Arizona Republic*, p. D5.
- Rudman, S.A. (2019). Serious games to study the influence of wildlife devaluation strategies on hunter behaviour. A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Master of Science. Victoria University of Wellington, 2019.
- Rusch, J. (1999). *The Social Engineering of Internet Fraud*. United States Justice Department – Proceedings of the 1999 Internet Society Conference.
- Russell, C.K. (2005). A taxonomy of serious games for education in the healthcare professions. In Proceedings of NMC Online Conference on Educational Gaming.
- Sawyer, B., & Rejeski, D. (2002). *Serious Games: Improving Public Policy Through Game-based Learning and Simulation*. Woodrow Wilson International Center for Scholars.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007). “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish”, in Proceedings of the 2007 Symposium On Usable Privacy and Security, Pittsburgh, PA, 18-20 July 2007.
- Sorace, S., Quercia, E., La Mattina, E., Charalampos, Z. Patrikakis, L., Bacon, G., & Mackinnon, L. (2018). Serious Games: An Attractive Approach to Improve Awareness. *Community-Oriented Policing and Technological Innovations*.
- Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I., et al. (2016). A serious game empowering the prediction of potential terrorist actions. *Journal of Policing, Intelligence and Counter Terrorism*, 11(1), 30.
- Spinelli, L. (2018). *Tabletop Role-Playing Games and Social Skills in Young Adults*. Honors College Theses. 192.
- Stapleton, A. (2005). Game issue report. Korea IT Industry Promotion Agency, Serial No. 25.
- Verizon Communications Inc. (2021). DBIR 2021 Data Breach Investigations Report. Retrieved December 16, 2021, from: <https://www.verizon.com/business/resources/reports/dbir/>.
- Vermillion, S. D., Malak, R. J., Smallman, R., Becker, B., Sferra, M., & Fields, S. (2017). An investigation on using serious gaming to study human decision-making in engineering contexts. *Design Science*, 3.
- Wright, R., & Bennett, T. (1990). *Exploring the Offender’s Perspective: Observing and Interviewing Criminals*. In: Kempf K.L. (eds) *Measurement Issues in Criminology*. Springer, New York, NY.
- Zyda, M (2005). From Visual Simulation to Virtual Reality to Games. *Computer*, September 2005, pp. 25–32.
- Yildirim, S. (2010). Serious game design for military training. In *Games: Design and Research Conference*, Volda University College (pp. 3-4).

B. Serious Game Material

B.1 Serious Game Script

Social Engineering War Gaming: Game Play

1. Draw Cards

- a. Each team draws one card from the set COMPLIANCE PRINCIPLES. The card deck contains the human behavioral patterns
- b. Each team draws three cards from the set of ATTACK VECTORS. The card deck contains attack techniques.

2. Brainstorming Phase

The teams take the role of the attacking social engineers and prepare a sophisticated attack with the combination of the following factors. The teams have ten minutes to prepare their attacks in writing.

a. COMPLIANCE PRINCIPLE

The card drawn with the COMPLIANCE PRINCIPLE forms the foundation of the attack preparation and must be implemented as precisely as possible. For example:

« DECEPTION is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation. »

b. ATTACK VECTOR

One of the three ATTACK VECTORS drawn must be selected and scheduled for the attack. For example:

« PRETEXTING is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack. »

c. Attacker

The team has to decide whether the attacker is an insider or an outsider of the organization. An insider is a known member of the organization who has already established trust. An outsider is new to the organization and has to establish trust to its employees. For example:

« The social engineer is an outside attacker. »

d. Targeted Person

A person from the corporate team has to be selected for the attack. For example:

« MIA is the assistant to the CEO. To support him, she has access to almost everything. She does ok with computers but is bothered by the many security precautions in the company. »

e. Targeted Asset

A realistic information goal can be freely defined. For example:

« The goal is to read the current email traffic of the CEO. »

f. Context

An outline of the situation shall be described as initial situation for the attack. For example:

« MIA always leaves her office door and computer unlocked. The cleaning guy takes it very seriously when cleaning the offices. »

g. Attack

The planned attack is to be described. For example:

« A social engineer can just enter her office pretending to be a new cleaning guy, so he can just enter and send an email using her computer and open an attachment with a trojan. »

3. Attack Phase

- a. The active team presents its attack to the group.
- b. Each attack consists of all factors of the brainstorming phase.
- c. The given factors are to be explained and the factors chosen are to be explained.
- d. After a team has proposed an attack it is initialized and cannot be changed anymore.

4. Discussion

- a. At this point, the group discusses whether the proposed attack is feasible or brings arguments why this could be unrealistic.
- b. If the proposed attack is not plausible, the turn ends immediately.
- c. Finally, the group has to make the choice on how many points are granted.
- d. In addition, the other teams can also propose improved versions of an attack and gain points.
- e. All attacks have to be documented.

5. Points

The following points can be gained per round:

a. COMPLIANCE PRINCIPLE

2 Points	Perfect match
1 Point	Somewhat a match
0 Point	No match

b. ATTACK VECTOR

1 Point	Perfect match
0 Point	No match

c. Attacker

2 Point	Inside attacker
1 Points	Outside attacker

d. Targeted Person, Targeted Asset, Context and Attack as one consistent whole

2 Points	Feasible
1 Point	Somewhat a match
0 Point	No match, the turn ends immediately with zero points for the attacking team







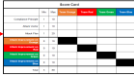

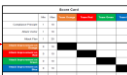
e. Attack Improvement by other teams

2 Points	Major improvement
1 Point	Minor improvement
0 Point	No improvement

6. Iteration

- a. The next team proposes an attack in the same fashion explained above.
- b. If several rounds are played, the cards are shuffled after each round and the teams pick up new cards.
- c. The brainstorming phase may be shortened at the discretion of the teams.
- d. The team with the most points wins.

B.2 Game Master Manual

GAME MASTER MANUAL			
Sequence	Action	Responsibility	Duration
First Iteration			
1)	Introduction Statement "...now we change point of views...you are now the social engineers and you will create a social engineering attack...we will play in 4 teams each with 2 players and you will attack a fictitious company...you are playing against the other teams and the best team will win...I will assign you in teams per 2 persons and afterwards you will receive from me the game material"	Comment	
2)	Assigning participants at table into 4 teams à 2 persons	Moderate	
3)	Distribute background information sheet (1 x per team) 1 x 	Distribute & demand reading	
4)	Distribution of game material per team (overall 4 teams) 1 x Situation Map 1 x  1 x Target Person Description <i>Mention structure of the description</i> 1 x 	Distribute	6-8 Min.
5)	INFORMATION-Phase - Teams make themselves familiar with game material	Time keeping & moderate	10 Min.
6)	Distribute compliance principles cards (3x) and attack vector cards (3x) per team 1 x attack plan sheet per team 3 x Compliance Principles  3 x Attack Vectors  1 x Attack plan (to be filled out) 	Distribute	2-3 Min.
7)	BRAINSTORMING- Phase - Preparation of attack & completion of attack plan sheet	Time keeping & moderate	15 Min.
8)	Explain process of evaluation phase - Each team presents its attack - Presentation evaluation per team via scoring cards	Comment	1-2 Min.
9)	PRESENTATION & DISCUSSION of Social Engineering Attacks per team - Moderation of evaluation phase - Request from evaluating teams to vote for scoring via scoring cards - Distribute and explain scoring cards - Collect scoring cards and sum up the distributed points per team on scorecard 	Time keeping & moderate	10 Min. per Team (x4)
BREAK			
Second Iteration			
10)	Distribute additional game material (map of relationship network) 	Distribute	1-2 Min.
11)	Repeat 6) - 7)	Moderate	1 Min.
12)	Repeat 8)	Comment	1-2 Min.
12)	Repeat 9) - Mention attack improvement proposals (Teams may win additional points for attack improvement potentials)	Time keeping & moderate	7 Min. per Team
13)	Evaluation of winner team Sum up points on scorecard per team 	Evaluation of Scorecard	1-2 Min.
14)	Request completion of post-game online survey via QR-Code or paper-based	Moderate & control	
15)	Collect game material completely and hand it to the researchers	Collect	

B.3 Serious Game Team Worksheets

Angriffsplan		
Compliance Principle	<p>Beispiel: <i>„Täuschung ist der Kern von unzähligen Betrugsszenarien. Dinge und Menschen sind oft nicht, was sie zu sein scheinen. Menschen werden oft hinteres Licht geführt, obwohl sie denken, vorsichtig zu sein. Social Engineers nutzen den Vorteil, dass die meisten Opfer sich gemäss ihren Erwartungen von bestimmten Situationen verhalten.“</i></p> <p>Notizen:</p>	5 Punkte
Attack Vector	<p>Beispiel: <i>«Pretexting ist ein Social Engineering Angriff, welcher auf ein ausgewähltes Opfer zugeschnitten wird. Es wird ein Szenario erfinden, um Informationen von einer unwissenden Zielperson zu erhalten. Social Engineers recherchieren über ihr Opfer und sammeln genug Informationen, um diese als Manipulation gegen sie zu verwenden. Damit dieser Angriff erfolgreich ist, ist ein solider Vorwand nötig. Die Stufen beinhalten Recherche, Informationen sammeln, Planung des Vorwands sowie der erfolgreiche Angriff.»</i></p> <p>Notizen:</p>	5 Punkte
Zielperson	<p>Beispiel: <i>«Olivia ist die Assistentin des CEO. Um ihn zu unterstützen, hat sie Zugang zu fast allem. Ihre Computerkenntnisse sind ok, aber sie ist genervt von den zahlreichen Sicherheitsvorkehrungen und Verordnungen innerhalb der Firma.»</i></p> <p>Notizen:</p>	
Angriffsziel	<p>Beispiel: <i>«Das Ziel ist, den E-Mail-Verkehr des CEO zu lesen.»</i></p> <p>Notizen:</p>	
Kontext	<p>Beispiel: <i>«Olivia lässt regelmässig ihre Bürotür unverschlossen sowie ihren PC entsperrt. Das Reinigungsmann ist sehr gründlich, wenn er die Büros säubert.»</i></p> <p>Notizen:</p>	5 Punkte
Angriff	<p>Beispiel: <i>«Ein Social Engineer hat einfaches Spiel ihr Büro zu betreten und vorzugeben ein neuer Reinigungsmann zu sein. Er kann einfach ihr Büro betreten und E-Mails auf ihrem Computer empfangen oder senden. (z.B. E-Mails mit einem Trojaner öffnen).»</i></p> <p>Notizen:</p>	

B.4 Fictitious target persons



THOMAS

Thomas is the CEO of the company. Since he travels a lot commercially, he delegates many of his tasks while on the move.

He is a shark circling the ranks of his subordinates. He makes sure they are not on Facebook or wasting their time.

Computers are tools to him. As long as he has network access, he works from everywhere.

He is concerned that his company might fall behind the market. Therefore, he puts a lot of pressure on the developers.

In his spare time, he does a lot of endurance sports and regularly takes part in races.



MIA

Mia is the assistant to the CEO. To support him, she has access to almost everything.

She is a little miss sunshine goes to great efforts to cheer everyone up and give a personal touch to a sometimes clinical workplace.

She does ok with computers but is bothered by the many security precautions in the company.

Mia is concerned that she is less and less able to distance herself and must always be available.

She is fond of cats and writes regularly about keeping and caring for them in her blog.



AXEL

Axel works at the reception. He decides who is allowed to enter the building and who not.

He is the chatterbox in the office and regaling the team with stories from the movie he most recently watched at the cinema, current affairs in the news or even what he had for lunch.

Axel lived most of his life without computers and knows how to operate basic software.

He is concerned with keeping the office free of unauthorized persons.

Axel informs himself about new ways of surveillance useful for the company.



EMMA

Emma works in the marketing department. She is responsible for sales and customer care.

She is the creative juice in the office, is quick to get enthusiastic about innovations, but focuses more on aesthetics and design than on functionality.

Emma is the only one who could convince the boss that she can work on a more creative operating system than anyone else.

She is concerned that she might miss a trend and always has the latest electronic gadgets.

She travels a lot and doesn't miss a chance to talk about the latest product developments.



BAPTISTE

Baptiste works at the bookkeeping department. He's responsible for all payments.

He is friendly but quiet and focused on getting his job done and take pleasure in not being noticed too much.

He is glad that the new accounting software has not yet been introduced. Even if it means that he has to work on an outdated computer.

He is concerned that all employees and suppliers always receive their payments on time.

Baptiste finds it difficult to make new contacts and feels lonely. Therefore, he is present on different dating platforms



SANDRA

Sandra works in human resources. She organizes hiring new employees and supporting existing ones.

She often chooses to work late. Even if she has no immediate work deadlines, she finds an excuse to stay a bit longer.

Sandra likes to try new software and is curious about any related news.

She is concerned with the privacy of employee and applicant information.

Sandra advertises open positions on many job fairs and universities.



WILLIAM

William is the head of software development and responsible for the products.

He loves lists, flow charts and spreadsheets. He's obsessed with details and a perfectionist.

William is a gifted engineer and he's constantly updating himself.

He is concerned that technologies could be stolen and that they would continue to come under further pressure.

William is often called as a speaker for seminars and congresses. It makes him proud that he even receives enquiries from Asia and the Middle East.



CLAIRE

Claire is a software developer and takes care of bug fixing.

She is always that one person in the office who is upbeat and funny. No matter what crisis is brewing at work, she is able to put a light-hearted spin on current affairs and cheer everyone up.

Her skills as a software developer are limited and she often needs help from others.

Claire is concerned that her position will be outsourced and that she will lose her position.

She often communicates with her friends abroad using the various apps.



ROBERT

Robert is the computer administrator and is responsible for the computer infrastructure.

He always does the bare minimum to get by. He often strolls in late and spends more time discussing last night's Netflix show than working on his tasks.

He's a computer genius. But that also makes him a little arrogant.

He is concerned that someone may penetrate his area of responsibility and compromise the network.

He's a lot on file-sharing sites and has trouble separating private and business.

B.5 Compliance Principles sheets



Frank Stajano & Paul Wilson I

SOCIAL COMPLIANCE

Society trains people not to question authority, so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority. Using the right clothes, body language, and even having a fake business cards has worked for many social engineers in presenting themselves as an authority figure and keeping their victims in autopilot.



Frank Stajano & Paul Wilson II

HERD

People tend to mimic what the majority of people do or seem to be doing. This can lead to conformity of large groups of individuals in either correct or mistaken choices. They let their guard and suspicion down when everyone else appears to share the same behaviors and risks. In this way, they will not be held solely responsible for their actions. This is influenced not only by large groups, but also by high-profile individuals.



Frank Stajano & Paul Wilson III

DECEPTION

Deception is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation. In computing, the well-known tension between security and usability is also related to Distraction.



Frank Stajano & Paul Wilson IV

DISHONESTY

Anything illegal a victim does will be used against them by social engineers, making it harder for the victim to seek help once the victim realizes they have been conned. When corporate users fall prey to a Trojan horse program claiming to offer free access to pornography, they have strong incentives not to cooperate with the forensic investigator to avoid the associated stigma, even if the incident affected the security of the whole company network.



Frank Stajano & Paul Wilson V

TIME

When people are under time pressure to make an important choice, they use a different decision strategy. When there's no time to think, people rely on short cuts and emotional responses to a situation. So social engineers make sure the victim is under time pressure to ensure the victim will respond in a predictable fashion, usually by being greedy, and giving in to the herd principle or by bending to the will of an authority figure.



Frank Stajano & Paul Wilson VI

NEED & GREED

This principle refers to the spectrum of human needs and desires such as the cravings associated with drug addiction, drive states (such as hunger, thirst, and sexual desire), moods and emotions and physical pain, regardless of moral judgment. This makes people vulnerable. Once social engineers know what a victim wants, even if it doesn't exist, he is in a position to manipulate the victim. The more desperate people are, the easier they are to con.



Frank Stajano & Paul Wilson VII

DISTRACTION

People focus on one thing and ignore other things that may happen without them noticing. They focus their attention on what they can gain, what they need, what they can lose or miss out on, what is restricted or will be more expensive later. These distractions can heighten people's emotional state and make them forget other logical facts to consider when making decisions.



David Gragg I

AUTHORITY

Society trains people not to question authority, so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority. Using the right clothes, body language, and even having a fake business cards has worked for many social engineers in presenting themselves as an authority figure and keeping their victims in autopilot.



David Gragg II

DIFFUSION RESPONSIBILITY & MORAL DUTY

People are made to feel that they cannot be held responsible for their actions. They can be further compromised when they are made to feel that any actions they take will be for the greater good. The victim is persuaded that he or she is making decisions that will be the difference between the success or failure of the company or of the employee who is calling, implying that the caller may lose their job based on his or her decision.



David Gragg III

DECEPTIVE RELATIONSHIP

Social engineering relies on relationships with the purpose of exploiting the other person. Building a relationship on perceived common ground can be achieved by appealing to common interests or goals. After the relationship has grown, social engineers can gain all kinds of information. After the connection is made, it is harder for the victim to refuse a request.



David Gragg IV

INTEGRITY & CONSISTENCY

There is a natural tendency to measure others with what we know and expect from ourselves. Unless there is strong evidence to the contrary, people will believe that the person with whom they are talking is telling the truth about what they feel or need. People have a tendency to follow through with commitments in the workplace, even though those commitments may not have been very wise in the first place.



David Gragg V

OVERLOADING

Mistaken premises go unchallenged when they are heard rapidly and are sandwiched between convincing truisms. Having to deal with a lot of information quickly affects logical functioning and can lead to sensory overload. With too much information to process, people become mentally passive. The victim will tend to accept the information since they can no longer scrutinize or process it.



David Gragg VI

RECIPROCATION

There is a well-recognized rule in social interactions that if someone gives us something or promises us something, we should return the favor. This tends to be true even if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. The rule of reciprocity is important because often the returned favor is done unconsciously. Reciprocation is seen constantly in the corporate environment.



David Gragg VII

STRONG AFFECT

Social engineers attempt to induce a heightened state of emotions that compromise's the victim's ability to use logic or to employ a counter argument. The emotion can be positive or negative such as anger, surprise, panic or excitement. Strong affect is introduced when the social engineer makes some statement at the outset of the interaction that triggers strong emotions. The goal is to disengage the victim from their reasoning or skepticism.



Robert Cialdini I

AUTHORITY

Society trains people not to question authority, so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority. Using the right clothes, body language, and even having a fake business cards has worked for many social engineers in presenting themselves as an authority figure and keeping their victims in autopilot.



Robert Cialdini II

SOCIAL PROOF

People tend to mimic what the majority of people do or seem to be doing. This can lead to conformity of large groups of individuals in either correct or mistaken choices. They let their guard and suspicion down when everyone else appears to share the same behaviors and risks. In this way, they will not be held solely responsible for their actions. This is influenced not only by large groups, but also by high-profile individuals.



Robert Cialdini III

LIKING & SIMILARITY

People like people who like them. They are also more likely to be persuaded by people they like. An important aspect of liking is physical attractiveness. People tend to automatically like those they find attractive. Going beyond physical attractiveness, another principle in liking is similarity. We like people who are similar to us; people who enjoy the same hobbies, have comparable personalities or come from the same type of background.



Robert Cialdini IV

COMMITMENT & CONSISTENCY

People value consistency in others, and they also want to appear consistent in their own behavior. Generally, people want their words, attitude, and deeds to be consistent and congruent. Consistency reduces the need to reprocess information and offers shortcuts through complex decisions. People feel more confident in their decision once they commit to a specific action and need to follow it through until the end.

B.6 Attack Vector Sheets



BAITING

Baiting is when a social engineer leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware. Another form are digital offers that are too good to be true such as a free cruise or a free iPad that easily captures a victim in a well-thought-out bait scheme.



DUMPSTER DIVING

Dumpster diving is considered as a low-tech attack, but with serious implications. This term refers to examining waste and discarded products to find useful information. The information can be obtained from anything like company manuals, password files, storage medium, sensitive documents, credit card numbers, receipts, or financial reports. Later this information can be used by social engineers for performing identity fraud.



SHOULDER SURFING

Shoulder Surfing means watching a victim use its computer from over the shoulder. This technique allows social engineers to catch sensitive information and passwords. Commuter trains and buses are an obvious choice of social engineers for Shoulder Surfing and so is a queue at an ATM, but it can happen basically any public place. This is a passive kind of technique which can be done physically or remotely by cameras or by software.



QUID PRO QUO

This attack promises the victim a benefit for exchange of information. Social Engineers pose as professionals and offer IT assistance to the users. Thinking that providing network credentials is required to solve the problem, users provide them to the Social Engineers giving them all the access he needs. Real world examples have shown that employees revealing their network credentials for free gifts such as candy and pens.



REVERSE SOCIAL ENGINEERING

The idea behind this is that the social engineer initially sabotages the network. Then he advertises himself posing as someone from a legitimate organization such as a tech support service capable enough to solve the problem. When the victim sees the advertisement and thinking the attacker as the genuine consultant, welcomes him and allows him to work on the system or the network.



PRETEXTING

It is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack.



PHISHING

Phishing has been the most prolific form of social engineering and the number of victims is always on the rise. Phishing involves creating websites and emails that are carefully designed to look just like the legitimate ones. These trick the user into disclosing their personal information. While E-mail phishing remains the most widely used phishing attack, it can also be carried out by phone calls, text messages or even through social media.



SPEAR PHISHING

Spear phishing is like phishing but tailored for a specific individual or organization. Although often intended to steal data for malicious purposes, Social engineers may also intend to install malware on a targeted user's computer. Spear phishing attempts are not typically initiated by random social engineers but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.



VISHING

Vishing is an electronic fraud scheme whose objective is to extract sensitive information from the victim and makes use of voice technology. The victims are lured into divulging their confidential information like credit card numbers, pin numbers, account numbers or passwords. These attacks commonly involve a scheme called as caller ID spoofing making the calls look like coming from a trusted source like a bank or law enforcement agencies.



SMISHING

Smishing is a combination of SMS and phishing which uses SMS messages to defraud an individual. Bogus text messages masqueraded as threats or offers from legitimate sources like banks or stores lure the individuals to enter their personal data and ultimately become a victim. With more and more people relying on their smart phones to access corporate data and networks, smishing has become the easier way to perform an attack for the criminals.



TAILGATING

Tailgating is another form of social engineering attack also known as piggybacking. Here the social engineers seeking entry into a restricted area can actually walk behind a person having legitimate access. Sometimes, in case of medium sized offices, the social engineers try to strike up conversations with employees and later use this relationship to get past the front desk. The ultimate goal in this kind of attack is to get physical access to the site.



RANSOMWARE

Ransomware has emerged to become the most dangerous cyber threat for both organizations and consumers. It involves installation of a malware which holds a user's computer hostage until a ransom fee is paid or other resources are exchanged. Though there are many ways of distributing the malware or the Trojan horse, high percentage of distribution is through clicking on links attached to phishing emails.



SCAREWARE

Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem. In reality, the victim is simply tricked into downloading and installing the social engineer's malware.



DIVERSION THEFT

In this type of attack, the social engineers trick a delivery or courier company into going to the wrong pickup or drop-off location, thus intercepting the transaction. Diversion theft can also occur on the Internet when attackers steal some confidential information by persuading a legitimate person to deliver or send that information to someone else who is associated with them.



HONEY TRAP

This is one of the popular methods of social engineering when it comes to high requirements. Men are usually more prone to honey traps than women. Social engineers pretend to be an attractive person to interact with a person online, fake an online relationship and then trick them to reveal sensitive information such as passwords, financial details or enterprise security details.



SEXTORTION

Social engineers pose as potential lovers to lure victims to share compromising videos and photos and then blackmail them. The most common is the manipulation of social media, through which the perpetrators of the crimes deceive the victim to send them compromising photos. Another possible method is to invade the victim's webcams and take pictures of them when they think that no one is looking.



FALSE RECRUITER

With so many headhunters looking for job seekers, no one suspects when a fake recruiter comes to inflate an employee's ego and offer seductive positions just to get information. The attacker can also threaten to tell the boss of the employee that he is planning to leave the company and has already shared confidential information to make the victim disclose system access passwords.



WATERHOLING

A watering hole attack is when social engineers exploits a website that a targeting group of user visit. Social engineers first observes the behavior of the users to know what sites they often visit and then they inject some HTML or JavaScript code that redirects the victim to some other webpage. This webpage will further infect the computer of the victim with malware to gain access to the network.

B.7 Evaluation Sheet – Score Card

Score Card						
	Min	Max	Team Orange	Team Red	Team Green	Team Blue
Compliance Principle	1	5				
Attack Vector	1	5				
Attack Plan	1	5				
Total Round I	3	15				
Compliance Principle	1	5				
Attack Vector	1	5				
Attack Plan	1	5				
Attack Improvement on Orange	0	5				
Attack Improvement on Red	0	5				
Attack Improvement on Green	0	5				
Attack Improvement on Blue	0	5				
Total Round II	3	30				
Total Round I & II	6	45				

B.8 Background Information Sheet

Serious Gaming Story Line

Company X, an information engineering enterprise, is an industry leader of high requirement software. In the past couple of years, the business has seen extraordinary growth in terms of revenue and profit. The competitors in the market did not yet manage to reach the level of innovation, quality and productivity of company X. One reason for its success story was the introduction of a ground-breaking artificial intelligence software that received funding from international investors. Luckily, CEO and founder Thomas filed patents for this innovation while starting the business. By now, the company has grown out of a start-up status and is even able to pay out its investors for becoming more independent.

Nevertheless, the company faces heavy competition, as on the one hand its first-mover advantage is continuing to shrink and on the other side the patent for its lead product will expire within the next 12 months. Therefore, the CEO puts a lot of pressure on the employees to drive the innovation process. His skilled team already has another promising software in the pipeline that could revolutionize the market once again. However, in order to finalize the product as fast as possible and to start the patent filing process, the company desperately looks for new software developers. With the international skill shortage in the information technology sector this is a heavy task to complete and takes valuable time.

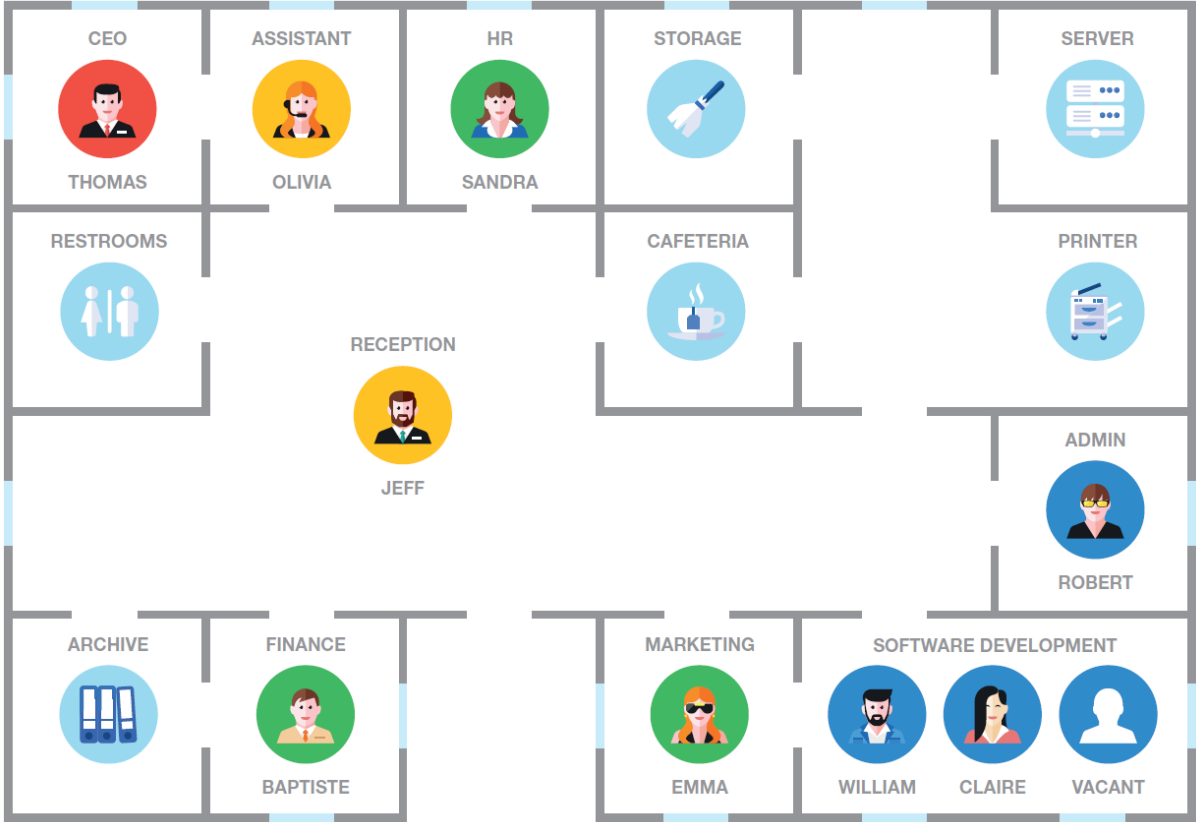
Apart from the business-related challenges, the company faces more and more administrative issues that came in with the steady growth of the business. In the current business year, the company will pass for the first time the critical threshold that requires it by law to be independently audited. The CEO is therefore currently in the process of looking for an external auditor and at the same time thinks of delegating tax filing to external consultants as well.

Finally, the new tightened international regulations for data protection and its implementation causes the CEO and his software developers sleepless nights. Not only will employee and job candidate information need to be handled more restricted, but also software sequences of the new products in the pipeline have to be redesigned in order to be compliant to the new law.

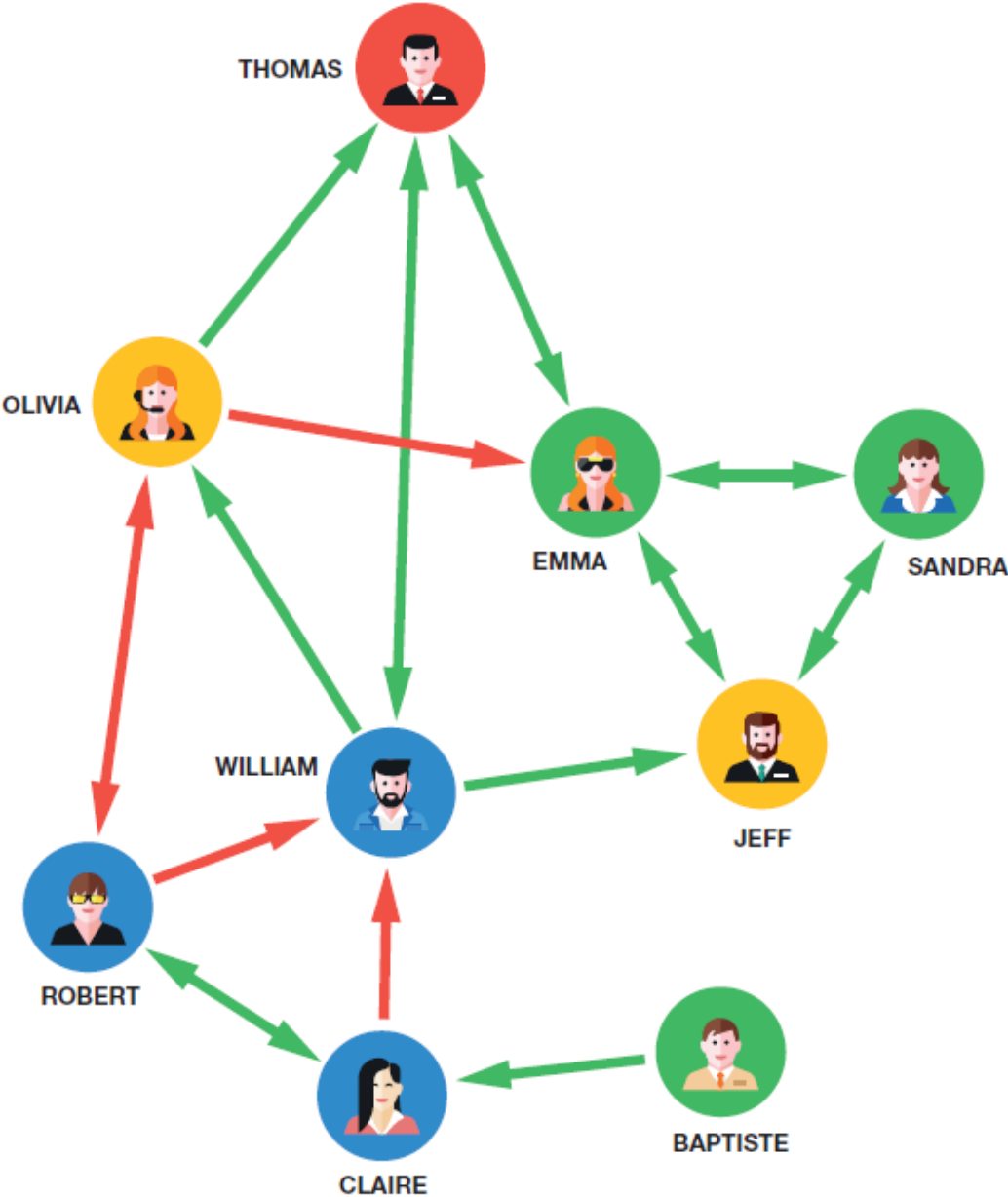
The company will see a challenging business year lying in front of it with additional continuously growing cyber threats all around within the more and more digitized economy. While it has taken specific cybersecurity measures to protect its business and its employees, it lacks the understanding of the potential threat that devious and deceptive Social Engineers pose to its business and its valuable information.

- Now it is your turn to seize this awareness gap of the importance of the human factor for cybersecurity by masquerading yourself as a Social Engineer and launch a successful Social Engineering Attack on company X.

B.9 Situation Map Sheet



B.10 Sociogram



B.11 Excerpt of Sample Documentation
Attack Plans Examples

Attack Plan Team Orange		1
Compliance Principle	<p>Example: «Deception is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation.»</p> <p>Notes: <i>Distraction</i></p>	10 Points
Attack Vector	<p>Example: «Pretexting is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack.»</p> <p>Notes: <i>Honey Trap</i></p>	10 Points
Targeted Person	<p>Example: «Olivia is the assistant to the CEO. To support him, she has access to almost everything. She does ok with computers but is bothered by the many security precautions in the company.»</p> <p>Notes: <i>Daphne</i></p>	
Targeted Asset	<p>Example: «The goal is to read the current email traffic of the CEO.»</p> <p>Notes: <i>LinkedIn like</i></p>	
Context	<p>Example: «Olivia always leaves her office door and computer unlocked. The cleaning guy takes it very seriously when cleaning the offices.»</p> <p>Notes: <i>Big platform</i></p>	20 Points
Attack	<p>Example: «A social engineer can just enter her office pretending to be a new cleaning guy, so he can just enter and send an email using her computer and open an attachment with a trojan.»</p> <p>Notes: <i>Link (Hook, webmess.)</i></p>	

Attack Plan Team Red **2**

Compliance Principle	<p><i>Example: «Deception is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">27honey / illegal</p>	10 Points
Attack Vector	<p><i>Example: «Pretexting is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">dhily / using kend / gadgets</p>	10 Points
Targeted Person	<p><i>Example: «Olivia is the assistant to the CEO. To support him, she has access to almost everything. She does ok with computers but is bothered by the many security precautions in the company.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">Fina</p>	
Targeted Asset	<p><i>Example: «The goal is to read the current email traffic of the CEO.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">raduchij / jprH "Pudchke" hpf /</p>	
Context	<p><i>Example: «Olivia always leaves her office door and computer unlocked. The cleaning guy takes it very seriously when cleaning the offices.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">- lateral el. gadgets - talk about lateral prod. dev.</p>	20 Points
Attack	<p><i>Example: «A social engineer can just enter her office pretending to be a new cleaning guy, so he can just enter and send an email using her computer and open an attachment with a trojan.»</i></p> <p>Notes:</p> <p style="font-size: 1.5em; font-family: cursive;">gadget download lateral use / supercrypto date</p>	

Score Card examples

Score Card						
	Min	Max	Team Orange	Team Red	Team Green	Team Blue
Compliance Principle	1	10	Lin Line 8	respeccom 6	stehen 9	
Attack Vector	1	10	Bewehr 7	son Fisch 4	Periode 9	
Attack Plan	1	20	14	12	15	
Attack Improvement on Orange	0	10		8	0	
Attack Improvement on Red	0	10	7			
Attack Improvement on Green	0	10				
Attack Improvement on Blue	0	10				
Total	3	80	36	30	33	

nach
news
angela
=

news
wo steht si
in der Geschichte
Li-Li.

Score Card						
	Min	Max	Team Orange	Team Red	Team Green	Team Blue
Compliance Principle	1	10	10	10	10	
Attack Vector	1	10	5	8	7	
Attack Plan	1	20	14	10	10 8	
Attack Improvement on Orange	0	10				
Attack Improvement on Red	0	10				
Attack Improvement on Green	0	10				
Attack Improvement on Blue	0	10				
Total	3	80	29	28	25	

Sample Data Reporting

Serious Gaming Data Reporting	
Research Method:	Field Observation
Researcher's involvement:	Administrator; Game Master - Observer-as-Participant
Sampling	Purposive Sampling
Data Collection/Recording:	Field Interview; Field Notes; Photographs; Game sheets
Sample No.:	1
Organization:	
Date:	05.12.2019
Time:	15:00 - 16:30
Location:	Zürich (CH)
Duration:	1.5h
Room:	Meeting Room Schaffhausen
Room conditions:	climatized, light, on company's business floor, almost too small for the training
Paid/unpaid:	unpaid
Game extent:	1 Round – Speed dating version; w time keeping
Table administration:	one table with 4 teams à 2-3 persons; 9 persons
Preceding SE presentation:	No
Pre-/post-questionnaire:	No
Language (game material):	English
Language game:	German / Swiss German
Game masters No.:	9
Game Master Training:	No
GM Training administration:	
Sample size:	9
Population demographics	
<i>Male-Female ratio:</i>	78% male (7/9)
<i>Age range:</i>	23 - 50
<i>Sample industries:</i>	telecommunication, consumer electronics
<i>Sample professions:</i>	Finance specialist, Controller, Key Account Manager, Consultant, Self-employed consultant, Marketing specialist
<i>Sample behaviour:</i>	The population was in general interested in the game, but they did not take it seriously in the same manner. All of the participants volunteered to help and be a game master in the succeeding serious gaming event. Nevertheless, most of the participants were engaged in understanding the game material and playing the game. As the purpose was to train the game masters, the administration of the game was not comparable to the event. Some took it easily and thought they know better than others, without the need to understand precisely. Some of the participants were nervous and feared the succeeding event, where they had to be game masters. The time for preparing the game masters was not sufficient enough and they lacked the SE presentation for understanding the rationales behind the SE and how this is reflected within the game.
<i>Socio-cultural behaviour:</i>	The participants reflected a diverse demography in terms of gender, age, education, profession, personality and extent of professional experience. This was partially recognizable during the game as well, whereas older participants, participants with higher education and participants who seemed to be more open and extravert dominated during the discussions of the game proceedings. interesting game and educational, fun, wished to have more time available
<i>Population feedbacks:</i>	
<i>Criminal behaviour/intentions:</i>	
Citations of feedbacks:	1) "The game wasn't perfectly administered. The introduction to the game material could have been better." 2) "An introductory presentation was missing for leading the participants."
Other observations:	Participants filled out the Attack Plan sheet as requested. Either they understood quite well their task or it was more focused on by the researcher to make clear their task and how to proceed with the sheet.
Other Remarks	Participants volunteered for the game, but received a prize from the organizer for their efforts.

Serious Gaming Data Reporting	
Research Method:	Field Observation
Researcher's involvement:	Administrator - Observer-as-Participant
Sampling	Purposive Sampling
Data Collection/Recording:	Field Interview; Field Notes; Photographs; Game sheets
Sample No.:	2
Organization:	
Date:	05.12.2019
Time:	17:30 -19:00
Location:	Zürich (CH)
Duration:	1.5h
Room:	Plenary hall
Room conditions:	climatized, light, separated from company's business floor
Paid/unpaid:	unpaid
Game extent:	1 Round – Speed dating version; w time keeping
Table administration:	9 tables up to 10 persons per table; teams à 2-3 persons; people were allocated randomly to the table by drawing table number while entering the playground
Preceding SE presentation:	Yes
Pre-/post-questionnaire:	No
Language (game material):	English
Language game:	German / Swiss German
Game masters No.:	9
Game Master Training:	Yes
GM Training administration:	1.5h immediately before the Serious Gaming event
Sample size:	70
Population demographics	
<i>Male-Female ratio:</i>	
<i>Age range:</i>	35-60
<i>Sample industries:</i>	telecommunication, consulting, SME, engineering
<i>Sample professions:</i>	CEO, CFO, company owner, CISO, Head of R&D, Manager
<i>Sample behaviour:</i>	The population was generally heavily interested in the presentation and the following serious game. The population consisted primarily of C-level employees. A high engagement during the game was observed. The seniority and position of the employees also let us observe a high intention to win and succeed in the game, being a good Social Engineer. Even participants that arrived late regretted to do so. As it was an ASUT member apéro, people often just come after the presentation for the free apéro. People clearly regretted this. Group discussions were on an intense level from the beginning, although it was played only 1 round with time keeping in place. However, time didn't matter and passed by without people being disengaged.
<i>Socio-cultural behaviour:</i>	The participant table composition was randomly assigned. The co-operation among the teams and within the teams differed. Among the teams there were frequently discussion about proposing attack improvements. For sure, also driven by the motivation to win, which could also correlate to the fact that the participants were primarily C-level. The co-operation within the teams was ranging from being directive, co-operative or being authoritarian.
<i>Population feedbacks:</i>	interesting game and educational, fun, wished to have more time available, possible to replicate in other scenarios?
<i>Criminal behaviour/intentions:</i>	The time keeping was administered by using stylish egg timers and it was clearly visible that these are part of the game material and not a present to the population. It appeared that one of the participants managed to steal an egg timer. The researcher was in a position to see the process of thieving. The thief managed to distract the game master at the table and in a moment of absence put the egg timer into his pocket. At this point, it is not clear, whether the participant just wanted to test his abilities of being a good Social Engineer and showing them off or whether he really wanted to take the egg timer with him. It turned out that the participant was colleague of the presentation presenter and only gave it back once on the way back home while saying goodbye, telling that he thought it was a present to the participants by the organizer. Without mentioning the theft to the presenter, the thief would have taken with him the egg timer willingly. Although it might not be clear, whether there was a real criminal intention or whether it was solely for the purpose of showing off, it is nevertheless an indicator that the game might unveil criminal dispositions and their succeeding behaviour. Thus, together with some personality profile, the game could probably act as an identifier of white collar insider threats, being crime preventive.
Citations of feedbacks:	1) "The room was almost too small, as it has become too noisy." 2) "Did you develop this game? We think this has huge potential and we could play it in our company as well." 3) "Can we take the game material with us?" 4) "The game should be digitized in order to scale it and make it more accessible." 5) "This was the best ASUT member event, I have ever been. I wish all would be that enjoyable." 6) "The game was really fun and we could administer it in our company as well. The only problem I had was with the game material, as I am not perfectly fluent in English." 7) "This was an interesting and educational event. One suggestion for the game from my side would be an introduction sheet at the beginning of the game."
Other observations:	As the population consisted primarily of C-level employees and as the game was part of a regularly recurring event of the Swiss Association of Telecommunication, the participants had a specific expectation of the event. At the beginning of the event a little scepticism was observed. Especially as it came to the random table assignment of the participants, they were rather reserved and by far not open or flexible, but rather annoyed of being deprived their freedom of table and sitting neighbor selection. It could be that this was primarily to the experiences with previous events and facing the unexpected. Nevertheless, the serious game turned out to be entertaining for almost all people. Most of the participants were German mother-tongue speaking. Although the presentation was held in German, the game material was in English, only. Some participants seemed to have problems with understanding the material in English. For future case-studies the material will also be available in German. Most of the teams did not follow the instructions to fill out the Attack Plan sheet as provided in the example. Some didn't even fill it out, others filled it out but rather provisionally and not corresponding to the examples. This could mean that they did not understand the rationale of the game, which is not positive. However, this alone does not mean the awareness creation process was unsuccessful.
Other Remarks	Catering during game; the teams with the most achieved points per table won a prize sponsored by the organizer. The participants did not know in advance what the prize would be.

Serious Gaming Data Reporting	
Research Method:	Field Observation with Post-Questionnaire
Researcher's involvement:	Administrator; Game Master - Observer-as-Participant
Sampling:	Purposive Sampling
Data Collection/Recording:	Field Interview; Field Notes; Game sheets
Sample No.:	3
Organization:	
Date:	13.02.2020
Time:	8:30 - 12:30
Location:	Bern (CH)
Duration:	4h
Room:	Meeting room
Room conditions:	not climatized - hot; airless, muggy; on business floor; windows to the aisle
Paid/unpaid:	unpaid
Researcher's involvement:	Administrator; Game Master
Game extent:	2 Round - including Sociogram & improvement proposals in 2nd round; w/o time keeping
Table administration:	1 table with 3 teams à 2 persons
Preceding SE presentation:	Yes
Pre-/post-questionnaire:	Yes - post-questionnaire
Language (game material):	English
Language game:	German / Swiss German
Game masters No.:	2
Game Master Training:	No
GM Training administration:	-
Sample size:	5 -6 (6 in 1st round - 5 in 2nd round)
Population demographics	
<i>Male-Female ratio:</i>	100% male (5/5)
<i>Age range:</i>	19 - 22
<i>Population industries:</i>	IT Command
<i>Population professions:</i>	IT apprentices
<i>Population behaviour:</i>	Silent; restrained, shy, in 2nd round sample entities were more open
<i>Socio-cultural behaviour:</i>	good co-operation among team-members; per each team 1 member was taking the lead and presenting;
<i>Population feedbacks:</i>	interesting game; fun & interesting playing; good way to get to know about SE; wish to have more of such in their vocational training
<i>Criminal behaviour/intentions:</i>	One entity explicitly showed potential criminal dispositions by his imaginative power and his statements about previous fictious plans in his youth
Citations of feedbacks:	1) "And do you already have some idea for an attack? - Yes, we could poison the assistant's cat, such that she has to go to the doctor's and we can take advantage of her not being present in the office....we would smash the windows in the office...." - "These are things I already made up when I was 14 years old." 2) "Oh, we did not recognize the time passing by" 3)
Other observations/final remarks:	In general, the sample entities did a good job in imagining SE scenarios with an increasing breadth and depth over the duration of the game. Their continuous high involvement in the game, as well as their feedbacks suggest that the game is fun, encourages to think about SE attacks and their components. Sample entities did not recognize the time flying by, which could be assessed as an indicator of high cognitive involvement. One of the entities explicitly stated that Compliance principles and Attack Vectors should be omitted. This reflects that he did not get the rationale of SE and its application in the game right. Although the whole population was rather silent and shy, the entity being most shy showed the most imaginative power and criminal fantasy. Overall, the population did not manage to keep the guidelines of the game structure and the structure of the attack plan. Compliance Principles and Attack Vectors were not chosen uniquely, but rather a combination of the available cards was used or new other, not chosen or available, principles were applied. Although the population showed high imaginative power to form an attack, they did not manage to stay within the guidelines. Sometimes, their approach was rather unstructured, however extensively. The discussion among the groups increased in round 2, suggesting a learning effect and a familiarization with the game in general. Moreover, the evaluation phase discussions were deeper and with more content in round 2, as well. The possibility of proposing improvements to the attacks fostered the group discussions and the argumentation among the sample entities. This is also a good method for reflecting the principles and to deal with SE principles. By this approach to observe the population within an official professional environment, the population is likely to behave in a natural way compared to situations where the population is aware of being part of an experiment. In general, less compliance to the game structure was observed compared to the one in sample 02
Other Remarks	

C. Excerpt of Pre-experiment survey

Social Engineering - (Not) A Game: Survey

Information on the research study

Dear participant

thank you very much for taking part in this study.

I, Fabian Muhly (study director), am a research assistant at the Swiss Armed Forces Military Academy (MILAK) and a doctoral student at the University of Lausanne. As part of my doctoral thesis at the University of Lausanne on the subject of social engineering, I am conducting the experimental research study described below as study director with the support of the Swiss Armed Forces (ASTAB, MILAK, AFCSO), based on Art. 4, 13 and 22 of the Federal Act on Data Protection (DSG; SR 235.1). Due to the interest of the Armed Forces in the results of this study, they are supporting me in carrying it out.

Prof. Dr. Stefano Caneppele, University of Lausanne, is scientifically supervising me.

Objective and benefit:

According to Art. 58 of the Federal Constitution (SR 101), the armed forces serve to prevent war, defend the country and its population and support the civilian authorities in countering serious threats.

In many cyber-attacks, humans are the immediate target for cyber criminals and other motivated actors. In so-called social engineering attacks, attackers use methods of trickery to gain access to information that can be used for financial purposes or espionage. Even defence institutions are not spared from such attacks. Effective defence strategies against such attacks are still scarce. This research study aims to contribute to changing this.

In consultation with MILAK and the Armed Forces Command Support Organisation (AFCSO), we want to use the study to find out in particular how vulnerability to cyber trickery (so-called social engineering) can be reduced by means of an awareness-raising board game and by analysing individual personality patterns.

By participating in the study, you will help the Swiss Armed Forces to evaluate defence strategies against cyber trickery and contribute to increasing cyber security in the Swiss Armed Forces.

Study procedure:

You as members of the armed forces, resp. [REDACTED], will:

1. be asked below to declare your consent for voluntary participation in the experimental research study in question;
2. participate in the study by providing your personal e-mail address (not work or military related) during the subsequent online questionnaire for use in the cyber trickery test as described in section 4; be asked about demographics, self-perception and (cyber) risk attitude in this online questionnaire that takes about 15 minutes;
3. be invited to participate in the framework of the refresher course from 19.04.2022 to 06.05.2022 in an interactive tabletop game with comrades designed to evaluate the vulnerability to cyber trickery. This activity will be provided physically during ½ day of your repetition course, as agreed between the commander of [REDACTED] and the study director F. Muhly. The effective allocation is made by the commander [REDACTED];
4. receive cyber trickery that test the change in personal vulnerability to cyber trickery before and after the board game.

The total effort for the participants amounts to a maximum of about 5 hours. As said under 3. above, you have half a day of your repetition course at your disposal, as agreed with the commander [REDACTED].

Data processing:

All data goes directly to the study director F. Muhly. The army has no access to this data. In an agreement between the army and F. Muhly, the latter commits himself:

- To use all data (e-mail addresses, information on the questions in the questionnaire, information from the interactive online board game and from the cyber trick fraud test) exclusively personally for the study;
- To not disclose any data to third parties, not to employees of the University of Lausanne or the Swiss Armed Forces;
- To destroy the data after completion of the study, but at the latest upon completion of the doctorate, and report the completion to the army;
- To make the anonymized study results available and free of charge to the armed forces and the participants, or to publish them after consultation with the armed forces.

Risks of participation:

Participation in this study is voluntary, free of charge and gratuitous. You can cancel participation in the study at any time, without giving reasons and without disadvantages. The data will subsequently be destroyed immediately. Your data will only be used for the purpose of this study.

Persons of contact:

Alternatively, if you have any questions, concerns or complaints, contact:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Funding and audit of the study:

The study is financed by the study director's own funds.

The study was reviewed by the Ethics Committee of the faculty of Law, Criminal Sciences and Public Administration of the University of Lausanne with the review number: E_FDCA_102020_00003.

There are 129 questions in this survey.

Demographics/General Questions

General questions

Please state your participant-ID from the flyer hereafter: *

Please write your answer here:

(e.g.: 037)

I hereby confirm that I can be contacted via the e-mail address entered hereafter and that I am the rightful owner of it. *

Please choose only one of the following:

Yes

No

Your E-Mail address is used solely for the purpose of this study and to inform you. After successful completion of the study, it will be deleted according to legal requirements.

You have answered NO to the previous question. Please enter your correct e-mail address below, which belongs only to you.

Without providing your correct email address, you will falsify the study results and prevent the successful completion of an elaborate and valuable research study.

THANK YOU

Only answer this question if the following conditions are met:

Answer was 'No' at question ' [G02]' (I hereby confirm that I can be contacted via the e-mail address entered hereafter and that I am the rightful owner of it.)

Please state your personal E-mail address (not work or military related) hereafter: *

Please check the format of your answer.

Please write your answer here:

What is your gender?

Please choose the appropriate response for each item:

Male Female Diverse

What is your year of birth?

Choose one of the following answers

Please choose only one of the following:

2005

2004

2003

2002

2001

2000
1999
1998
1997
1996
1995
1994
1993
1992
1991
1990
1989
1988
1987
1986
1985
1984
1983
1982
1981
1980
1979
1978
1977
1976
1975
1974
1973

1972

1971

1970

1969

1968

1967

1966

1965

1964

1963

What is your mother tongue?

Check all that apply

Please choose all that apply:

French

German

Italian

English

Other

In the last 12 months, did you participate in a training that focused on how to protect personal data and information? *

Please choose the appropriate response for each item:

YES NO

Was it an online training?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [D04]' (In the last 12 months, did you participate in a training that focused on how to protect personal data and information? ())

Please choose the appropriate response for each item:

YES NO

In the last 12 months, did you participate in a training that focused on how to protect military-related data and information? *

Please choose the appropriate response for each item:

YES NO

Was it an online training?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [D05]' (In the last 12 months, did you participate in a training that focused on how to protect military-related data and information? ())

Please choose the appropriate response for each item:

YES NO

How important do you consider the security of personal information in your daily life? *

Please choose the appropriate response for each item:

Not important at all Not important Neutral Important Very important

How important do you consider the security of military-related information in daily life? *

Please choose the appropriate response for each item:

Not important at all Not important Neutral Important Very important

Individual patterns (1/3)

Questions about self-perception. Please indicate how much the statement applies to you.

I would be quite bored by a visit to an art gallery. *

Please choose the appropriate response for each item:

Disagree strongly Disagree a little Neither agree nor disagree Agree a little Agree strongly

I plan ahead and organize things, to avoid scrambling at the last minute. *

Please choose the appropriate response for each item:

Disagree strongly	Disagree a little	Neutral	Agree a little	Strongly agree
----------------------	----------------------	---------	----------------	-------------------

I rarely hold a grudge, even against people who have badly wronged me. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I feel reasonably satisfied with myself overall. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I would feel afraid if I had to travel in bad weather conditions. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I'm interested in learning about the history and politics of other countries. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I often push myself very hard when trying to achieve a goal. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

People sometimes tell me that I am too critical of others. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I rarely express my opinions in group meetings. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I sometimes can't help worrying about little things. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

If I knew that I could never get caught, I would be willing to steal a million dollars. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I would enjoy creating a work of art, such as a novel, a song, or a painting. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

When working on something, I don't pay much attention to small details. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

People sometimes tell me that I'm too stubborn. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I prefer jobs that involve active social interaction to those that involve working alone.
*

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

When I suffer from a painful experience, I need someone to make me feel comfortable. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

Having a lot of money is not especially important to me. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I think that paying attention to radical ideas is a waste of time. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I make decisions based on the feeling of the moment rather than on careful thought. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

People think of me as someone who has a quick temper. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

On most days, I feel cheerful and optimistic. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I feel like crying when I see other people crying. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

I think that I am entitled to more respect than the average person is. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

If I had the opportunity, I would like to attend a classical music concert. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

When working, I sometimes have difficulties due to being disorganized. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

My attitude toward people who have treated me badly is “forgive and forget”. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I feel that I am an unpopular person. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

When it comes to physical danger, I am very fearful. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

If I want something from someone, I will laugh at that person's worst jokes. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I've never really enjoyed looking through an encyclopedia. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I do only the minimum amount of work needed to get by. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I tend to be lenient in judging other people. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

In social situations, I'm usually the one who makes the first move. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I worry a lot less than most people do. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I would never accept a bribe, even if it were very large. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

People have often told me that I have a good imagination. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I always try to be accurate in my work, even at the expense of time. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I am usually quite flexible in my opinions when people disagree with me. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

The first thing that I always do in a new place is to make friends. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I can handle difficult situations without needing emotional support from anyone else. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I would get a lot of pleasure from owning expensive luxury goods. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I like people who have unconventional views. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I make a lot of mistakes because I don't think before I act. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

Most people tend to get angry more quickly than I do. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

Most people are more upbeat and dynamic than I generally am. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I feel strong emotions when someone close to me is going away for a long time. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I want people to know that I am an important person of high status. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I don't think of myself as the artistic or creative type. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

People often call me a perfectionist. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

Even when people make a lot of mistakes, I rarely say anything negative. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I sometimes feel that I am a worthless person. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

Even in an emergency I wouldn't feel like panicking. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I wouldn't pretend to like someone just to get that person to do favors for me. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I find it boring to discuss philosophy. *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
-------------------	----------	---------	-------	----------------

I prefer to do whatever comes to mind, rather than stick to a plan. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Neutral Agree Strongly agree

When people tell me that I'm wrong, my first reaction is to argue with them. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Neutral Agree Strongly agree

When I'm in a group of people, I'm often the one who speaks on behalf of the group. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Neutral Agree Strongly agree

I remain unemotional even in situations where most people get very sentimental. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Neutral Agree Strongly agree

I'd be tempted to use counterfeit money, if I were sure I could get away with it. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Neutral Agree Strongly agree

Victimization

Victimization

In the past 12 months, have you ever received an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords? *

Please choose the appropriate response for each item:

YES NO

How often?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [V01]' (In the past 12 months, have you ever received an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords? ())

Please choose the appropriate response for each item:

1 2- >5
5

In the past 12 months, have you ever opened an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords? *

Please choose the appropriate response for each item:

YES NO

How often?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [V02]' (In the past 12 months, have you ever opened an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords? ())

Please choose the appropriate response for each item:

1 2- >5
5

In the past 12 months, have you ever sent online sensitive data (personally identifiable information, banking and credit card details, and passwords) to someone - posing as a trusted institution- who sent you the request through an email? *

Please choose the appropriate response for each item:

YES NO

How often?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [V03]' (In the past 12 months, have you ever sent online sensitive data (personally identifiable information, banking and credit card details, and passwords) to someone - posing as a trusted institution- who sent you the request through an email? ())

Please choose the appropriate response for each item:

1 2-
5 >5

If you have suffered financial losses, please indicate how much money you lost in CHF:

Please write your answer here:

Did you report the fact to police? *

Please choose the appropriate response for each item:

YES	NO	Not applicable
-----	----	-------------------

You said you have reported. Could you tell us, why you decided to report?

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [V05]' (Did you report the fact to police? ())

Choose one of the following answers

Please choose only one of the following:

To protect other persons

To assist the police in prosecuting

To be entitled to an insurance benefit

Other

You said you have not reported. Could you tell us, why you decided to not report?

Only answer this question if the following conditions are met:

Answer was 'NO' at question ' [V05]' (Did you report the fact to police? ())

Choose one of the following answers

Please choose only one of the following:

I would have had no advantage from a report

I was ashamed

A report does not help the police to solve the case

Reporting it is too inconvenient and/or I don't know how and where to report it

Other

In the next 12 months, how likely is it you, unvoluntary, disclose personal information online to someone who via email - posing as a trusted institution - asked you to provide sensitive data (e.g. banking and credit card details, and passwords)? *

Please choose the appropriate response for each item:

Very unlikely Unlikely Neutral Likely Very Likely

| No, not at all | Yes, extremely

Individual patterns (2/3)

Please indicate for the below statements how often you engaged in the described activity in the last 6 months (Never - Daily).

Sharing passwords with friends and colleagues. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Using or creating passwords that are not very complicated (e.g. family name and date of birth). *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Using the same password for multiple websites. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Using online storage systems to exchange and keep personal or sensitive information. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Entering payment information websites that have no clear security information/certification. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Using free-to-access public Wi-Fi. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Relying on a trusted friend or colleague to advise you on aspects of online-security. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Downloading free anti-virus software from an unknown source. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Disabling the anti-virus on my work computer so that I can download information from websites. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Bringing in my own USB to work in order to transfer data on to it. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Checking that software for your smartphone/tablet/laptop/Pc is up-to-date. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Downloading digital media (music, films, games) from unlicensed sources. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Sharing my current location on social media. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Accepting friend requests on social media because you recognise the photo. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Clicking on links contained in unsolicited emails from an unknown source. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Sending personal information to strangers over the Internet. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Clicking on links contained in an email from a trusted friend or work colleague. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Checking for updates to any anti-virus software you have installed. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Downloading data and material from websites on my work computer without checking its authenticity. *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop). *

Please choose the appropriate response for each item:

Never Once Quarterly Monthly Bi-weekly Weekly Daily

Individual patterns (3/3)

For each statement, please indicate how much you agree with this.

I think that the military command has the responsibility to ensure the army is protected from cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I am aware of my role in keeping the army protected from potential cybercriminals. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I believe everyone in the army has a role to play in protecting against threats from cybercriminals. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

It is hard to know how I can help protect the army from cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I don't have the right skills to be able to protect the army from cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I do not feel that IT security is a priority within the army. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

Computer systems provide all the protection the army needs. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I think that reporting cybercrime is a waste of time. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

The Police lack the capacity to deal with cybercrime effectively. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I believe that cybercriminals are more advanced than the people who are supposed to be protecting us. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I think that information provided by the Government and Police on cybercrime is not relevant to the army. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I feel that the Police are far too busy to deal with cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I worry that if I report a cyberattack to the Police it might damage the reputation of the army. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I think more could be done to communicate the risks from cybercrime to individuals in the army. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I am aware of the army's IT use policy and attempt to follow it. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I would not know how to report a cyberattack if one happened. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I don't think that reporting a cyberattack on the army is my responsibility. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I don't pay attention to army material about the threats from cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I am confident that I would be able to spot the signs of a cyberattack. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I think the biggest threat for IT systems comes from people within the army. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I feel that any individual within the army are at risk of manipulation from confidence tricksters. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I think that cybercriminals only target the army when there is a substantial financial gain. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I believe only large organizations are targeted by hackers and cybercriminals. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I feel that only organizations that take payments using online systems are at risk of being victims of cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree

I don't think I know who is responsible for protecting the army from cybercrime. *

Please choose the appropriate response for each item:

Strongly disagree Disagree Agree Strongly Agree


Thank you very much for completing the survey and helping me with my research study. Your responses are now saved and transmitted.

04-02-2022 – 23:59

Submit your survey.

Thank you for completing this survey.

D. Ethical approval CER-UniL


UNIL | Université de Lausanne

Mr. Fabian Muhly
University of Lausanne
ESC
1015 Lausanne

Lausanne, 9 November 2020

Decision of the Research Ethics Commission of the University of Lausanne (CER-UNIL)
Project number: E_FDCA_102020_00003

Title of the project: *The Human Factor in Cybercrime: Assessing Individual Social Engineering Risk and a Serious Game as a Risk Mitigation Tool*

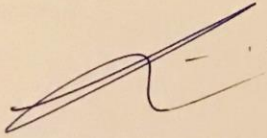
Principal applicant: Mr. Fabian Muhly (under supervision of Prof. Stefano Caneppele)
Mail adress: Fabian.Muhly@unil.ch
Date of submission: 07 Oct 2020

I. Decision authority
 CER-FDCA

II. Decision
 Approval

The research project meets the criteria of ethical compliance. Any comments made by the experts do not lead to changes in the documents approved by the Ethics Commission

III. Signature of the deciding authority



Prof. Laurent Bieri, President

Reporting obligations: Any adverse event that compromises the health or safety of participants or persons conducting the research, as well as any interruption, extension or major modification of the project, must be reported to the Ethics Commission that issued the approval.

|||||
|cer.unil@unil.ch

E. Flyer for participant recruitment



The flyer is divided into two main color sections: a red top section and a dark green bottom section. In the red section, on the left, is a white silhouette of a person sitting on a swing. The swing seat is replaced by a computer monitor with a large white 'X' over it. To the right of this icon, the words 'SOCIAL ENGINEERING' are written in large, bold, white capital letters. The green section contains the main text of the flyer. At the top of the green section, the title 'Social Engineering – (K)eine Spielerei' is written in white. Below it, a subtitle reads 'Cybersicherheit ist auch menschlich – Ihre Teilnahme an der Forschungsstudie zählt!'. The main body of text explains the purpose of the study. On the right side of the green section, there is a QR code with the text 'Hier geht es zur Studie:' above it and 'SCAN ME' below it. Below the QR code, it says 'Ihre Teilnehmer-ID:' followed by the number '001' which is enclosed in a red square. At the bottom left of the green section, there is a white rectangular box followed by a short paragraph of text.

SOCIAL ENGINEERING

Social Engineering – (K)eine Spielerei

Cybersicherheit ist auch menschlich – Ihre Teilnahme an der Forschungsstudie zählt!

Mit Ihrer Teilnahme an dieser experimentellen Forschungsstudie helfen Sie der Schweizer Armee bei der Evaluation von Verteidigungsstrategien gegen Cyber-Trickbetrug und tragen massgeblich zur Steigerung der Cybersicherheit in der Schweizer Armee bei.

Hier geht es zur Studie:



SCAN ME

Ihre Teilnehmer-ID:

001

Die Teilnahme an der Studie ist freiwillig. Die Studie beginnt mit einer 15-minütigen Umfrage nach dem Scannen des QR-Codes und Ihrer Einwilligung zur Teilnahme an der Studie.

Der Faktor Mensch der Cybersicherheit

Bei sehr vielen Cyberangriffen ist der Mensch die unmittelbare Angriffsfläche für Cyberkriminelle und für andere motivierte Akteure. Im Rahmen von sogenannten Social Engineering Angriffen erlangen Angreifer durch Methoden des Trickbetrugs Zugang zu Informationen, die Sie für finanzielle oder Spionage-Zwecke verwenden können. Auch Verteidigungseinrichtungen bleiben vor solchen Angriffen nicht verschont. Effektive Verteidigungsstrategien gegen solche Angriffe sind immer noch Mangelware. Diese Forschungsstudie leistet einen Beitrag dazu, dies zu ändern.

Ziel und Verwendung der Forschungsstudie

Das Ziel der Forschungsstudie ist es, die Effektivität eines interaktiven Brettspiels mit Rollenspielcharakter als Methode zur Verringerung der persönlichen Anfälligkeit für Cyber-Trickbetrug experimentell zu testen. Ihre freiwillige Teilnahme an der Studie unterstützt uns, Verteidigungsstrategien gegen solche Angriffe zu evaluieren und zu verbessern. Mit Ihrer Teilnahme an der Studie tragen Sie massgeblich zur Steigerung der Cybersicherheit in der Schweizer Armee bei.

Ablauf der Studie

- QR-Code scannen (bitte halten Sie Ihre Teilnehmer-ID bereit und bewahren Sie diese auf)
- Durchlesen der Information zum Forschungsprojekt
- Abgabe der Einwilligungserklärung zur freiwilligen Teilnahme
- An Umfrage bis **spätestens 20.03.2022** teilnehmen
- Einen halben Tag Ihres WKs an einem Brettspiel mit anderen Kameraden teilnehmen (effektive Zuteilung durch Kdt [REDACTED]) ... und
- ...das Spiel ist aus!



Weitere Informationen zur Studie

Die Studie umfasst Fragebögen, Cyber-Trickbetrug Tests sowie ein interaktives Brettspiel. Der Fragebogen beinhaltet demografische Fragen, Fragen zur Selbstwahrnehmung und zur (Cyber-)Risikoeinstellung. Bei bestimmten Fragen steht es Ihnen frei, nicht zu antworten. Hierzu klicken Sie bei der betreffenden Frage einfach auf „Weiter“.

Ihre Daten werden gestützt durch Art. 4 Abs. 5, 13 und 22 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) erhoben und lediglich durch den Studienleiter bearbeitet.

F. Phishing Scenarios

Pre-Test Phishing mail

5 von 1.466 < > De

TEST: Weiterentwicklung Brigade - Kaderpotential (Difficulty 3) Posteingang x

[REDACTED] @vtg.admin.ch über asbas.ch 07.04.2022, 15:34 (vor 4 Tagen) ☆ ↶ ⋮

an mich

Sehr geehrte(r) Kamerad(in)

Wie Sie sicher aus der Grussbotschaft 2022 des Kdt [REDACTED] entnommen haben, werden in den kommenden Jahren strategisch relevante Projekte in der Organisation umgesetzt. Die Bildung des Cyber Bat 42, das Projekt Cyber Kommando und das Projekt TKA. Für die präventive Ressourcenplanung wurde ich vom Kommandanten befohlen, das Kaderpotential im Bataillon zu evaluieren.

Ich ordne daher für das [REDACTED] an, über Ihr generelles Interesse an einer Kaderausbildung mit «JA» oder «NEIN» innerhalb der nächsten 72 Stunden abzustimmen. [Hier](#) gelangen Sie zum Portal.

Vielen Dank für Ihre Kooperation.

Freundliche Grüsse

Oberstleutnant [REDACTED]

Kdt [REDACTED]

TEST: Développement de la brigade – formation des cadres (Difficulty 3) Posteingang x

[REDACTED] @vtg.admin.ch über asbas.ch Do., 7. Apr., 15:34 (vor 4 Tagen) ☆ ↶ ⋮

an mich

Cher(e) camarade

Comme vous l'avez certainement entendu sur le vidéo des vœux pour le Nouvel An du commandant br [REDACTED], des projets stratégiques importants seront mis en œuvre dans l'organisation au cours des prochaines années. La création du Cyber Bat 42, le projet Cyber commandement et le projet TKA. Pour la planification préventive des ressources, le commandant m'a ordonné d'évaluer le potentiel des cadres au sein du bataillon.

J'ordonne donc pour le [REDACTED] de voter sur votre intérêt général pour une formation de cadres par "OUI" ou "NON" dans les prochaines 72 heures. Vous pouvez accéder [ici](#) au portail.

Nous vous remercions de votre coopération.

Salutations amicales

Oberstleutnant [REDACTED]

Cmdt [REDACTED]

TEST: Ulteriore sviluppo della brigata - Potenziale della squadra (Difficulty 3) Posteingang x

[REDACTED] @vtg.admin.ch über asbas.ch Do., 7. Apr., 15:34 (vor 4 Tagen) ☆ ↶ ⋮

an mich

Italienisch > Deutsch [Nachricht übersetzen](#) [Deaktivieren für: Italienisch x](#)

Caro compagno

Come avrete capito dal messaggio di saluto 2022 della Comandante br [REDACTED] nei prossimi anni saranno realizzati progetti strategicamente rilevanti nell'organizzazione. La formazione del Cyber Bat 42, il progetto Cyber Command e il progetto TKA. Per la pianificazione preventiva delle risorse, il comandante mi ha ordinato di valutare il potenziale dei quadri nel battaglione.

Ordino quindi che la [REDACTED] voti il vostro interesse generale per la formazione dei quadri con "SI" o "NO" entro le prossime 72 ore. Potete accedere al portale [qui](#).

Grazie mille per la vostra collaborazione.

Cordiali saluti

Oberstleutnant [REDACTED]

Kdt [REDACTED]

https://vtg.admin.ch/de/Kaderausbildung.html?p=a3e00866-b69f-465f-b4d1-9fb08db47c

Der Bundesrat > Département: VBS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee

Themen A-Z

Startseite Jobs Kontakt DE FR IT EN

Altuell Service **Mein Militärdienst** Karriere Organisation / Truppe Die Schweizer Armee

Startseite > Mein Militärdienst > Aufgebotsdaten

Startseite

Mein Militärdienst

Kaderausbildung

Kaderausbildung

Bitte tragen Sie Ihren Namen ein und geben Sie Ihr Interesse an einer Kaderausbildung bekannt.

Coronavirus: Informationen für Armeeangehörige.

Information

Aufgrund der aktuellen Lage kann es zu kurzfristigen Anpassungen gewisser Dienstleistungsdaten kommen.

Für Fragen – siehe Kontaktdaten Link: Coronavirus: Informationen für Armeeangehörige.

Interessensbekundung Kaderausbildung

Name

Vorname Nachname

Ja Nein

Abschicken

11:40
11.04.2022

https://vtg.admin.ch/fr/Formation_des_cadres.html?p=b20320c2-0c03-434f-97ab-ae0d288b6f66

Le Conseil fédéral > Département: DDPS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Armée suisse

Thèmes A-Z

Page d'accueil Emploi Contact DE FR IT EN

Actualité Service **Mon service militaire** Carrière Organisation/Truppe L'Armée suisse

Page d'accueil > Mon service militaire > Dates de convocation

Page d'accueil

Mon service militaire

Formation des cadres

Formation des cadres

Veuillez inscrire votre nom et indiquer votre intérêt pour une formation de cadre.

Coronavirus: Informations pour les militaires.

Information

En raison de la situation actuelle liée à la pandémie de Covid-19, il faut s'attendre à des ajustements à court terme de certains services.

Pour toute question voir contact à droite ou le lien : Armée et coronavirus

Manifestation d'intérêt pour la formation des cadres

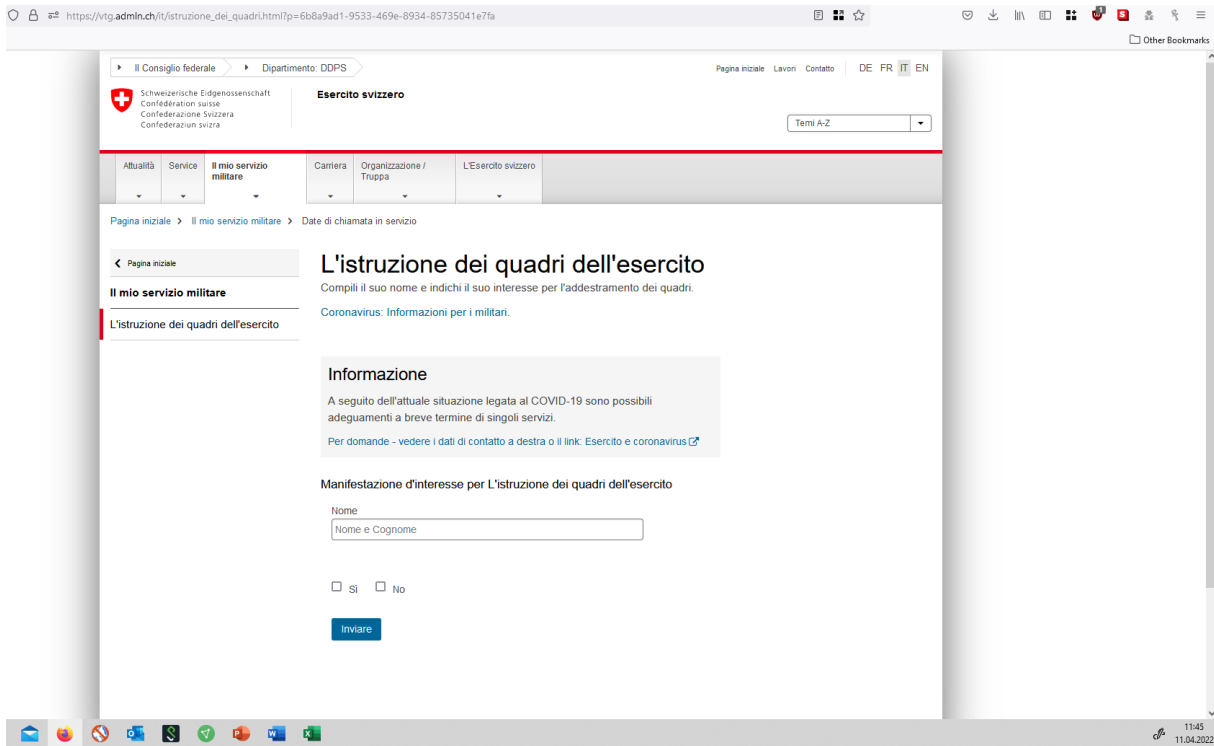
Nom

Prénom Nom

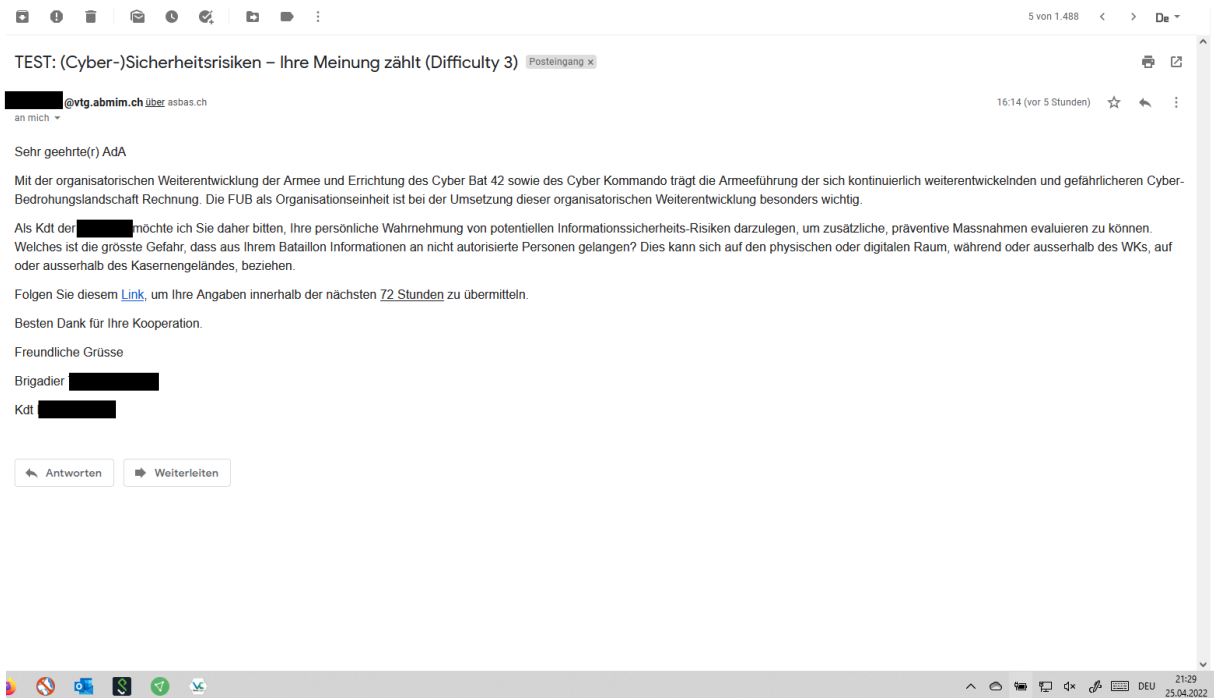
Oui Non

Envoyer

11:44
11.04.2022



Post-Test Phishing mail (1. Post-Test)



4 von 1.488 < > De -

TEST: Vulnérabilités de (cyber)sécurité - votre avis compte (Difficulty 3) [Posteingang x](#)

[@vtg.abmim.ch](#) über asbas.ch
an mich

16:14 (vor 5 Stunden) ☆ ↶ ⋮

Fransösisch > Deutsch > [Nachricht übersetzen](#) [Deaktivieren für: Französisch x](#)

Chers membres de l'armée

En poursuivant le développement organisationnel de l'armée et en créant le Cyber Bat 42, ainsi que le Cyber commandement, le commandement de l'armée tient compte du paysage des cybermenaces qui évolue continuellement et qui est de plus en plus dangereux. La BAC, en tant qu'unité organisationnelle, joue un rôle particulièrement important dans la mise en œuvre de ce développement organisationnel.

En tant que Cmdt br [REDACTED], je voudrais donc vous demander d'exposer votre perception personnelle des risques potentiels en matière de sécurité de l'information, afin de pouvoir évaluer des mesures préventives supplémentaires. Quel est le plus grand risque que des informations provenant de votre bataillon parviennent à des personnes non autorisées ? Il peut s'agir de l'espace physique ou numérique, pendant ou en dehors du cours de répétition, dans ou en dehors de l'enceinte de la caserne.

Suivez ce [lien](#) pour transmettre vos données dans les 72 heures.

Nous vous remercions de votre coopération.

Salutations amicales

Brigadier [REDACTED]

Cmdt br [REDACTED]

[↶ Antwoorden](#) [➔ Weiterleiten](#)

21:32 25.04.2022

6 von 1.488 < > De -

TEST: Vulnerabilità della sicurezza (cyber) - La vostra opinione conta (Difficulty 3) [Posteingang x](#)

[@vtg.abmim.ch](#) über asbas.ch
an mich

16:14 (vor 5 Stunden) ☆ ↶ ⋮

Italienisch > Deutsch > [Nachricht übersetzen](#) [Deaktivieren für: Italienisch x](#)

Cari membri delle forze armate

Con l'ulteriore sviluppo organizzativo delle forze armate e l'istituzione della Cyber Bat 42 e della Cyber Command, la direzione delle forze armate sta tenendo conto del panorama delle minacce informatiche in continua evoluzione e più pericoloso. La FUB come unità organizzativa è particolarmente importante nella realizzazione di questo sviluppo organizzativo.

Come Commandante br [REDACTED] vorrei quindi chiedervi di dichiarare la vostra personale percezione dei potenziali rischi per la sicurezza delle informazioni, al fine di poter valutare ulteriori misure preventive. Qual è il maggior rischio di fuga di informazioni dal suo battaglione a persone non autorizzate? Questo può riguardare lo spazio fisico o digitale, durante o fuori il corso di ripetizione, dentro o fuori la caserma.

Segui questo [link](#) per inviare i tuoi dati entro le prossime 72 ore.

Grazie per la vostra collaborazione.

Cordiali saluti

Brigadier [REDACTED]

Commandante br [REDACTED]

[↶ Antwoorden](#) [➔ Weiterleiten](#)

21:33 25.04.2022

Post-Test landing pages (1. Post-Test)

The screenshot shows a web browser window with the URL <https://vrtg.abmim.ch/de/Schwachstellenmeldung.html?p=e63654d3-7e79-49e3-8a84-a75e08e888df>. The page is for the Swiss Army (Schweizer Armee) and is titled 'Schwachstellenmeldung'. The main heading is 'IKT-Sicherheit ist ein Prozess und kein Zustand'. The text below the heading discusses the organizational development of the army and the importance of cybersecurity. There is a large empty text box for 'Anonyme Schwachstellenmeldung' and a blue 'Abschicken' button at the bottom.

Der Bundesrat > Departement: VBS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee

Themen A-Z

Aktuell Service Mein Militärdienst Karriere Organisation / Truppe Die Schweizer Armee

Startseite > Schwachstellenmeldung

← Startseite

IKT-Sicherheit ist ein Prozess und kein Zustand

Mit der organisatorischen Weiterentwicklung der Armee und Errichtung des Cyber Bat 42 sowie des Cyber Kommando trägt die Armeeführung der sich kontinuierlich weiterentwickelnden und gefährlicheren Cyber-Bedrohungslandschaft Rechnung. Die FUB als Organisationseinheit ist bei der Umsetzung dieser organisatorischen Weiterentwicklung besonders wichtig. Die Schweizer Armee ist auch auf Hinweise zu potentiellen physischen und technischen Sicherheitsrisiken der AdA angewiesen.

Anonyme Schwachstellenmeldung

Abschicken

21:31
25.04.2022

The screenshot shows a web browser window with the URL https://vrtg.abmim.ch/fr/Declaration_de_vulnerabilite.html?p=7a6aa232-d4bc-4745-8e9a-4dfeffec9734. The page is for the Swiss Army (Armée suisse) and is titled 'Déclaration de vulnérabilité'. The main heading is 'La sécurité informatique est un processus et non pas un état'. The text below the heading discusses the organizational development of the army and the importance of cybersecurity. There is a large empty text box for 'Déclaration anonyme des vulnérabilités' and a blue 'Envoyer' button at the bottom.

Le Conseil fédéral > Département: DDPS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Armée suisse

Thèmes A-Z

Actualité Service Mon service militaire Carrière Organisation/Troupe L'Armée suisse

Page d'accueil > Déclaration de vulnérabilité

← Page d'accueil

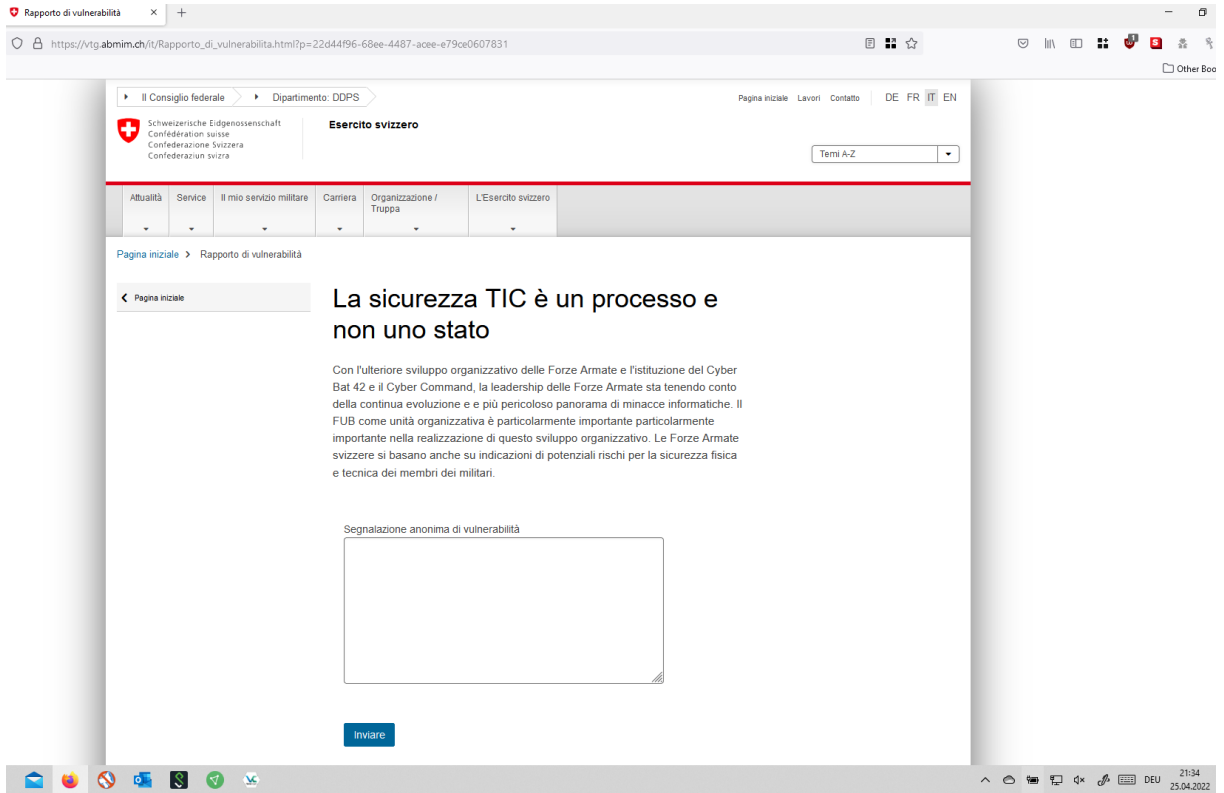
La sécurité informatique est un processus et non pas un état

Avec le développement organisationnel de l'armée et la mise en place du bat cyber 42 ainsi que le commandement cybernétique, le commandement de l'armée tient compte de l'évolution constante et menaces cybernétiques de plus en plus dangereuses. La BAC, en tant qu'unité organisationnelle, joue un rôle important dans la mise en œuvre de cette évolution organisationnelle est particulièrement importante. L'armée suisse a également besoin d'indications sur les risques potentiels pour la sécurité physique et technique des militaires.

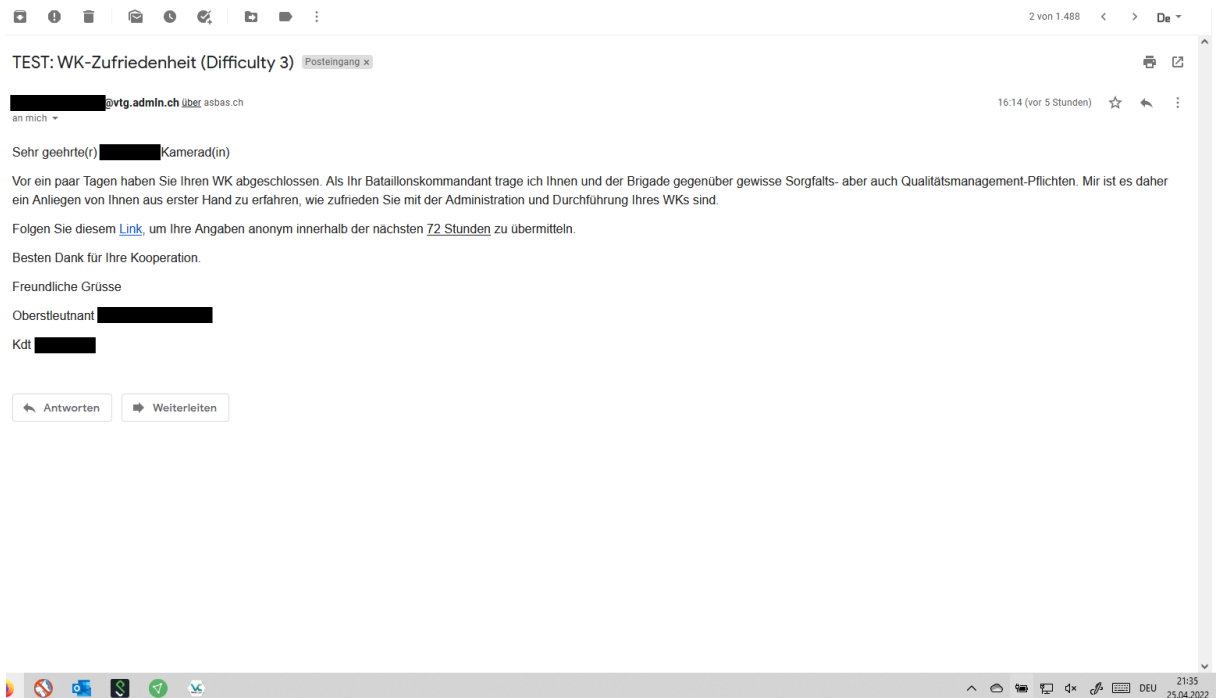
Déclaration anonyme des vulnérabilités

Envoyer

21:33
25.04.2022



Post-Test Phishing mail (2. Post-Test)



1 von 1.488 < > De

TEST: Satisfaction avec le cours de répétition (Difficulty 3) Posteingang x

[REDACTED] @vtg.admin.ch über asbas.ch 16:14 (vor 5 Stunden) ☆ ↶ ⋮
an mich

Cher(e) camarade de [REDACTED]

Il y a quelques jours, vous avez terminé votre cours de répétition. En tant que commandant de votre bataillon, j'ai certaines obligations de diligence et de gestion de la qualité envers vous et la brigade. Il me tiens donc à cœur d'entendre directement par vous dans quelle mesure vous êtes satisfait(e) de l'administration et du déroulement de votre cours de répétition.

Suivez [ce lien](#) pour transmettre vos données de manière anonyme dans les [72 heures](#).

Nous vous remercions de votre coopération.

Salutations amicales

Oberstleutnant [REDACTED]

Cmdt [REDACTED]

↶ Antworten ↷ Weiterleiten

21:37 25.04.2022

3 von 1.488 < > De

TEST: Soddifazione per il corso di ripetizione (Difficulty 3) Posteingang x

[REDACTED] @vtg.admin.ch über asbas.ch 16:14 (vor 5 Stunden) ☆ ↶ ⋮
an mich

Italienisch > Deutsch Nachricht übersetzen Deaktivieren für: Italienisch x

Caro compagno del [REDACTED]

Qualche giorno fa hai completato il tuo corso di ripetizione. Come vostro comandante di battaglione, ho certi doveri di cura e di gestione della qualità verso di voi e la brigata. Vorrei quindi sentire da voi in prima persona quanto siete soddisfatti dell'amministrazione e della realizzazione del vostro corso di formazione.

Segui questo [link](#) per inviare anonimamente le tue informazioni entro le prossime [72 ore](#).

Grazie mille per la vostra collaborazione.

Cordiali saluti

Oberstleutnant [REDACTED]

Commandante [REDACTED]

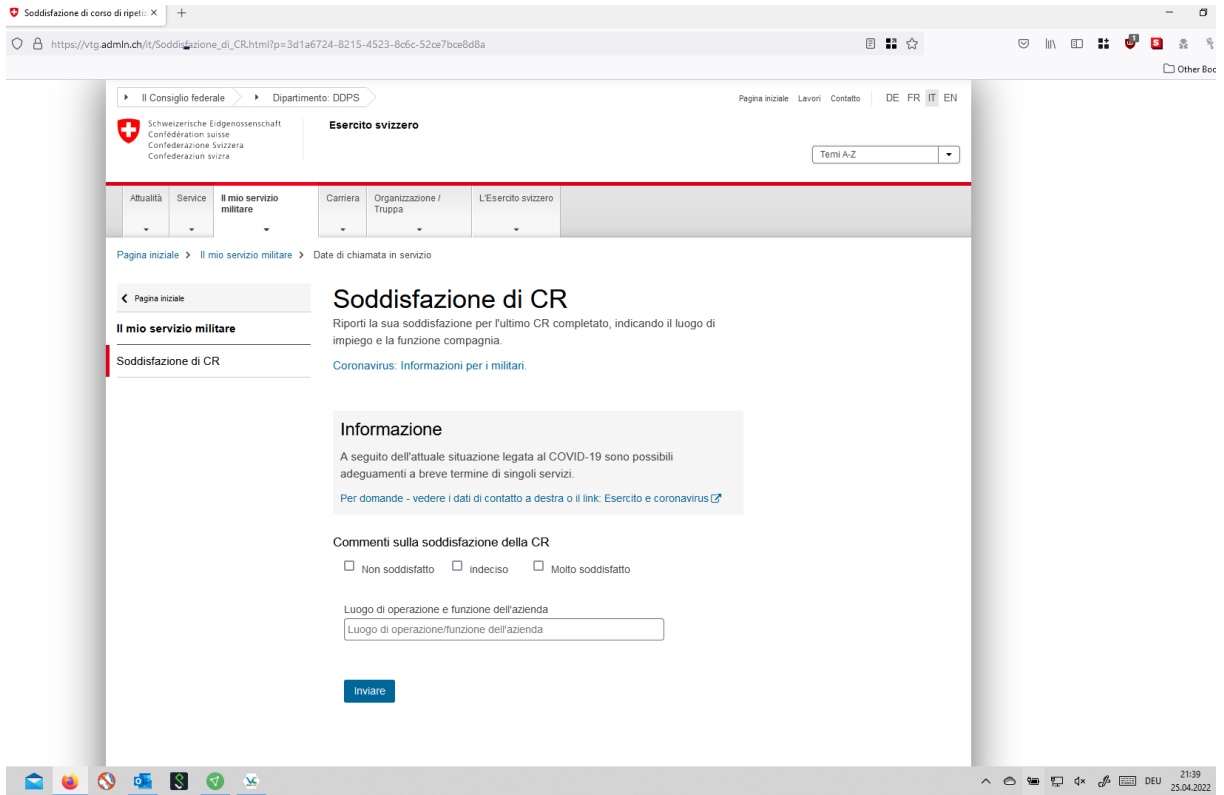
↶ Antworten ↷ Weiterleiten

21:38 25.04.2022

Post-Test landing page (2. Post-Test)

The screenshot shows a web browser window with the URL <https://vtg.admin.ch/de/WKZufriedenheit.html?p=0ct8cd36-b54f-4cfe-9558-8aaeb34338c7>. The page is for the 'Schweizer Armee' (Swiss Army) and is titled 'WK Zufriedenheit'. It features a navigation menu with 'Aktuell', 'Service', 'Mein Militärdienst', 'Karriere', 'Organisation / Truppe', and 'Die Schweizer Armee'. The main content area includes a breadcrumb trail 'Startseite > Mein Militärdienst > Aufgebotsdaten', a 'Startseite' button, and a 'Mein Militärdienst' section. The title 'WK Zufriedenheit' is followed by the instruction: 'Bitte melden Sie Ihre Zufriedenheit mit dem letzten absolvierten WK unter Angabe des Einsatzortes und der Kompaniefunktion zurück.' Below this is a link for 'Coronavirus: Informationen für Armeeingehörige.' An 'Information' box states: 'Aufgrund der aktuellen Lage kann es zu kurzfristigen Anpassungen gewisser Dienstleistungsdaten kommen. Für Fragen – siehe Kontaktdaten Link: Coronavirus: Informationen für Armeeingehörige.' The 'Rückmeldung WK Zufriedenheit' section contains three radio buttons: 'Nicht zufrieden', 'Unentschieden', and 'Sehr zufrieden'. A text input field is labeled 'Einsatzort und Kompaniefunktion' with the placeholder 'Einsatzort/Kompaniefunktion'. A blue 'Abschicken' button is at the bottom.

The screenshot shows a web browser window with the URL https://vtg.admin.ch/fr/Satisfaction_de_la_CR.html?p=3e8696c6-5883-49d5-9768-09e5e8ed27d1. The page is for the 'Armée suisse' (Swiss Army) and is titled 'Satisfaction de CR'. It features a navigation menu with 'Actualité', 'Service', 'Mon service militaire', 'Carrière', 'Organisation/Truppe', and 'L'Armée suisse'. The main content area includes a breadcrumb trail 'Page d'accueil > Mon service militaire > Dates de convocation', a 'Page d'accueil' button, and a 'Mon service militaire' section. The title 'Satisfaction de CR' is followed by the instruction: 'Merci de nous faire part de votre satisfaction concernant le dernier CR que vous avez effectué, en précisant le lieu d'affectation et la fonction de la compagnie.' Below this is a link for 'Coronavirus: Informations pour les militaires.' An 'Information' box states: 'En raison de la situation actuelle liée à la pandémie de Covid-19, il faut s'attendre à des ajustements à court terme de certains services. Pour toute question voir contact à droite ou le lien : Armée et coronavirus.' The 'Retour d'information sur la satisfaction de CR' section contains three radio buttons: 'Pas satisfait', 'indécis', and 'Très satisfait'. A text input field is labeled 'Lieu d'intervention et fonction de compagnie' with the placeholder 'Lieu d'intervention/fonction de compagnie'. A blue 'Envoyer' button is at the bottom.



G. Post serious game questionnaire

What is your participant-ID?

Please write your answer here:

How satisfied are you with the whole event?

Please choose the appropriate response for each item:

Very unsatisfied Unsatisfied Neutral Satisfied Very satisfied

How valuable do you consider the introductory presentation?

Please choose the appropriate response for each item:

Not at all valuable Not valuable Neutral Valuable Very valuable

How satisfied are you with the game master of your table?

Please choose the appropriate response for each item:

Very unsatisfied	Unsatisfied	Neutral	Satisfied	Very satisfied
---------------------	-------------	---------	-----------	-------------------

How valuable was the interactive serious game to you?

Please choose the appropriate response for each item:

Not at all valuable	Not valuable	Neutral	Valuable	Very valuable
------------------------	--------------	---------	----------	------------------

How much do you agree with the following statement:

The serious game has contributed to my knowledge about social engineering?

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

How much do you agree with the following statement:

I am now more aware of the threats posed by social engineering than before the event.

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
----------------------	----------	---------	-------	-------------------

How likely is the event to help you avoid becoming a victim of social engineering?

Please choose the appropriate response for each item:

Very unlikely	Unlikely	Neutral	Likely	Very likely
---------------	----------	---------	--------	----------------

Do you have any suggestions for improvement?

Please choose the appropriate response for each item:

YES NO

Please specify your suggestions for improvement

Only answer this question if the following conditions are met:

Answer was 'YES' at question ' [D9]' (Do you have any suggestions for improvement? ())

Thank you very much for taking the time and completing the survey. Your responses are now saved and transmitted.

04-28-2022 – 19:11

Submit your survey.

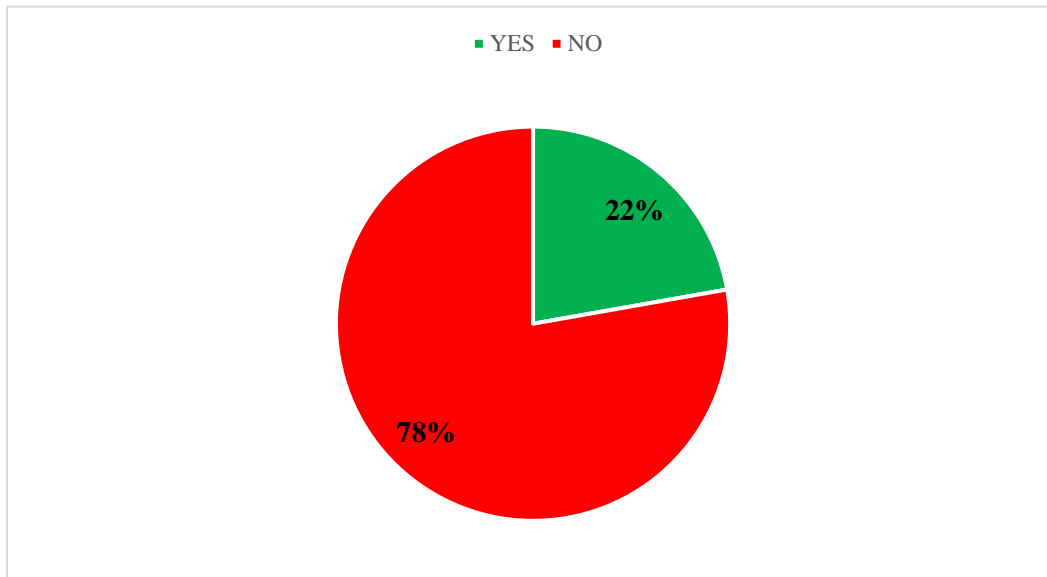
Thank you for completing this survey.

H. Pre- and Post Serious Game survey and Phishing results

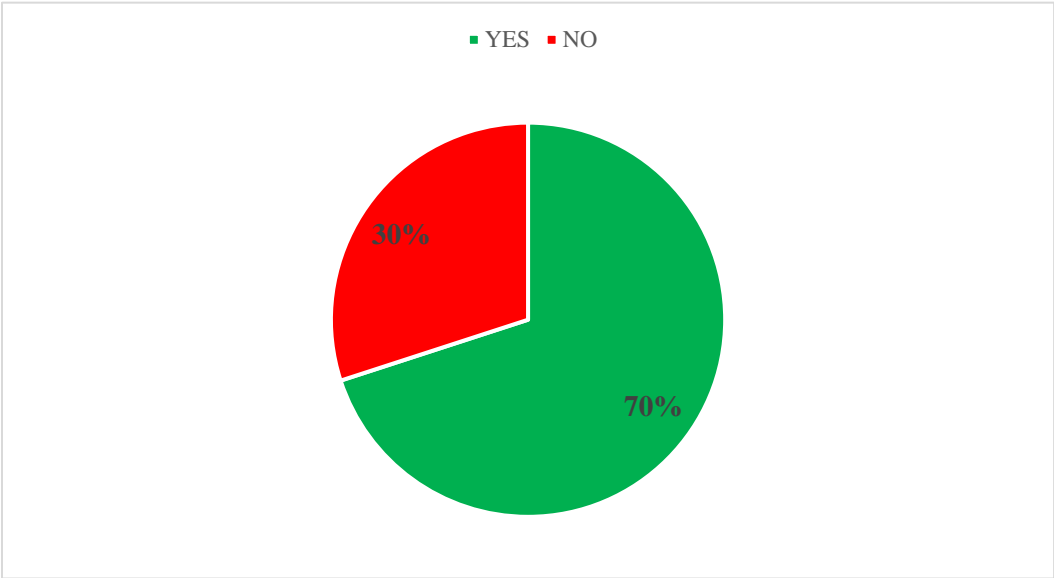
1. Pre-Serious Game Survey Results

1.1 Information Security Training and Importance

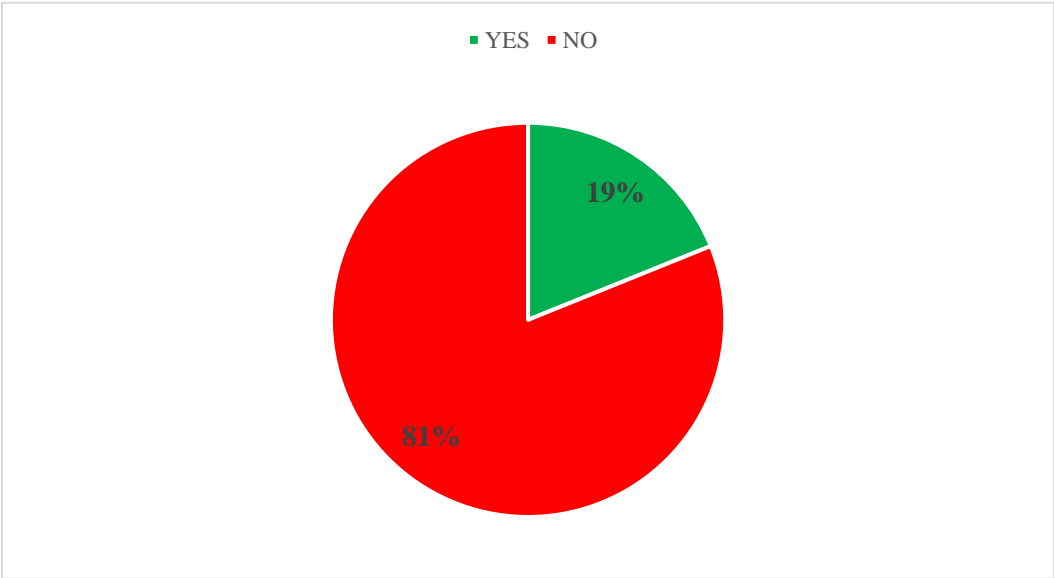
D04. In the last 12 months, did you participate in a training that focused on how to protect personal data and information?



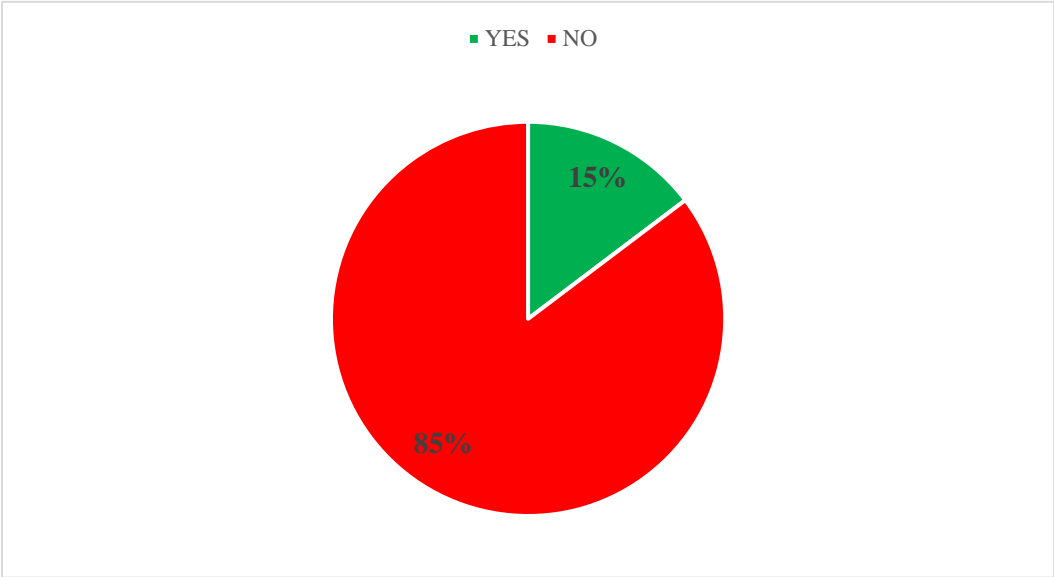
D04a. Was it an online training?



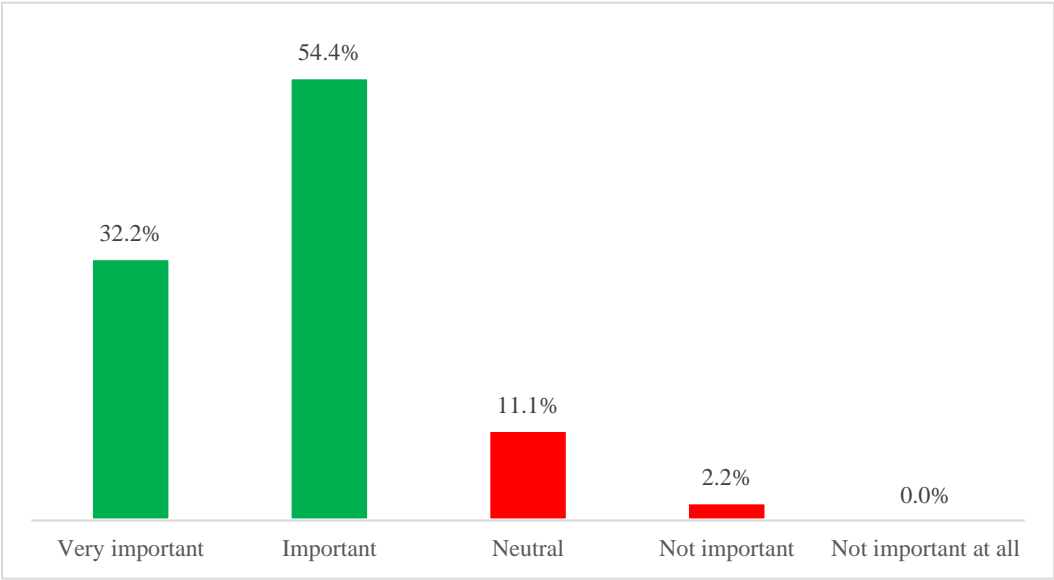
D05. In the last 12 months, did you participate in a training that focused on how to protect military-related data and information?



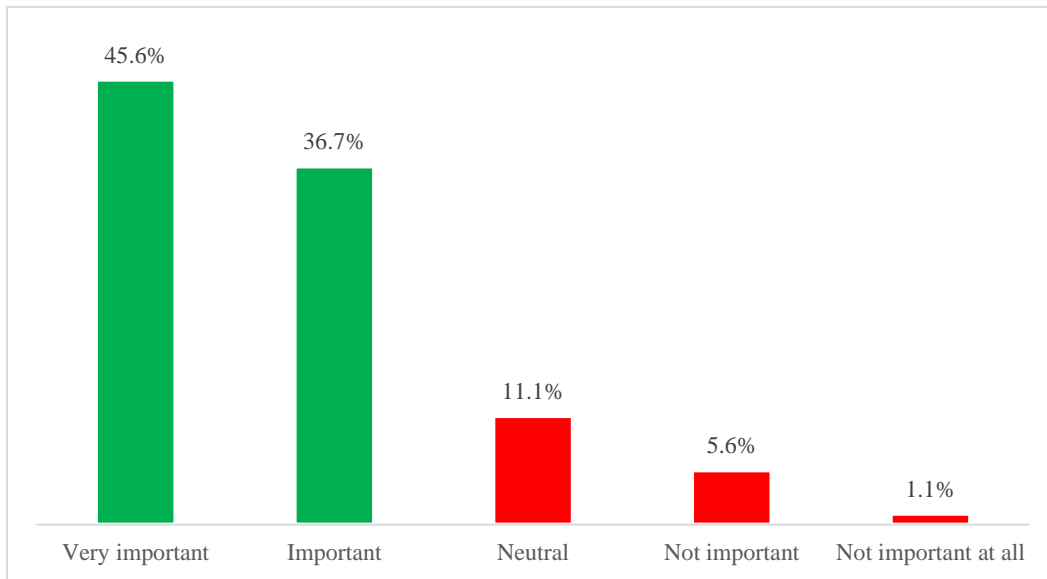
D05a. Was it an online training?



D06. How important do you consider the security of personal information in your daily life?

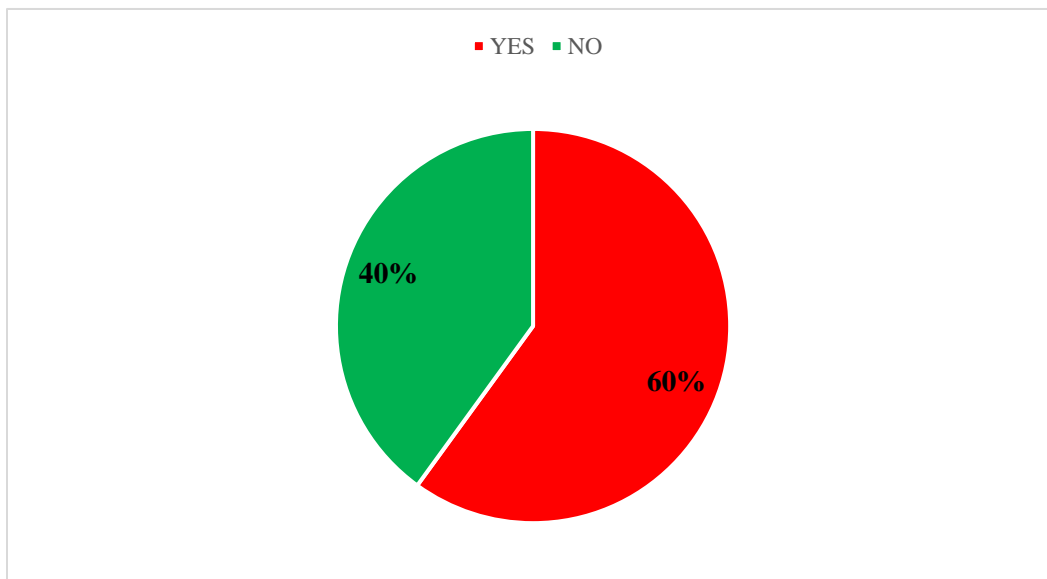


D07. How important do you consider the security of military-related information in daily life?

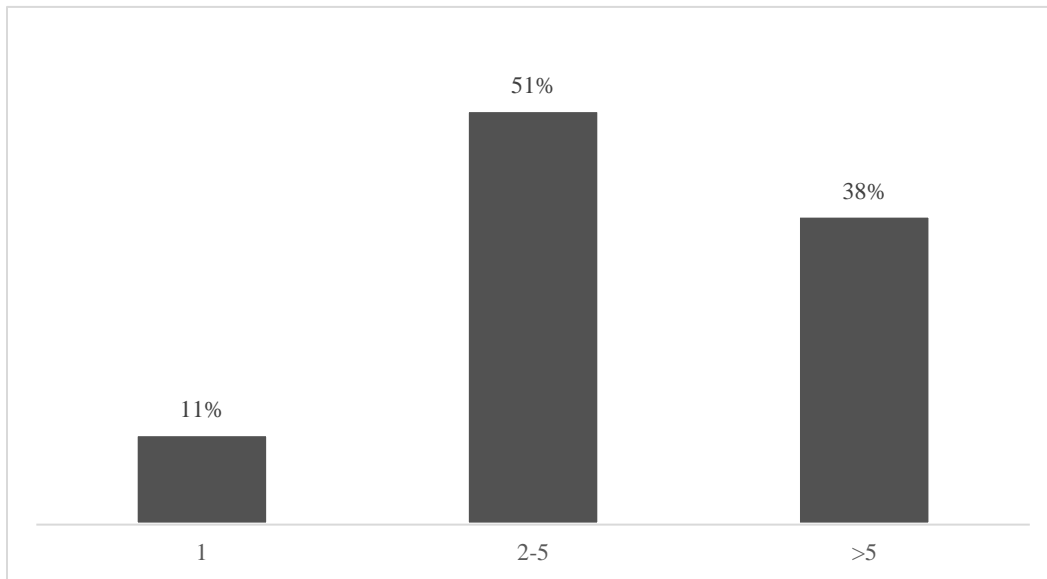


1.2 Victimization

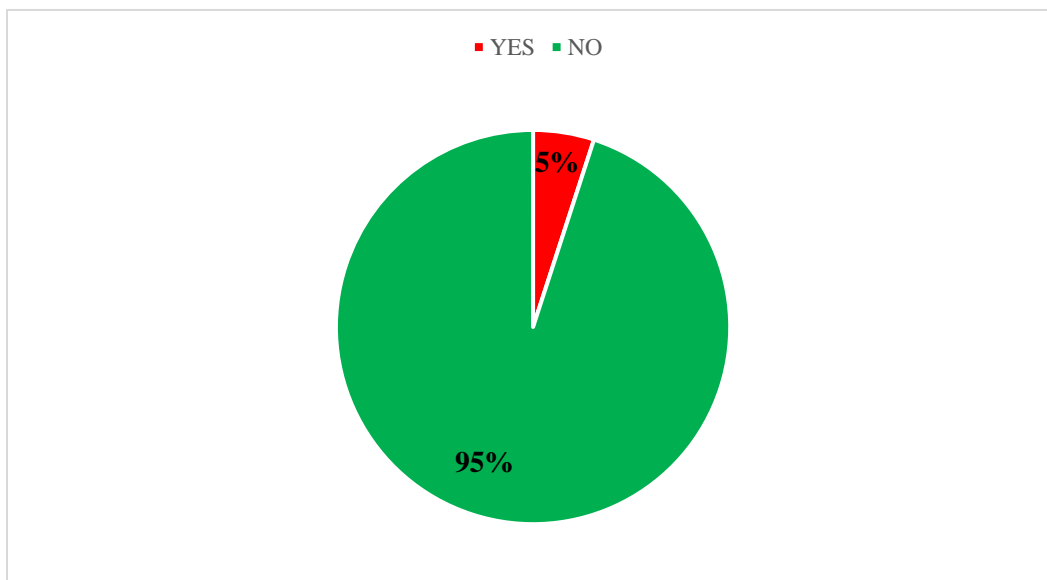
V01. In the past 12 months, have you ever received an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords?



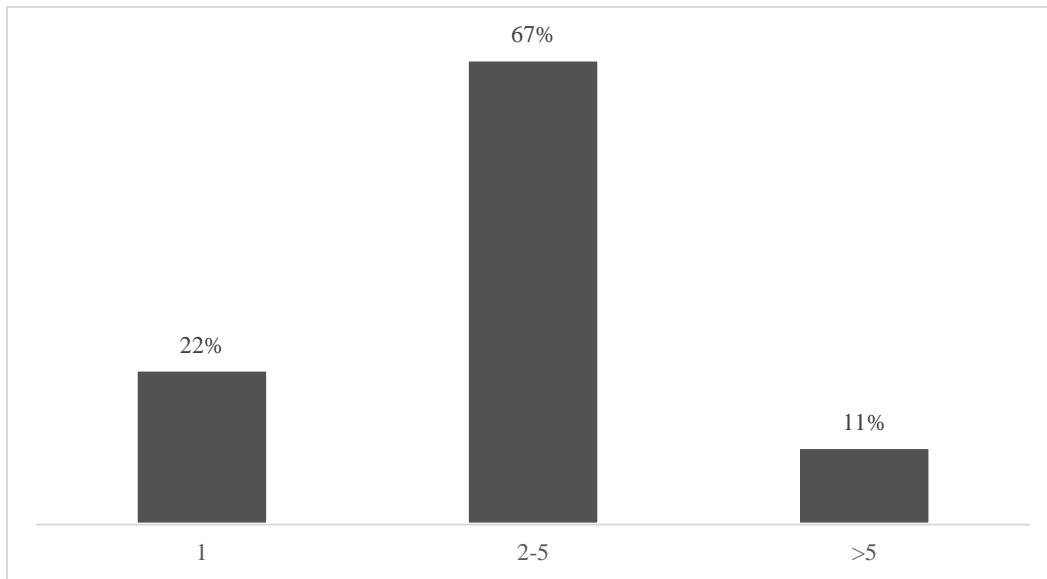
V01a. How often?



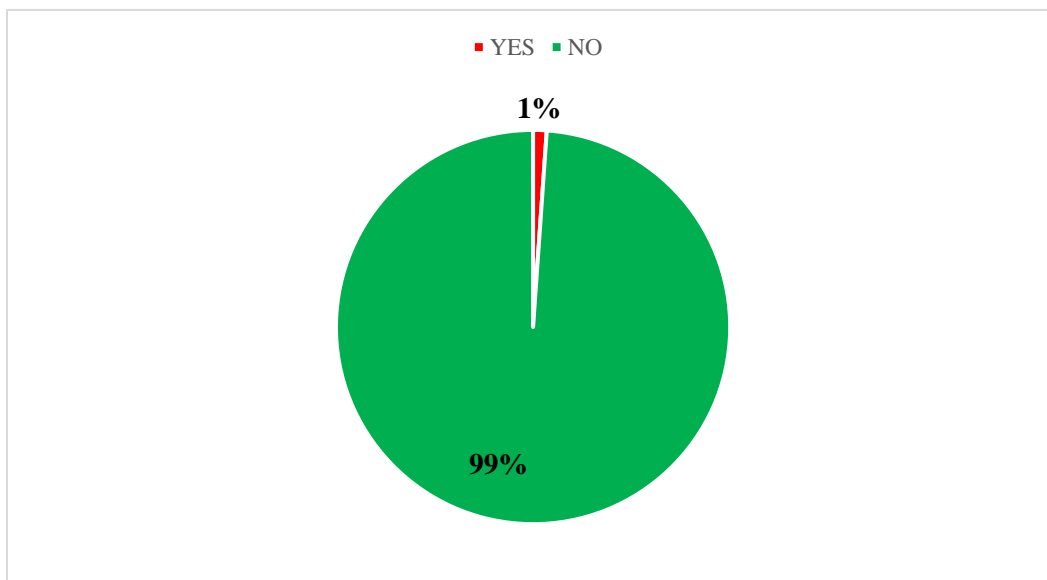
V02. In the past 12 months, have you ever opened an email link sent by someone who - posing as a trusted institution- asked you to provide sensitive data such as personally identifiable information, banking and credit card details, and passwords?



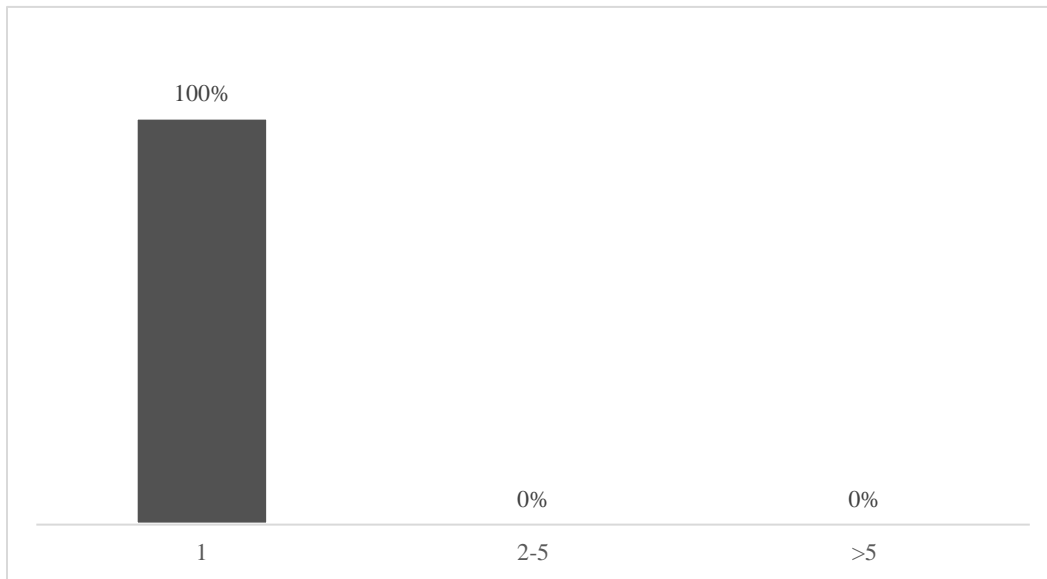
V02a. How often?



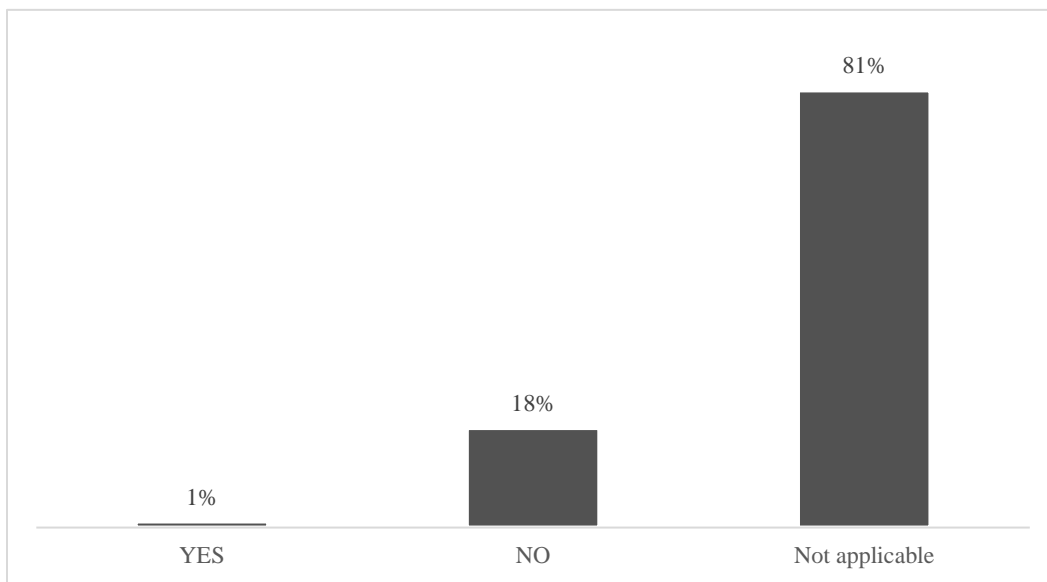
V03. In the past 12 months, have you ever sent online sensitive data (personally identifiable information, banking and credit card details, and passwords) to someone - posing as a trusted institution- who sent you the request through an email?



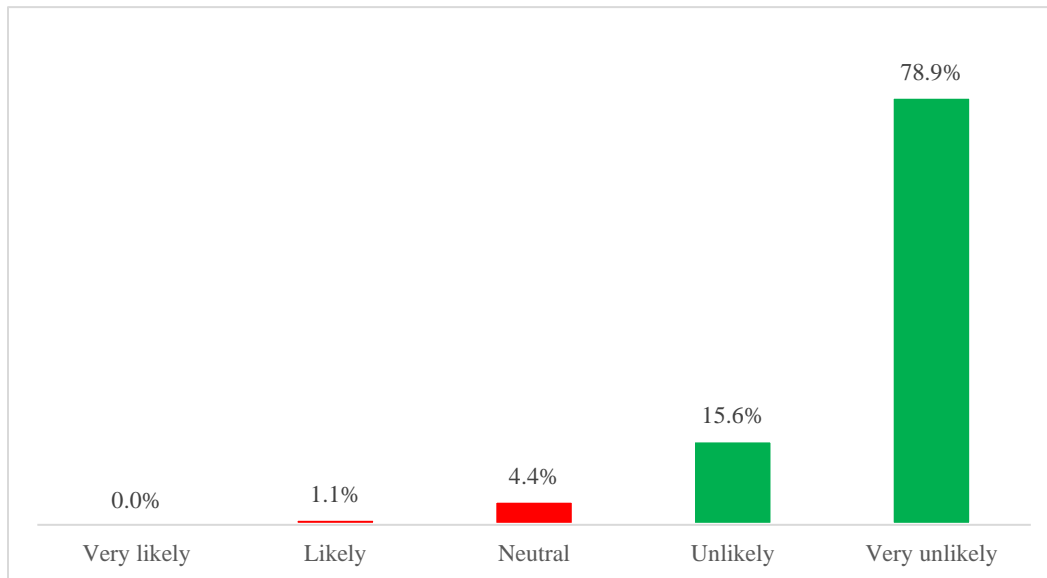
V03a. How often?



V05. Did you report the fact to police?



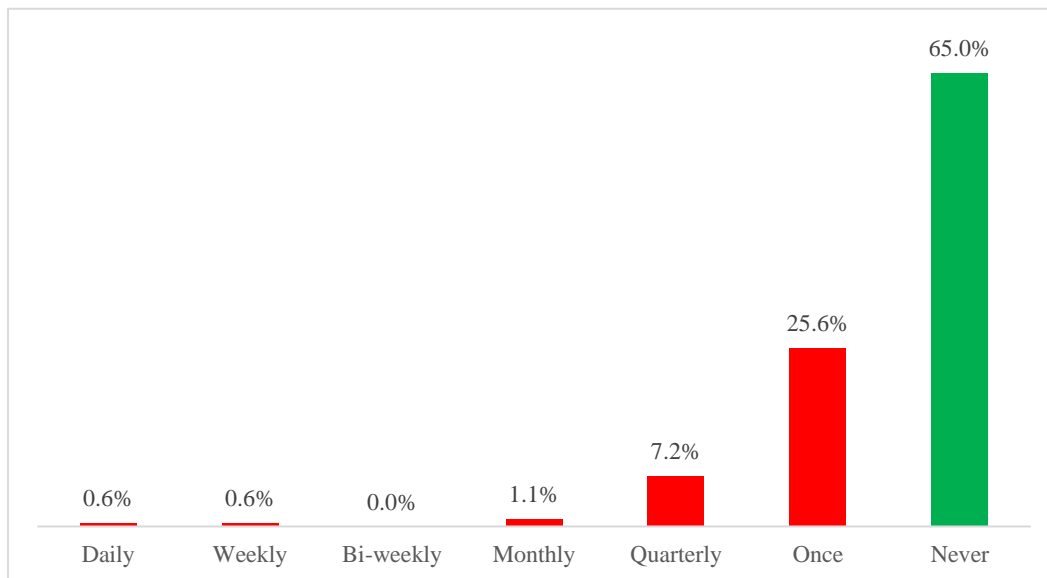
V06. In the next 12 months, how likely is it you, involuntary, disclose personal information online to someone who via email - posing as a trusted institution - asked you to provide sensitive data (e.g. banking and credit card details, and passwords)?



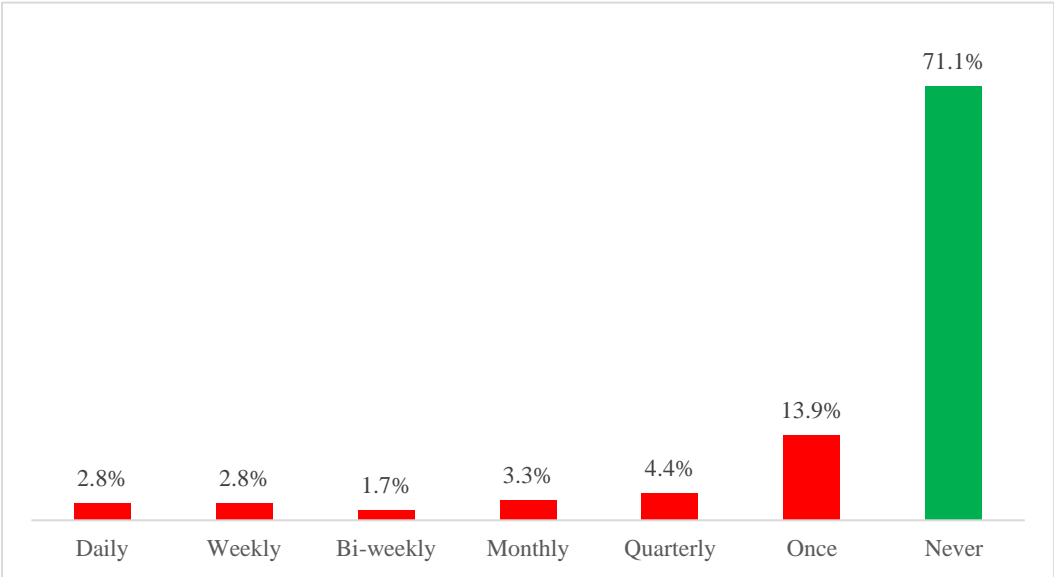
1.3 Risky Cybersecurity Behaviours (RCsB)

The RCsB inventory asked participants 20 questions about their personal behaviour with respect to cybersecurity during the last 6 months before the questionnaire.

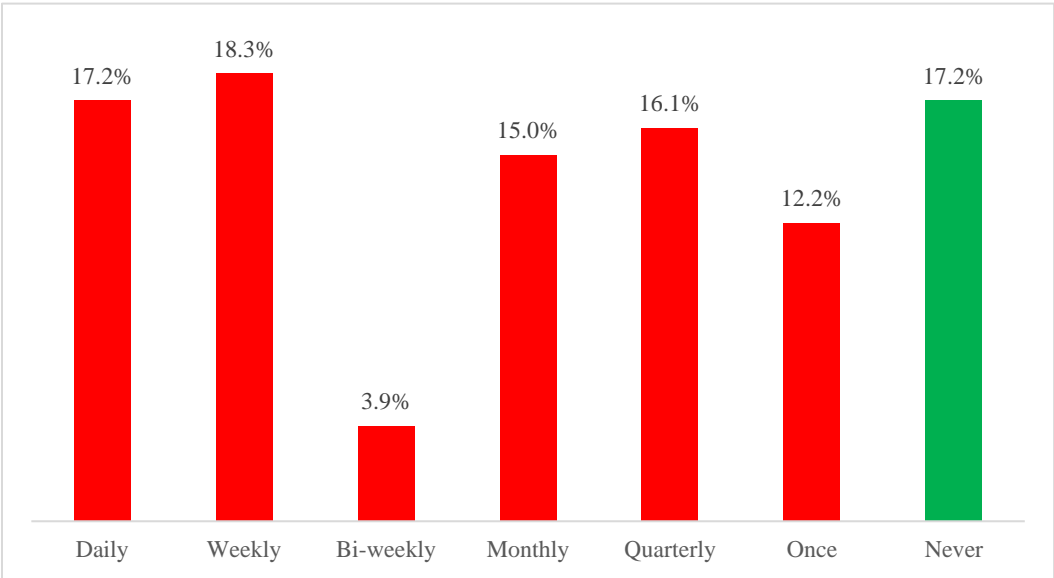
RB01. Sharing passwords with friends and colleagues.



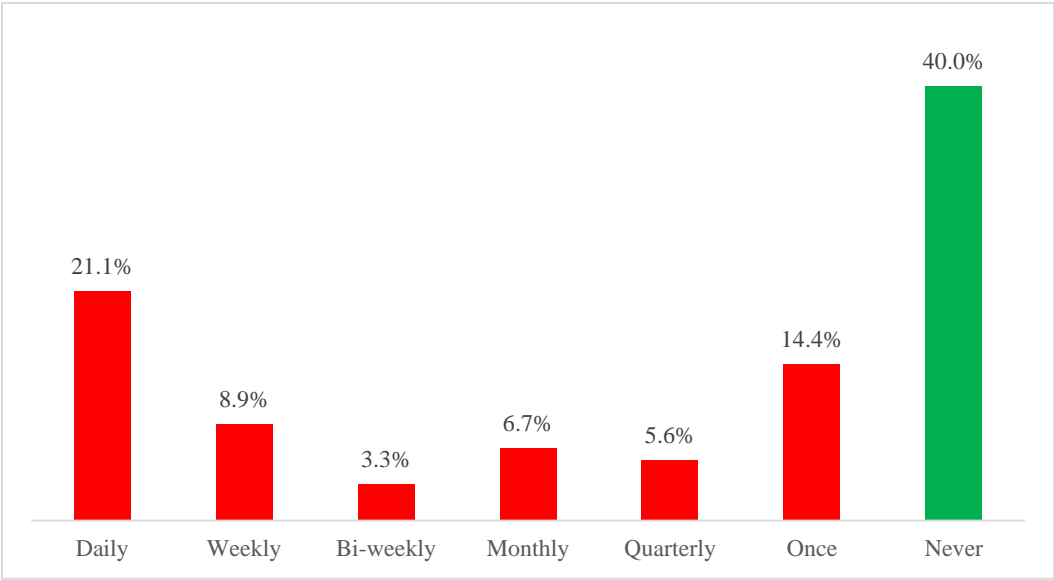
RB02. Using or creating passwords that are not very complicated (e.g. family name and date of birth).



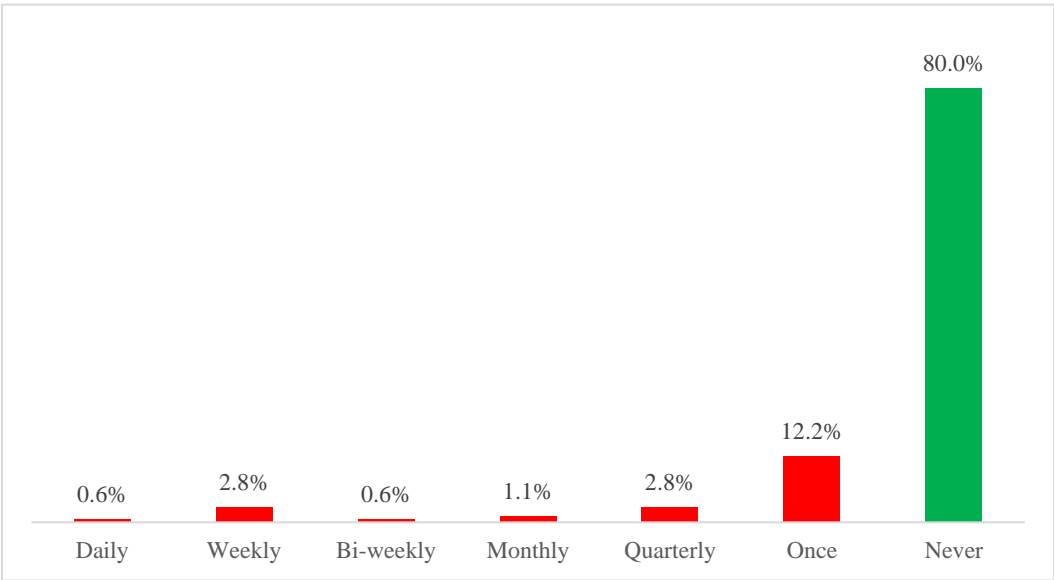
RB03. Using the same password for multiple websites.



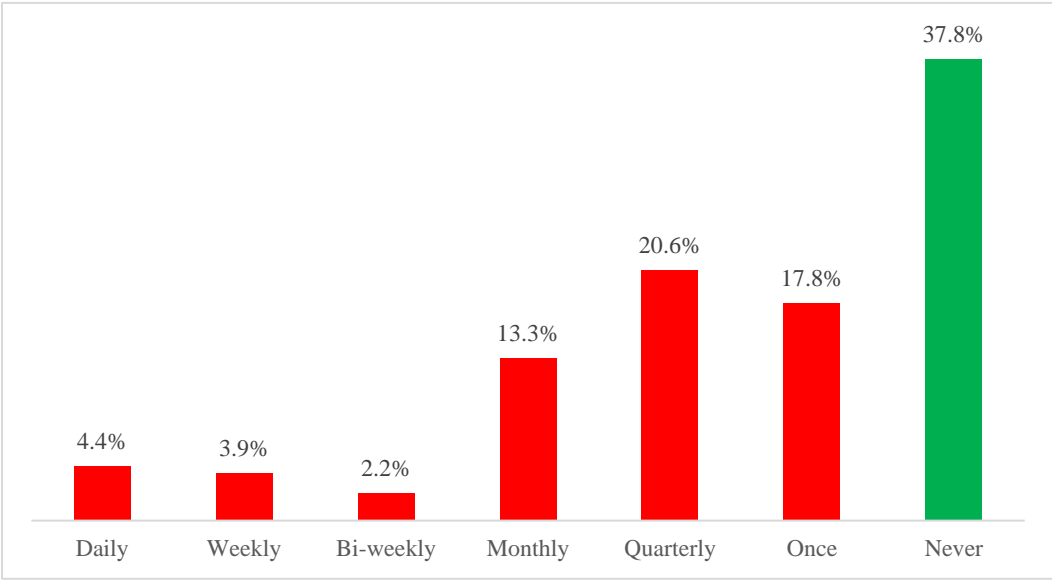
RB04. Using online storage systems to exchange and keep personal or sensitive information.



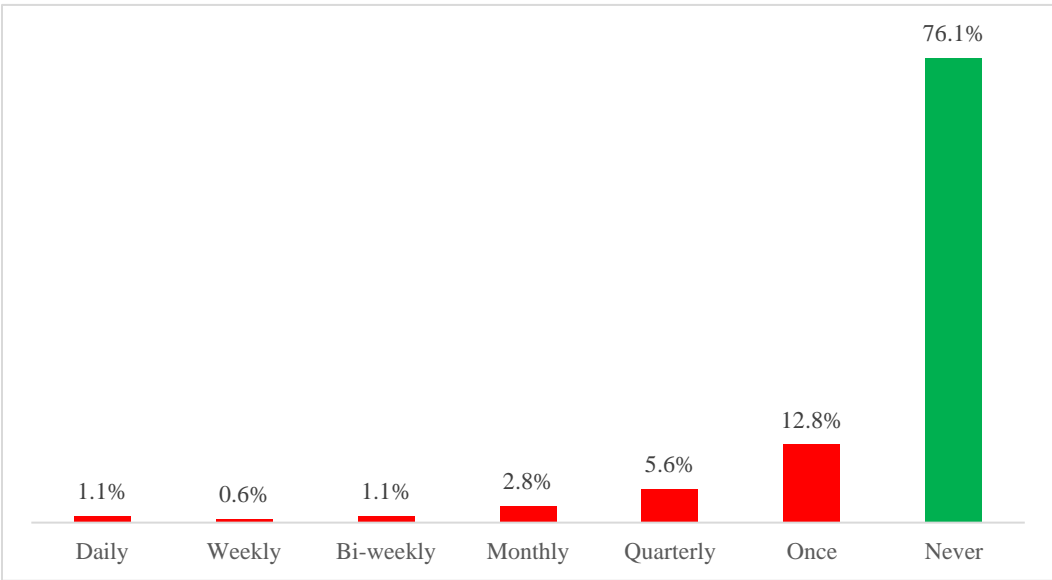
RB05. Entering payment information websites that have no clear security information/certification.



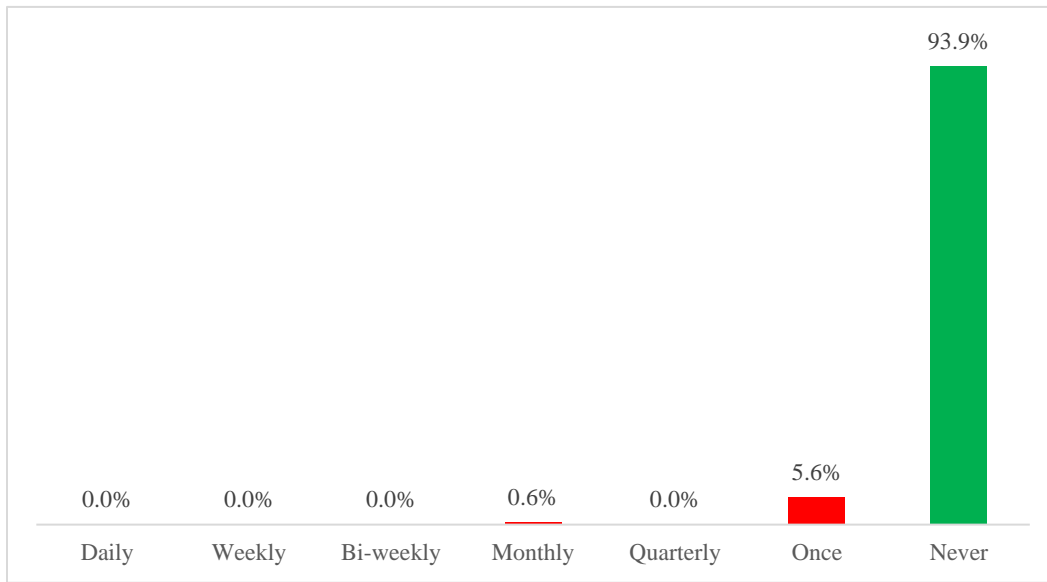
RB06. Using free-to-access public Wi-Fi.



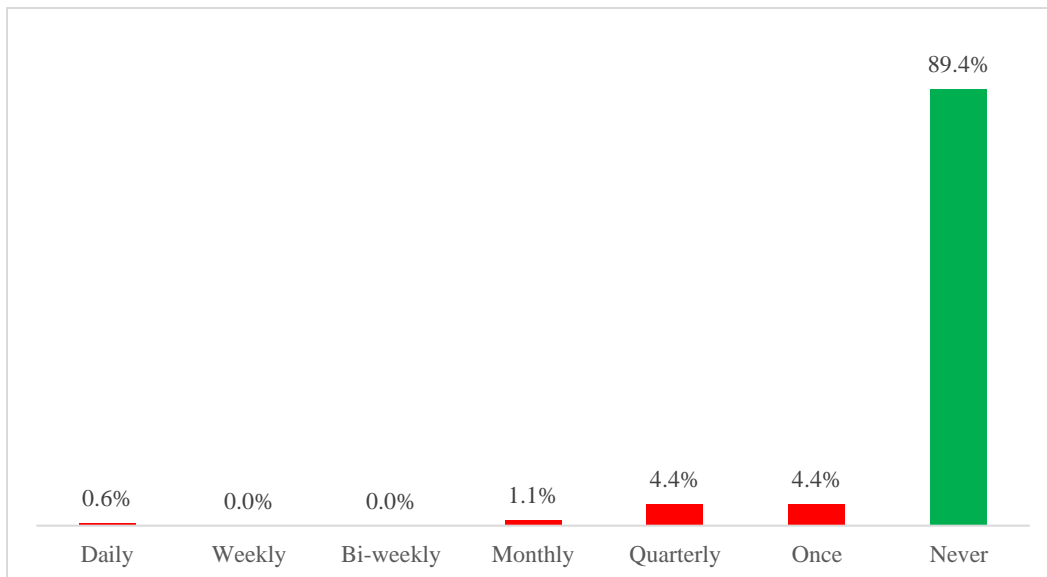
RB07. Relying on a trusted friend or colleague to advise you on aspects of online-security.



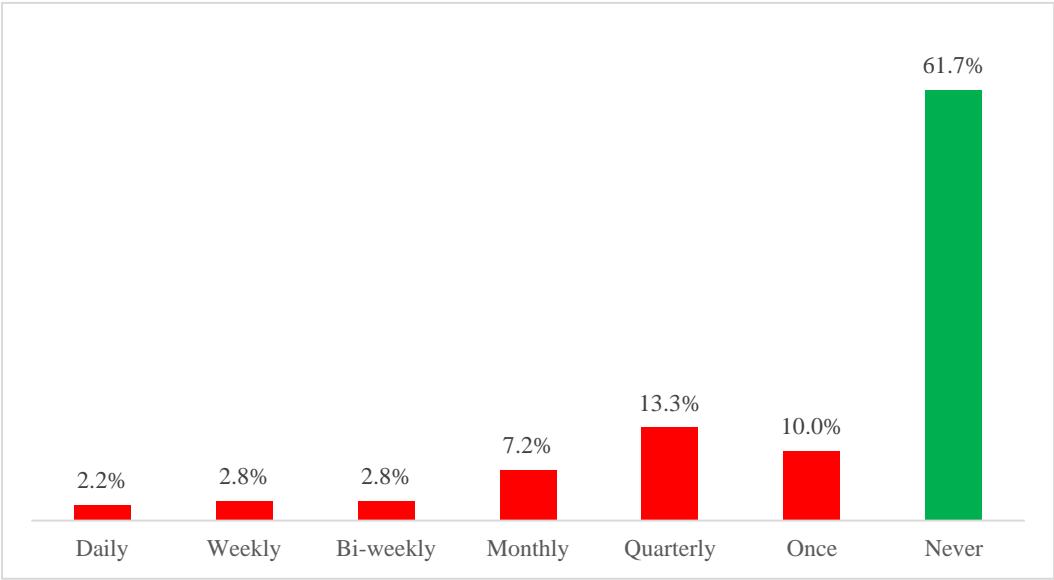
RB08. Downloading free anti-virus software from an unknown source.



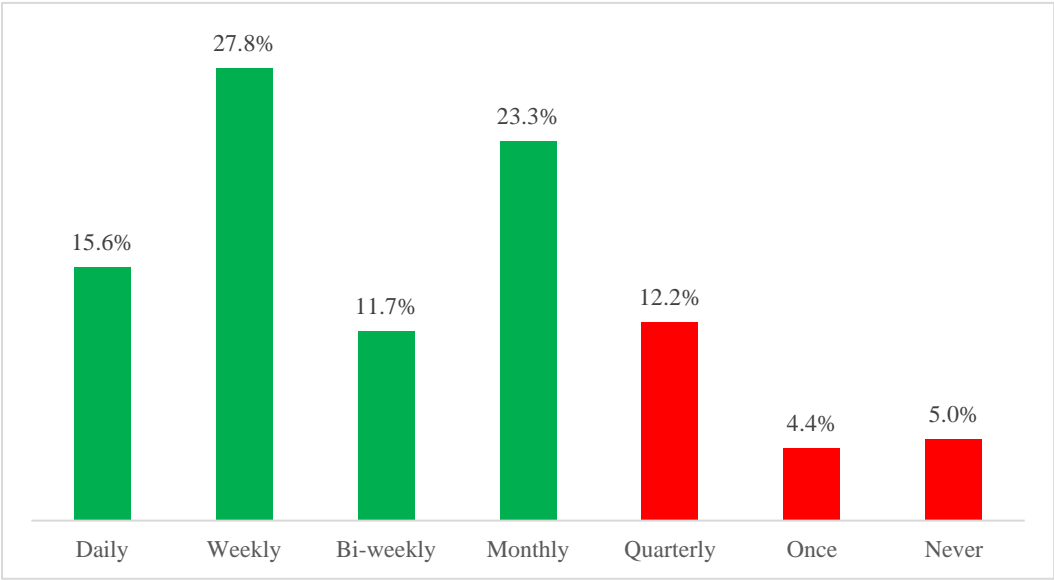
RB09. Disabling the anti-virus on my work computer so that I can download information from websites.



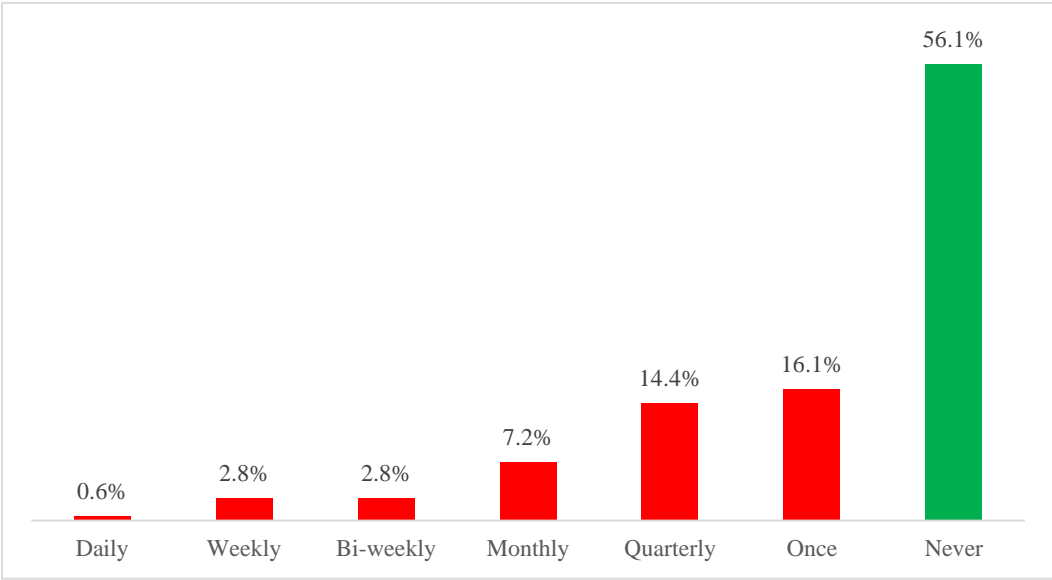
RB10. Bringing in my own USB to work in order to transfer data on to it.



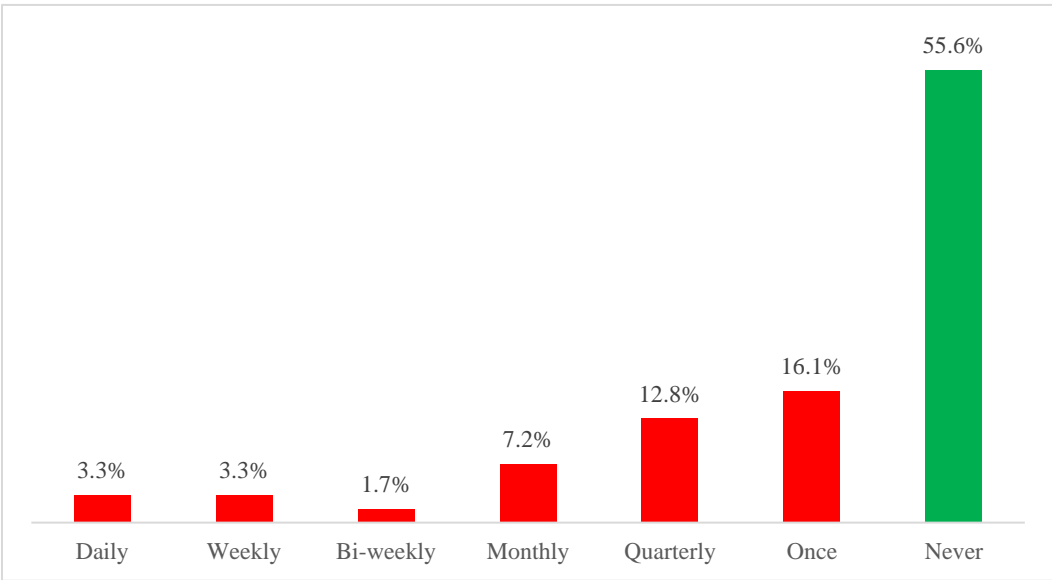
B11. Checking that software for your smartphone/tablet/laptop/Pc is up-to-date.



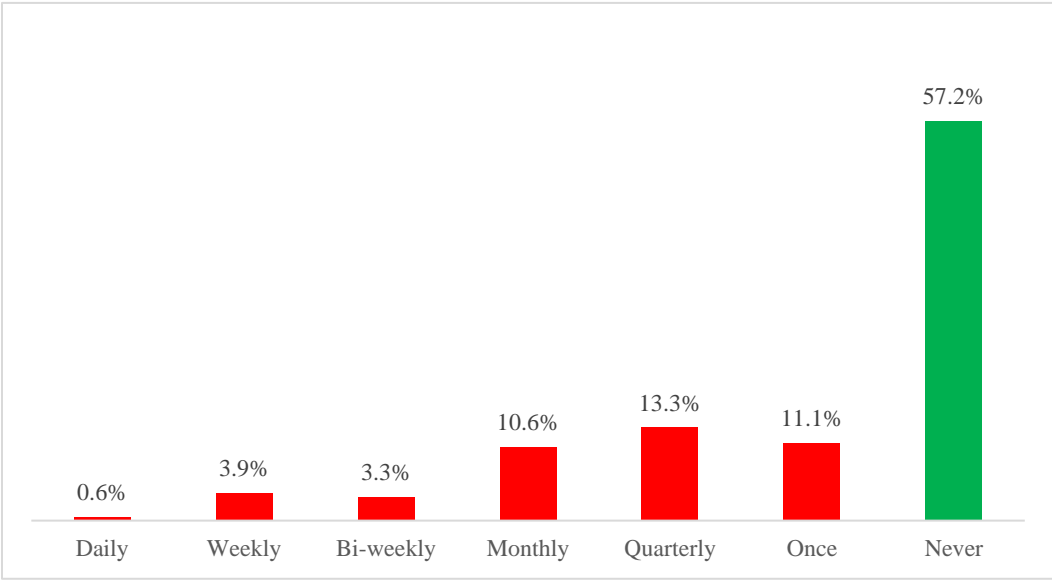
RB12. Downloading digital media (music, films, games) from unlicensed sources.



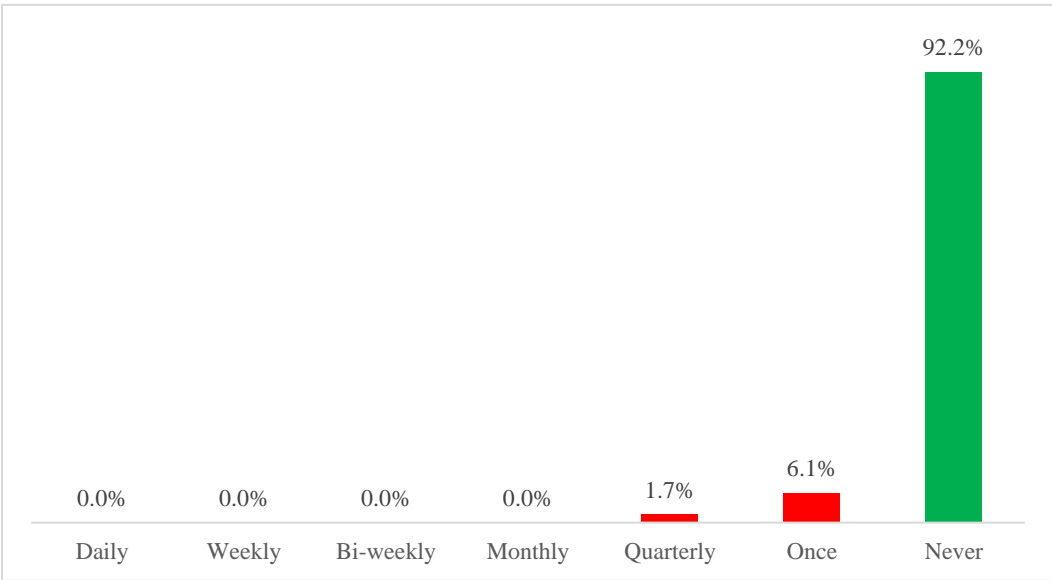
RB13. Sharing my current location on social media.



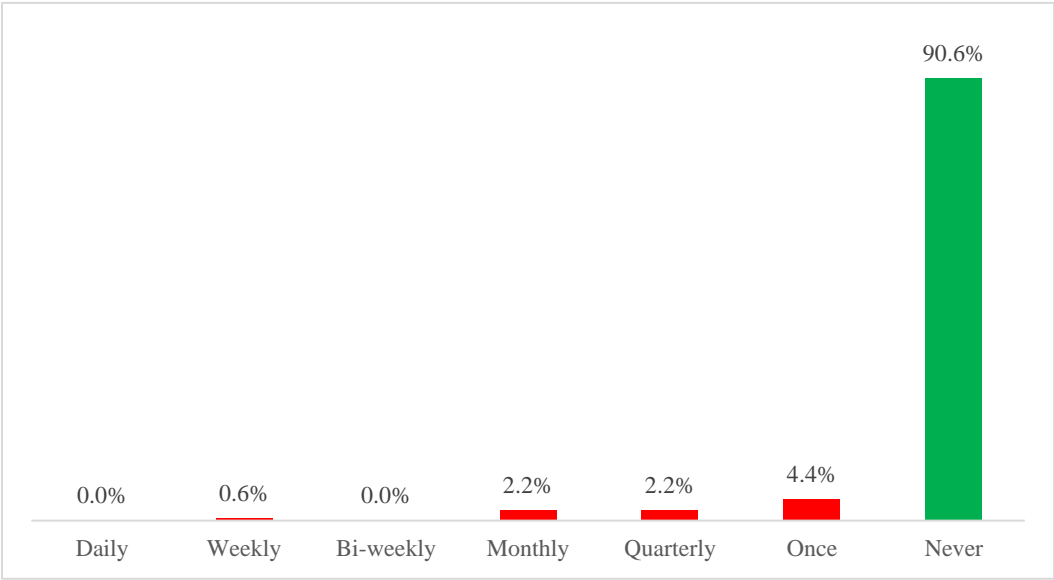
RB14. Accepting friend requests on social media because you recognise the photo.



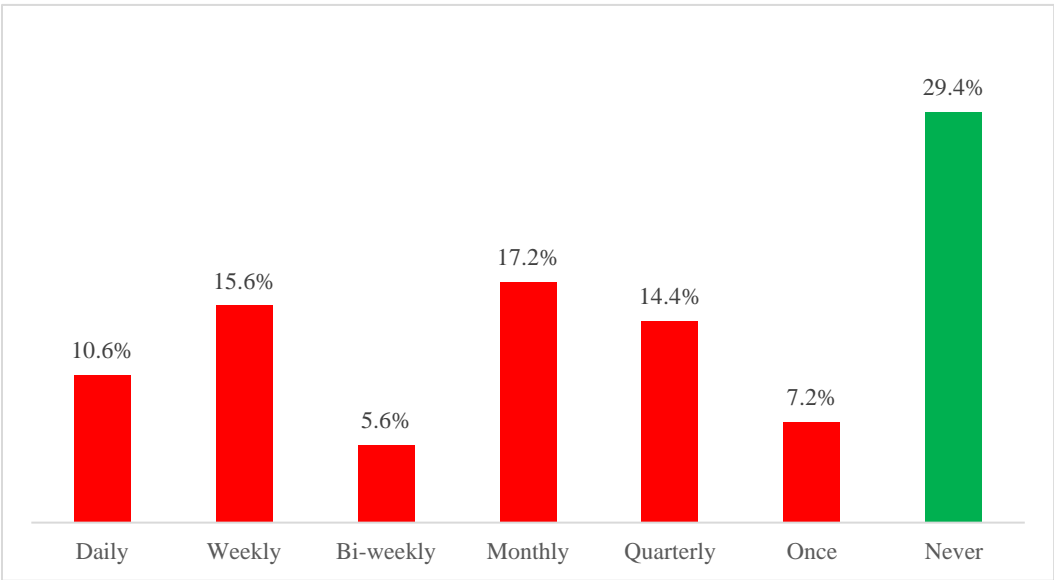
RB15. Clicking on links contained in unsolicited emails from an unknown source.



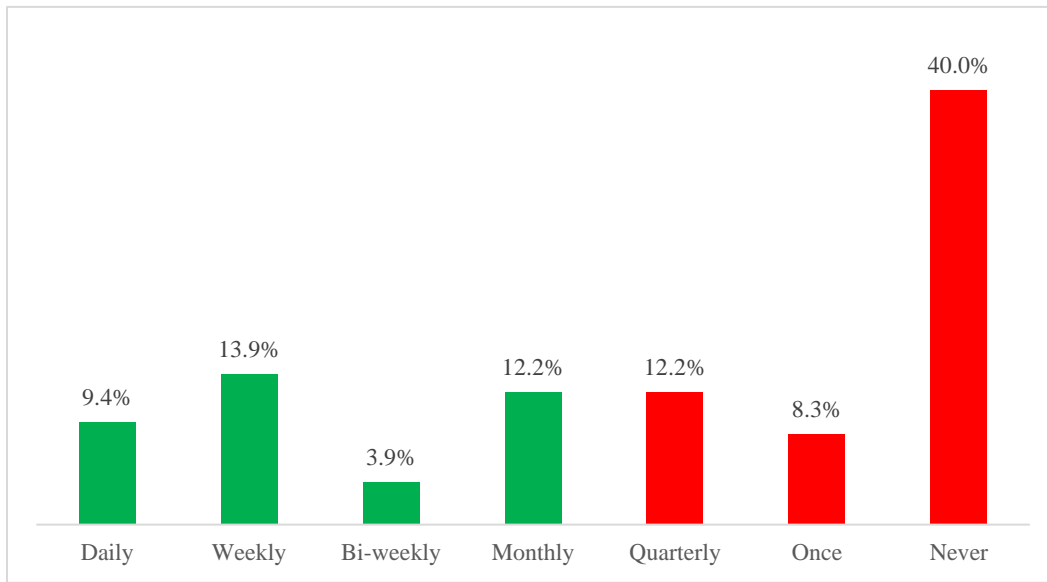
RB16. Sending personal information to strangers over the Internet.



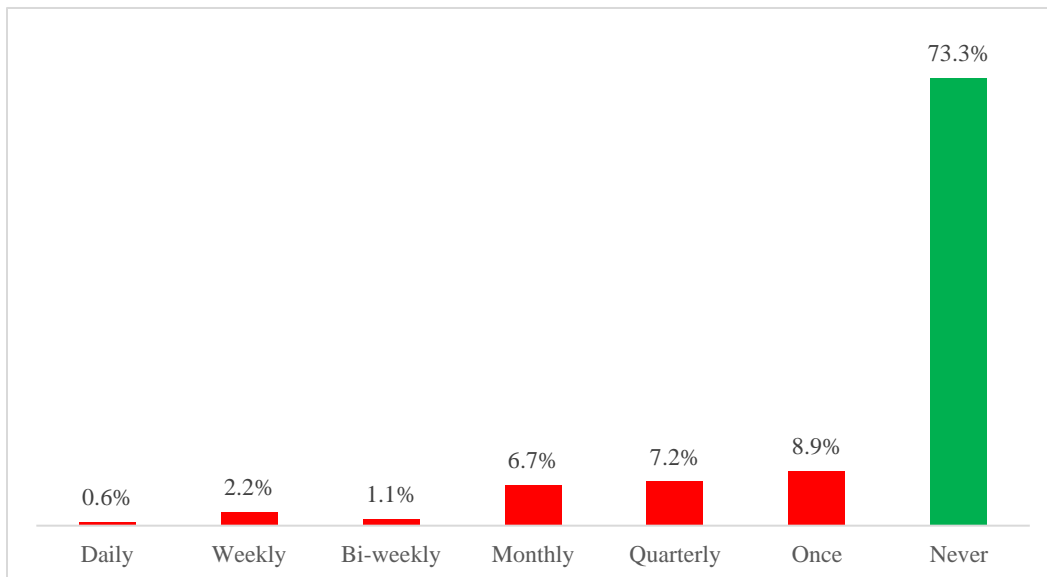
RB17. Clicking on links contained in an email from a trusted friend or work colleague.



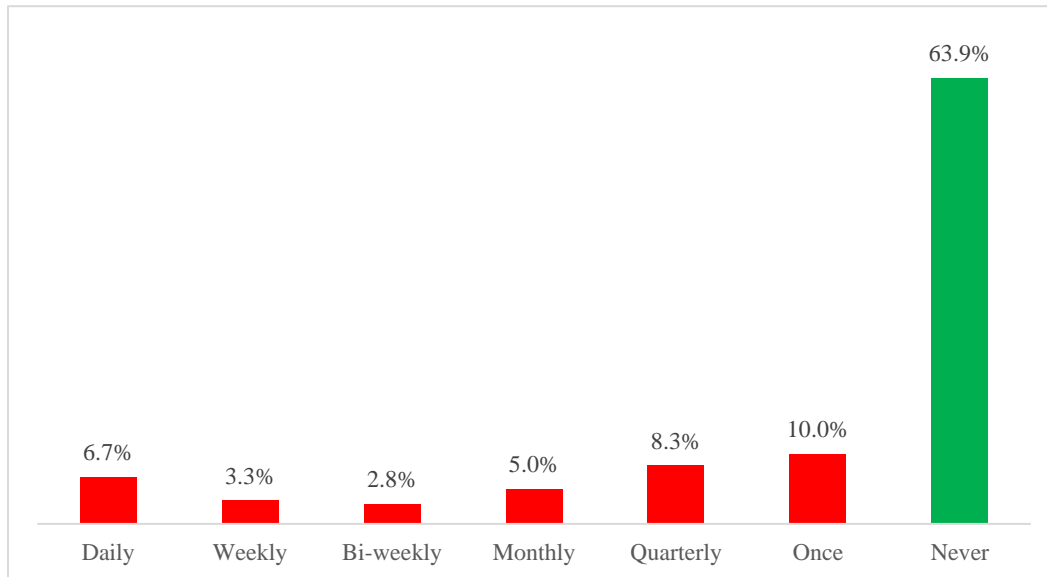
RB18. Checking for updates to any anti-virus software you have installed.



RB19. Downloading data and material from websites on my work computer without checking its authenticity.



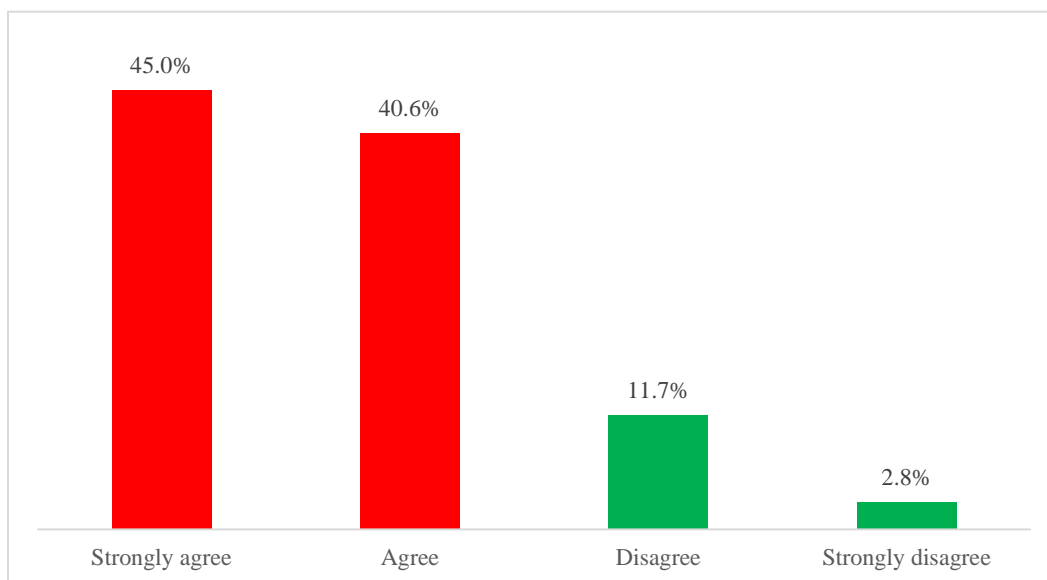
RB20. Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop).



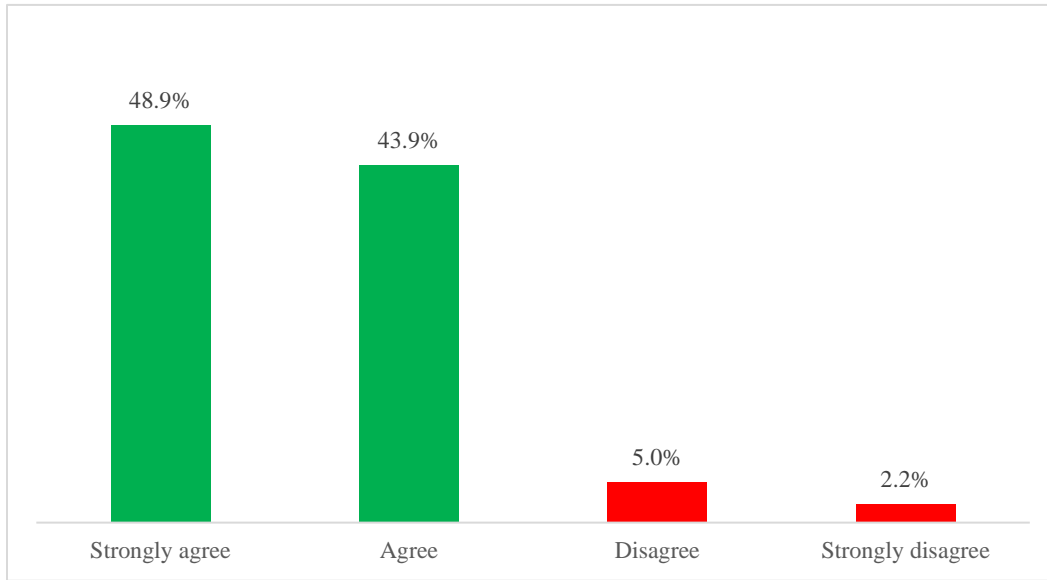
1.4 Attitudes Towards Cybersecurity and Cybercrime in Business (ATC-IB)

The ATC-IB inventory asked participants 25 questions about their individual attitudes towards cybersecurity and cybercrime issues mainly with respect to the Swiss military.

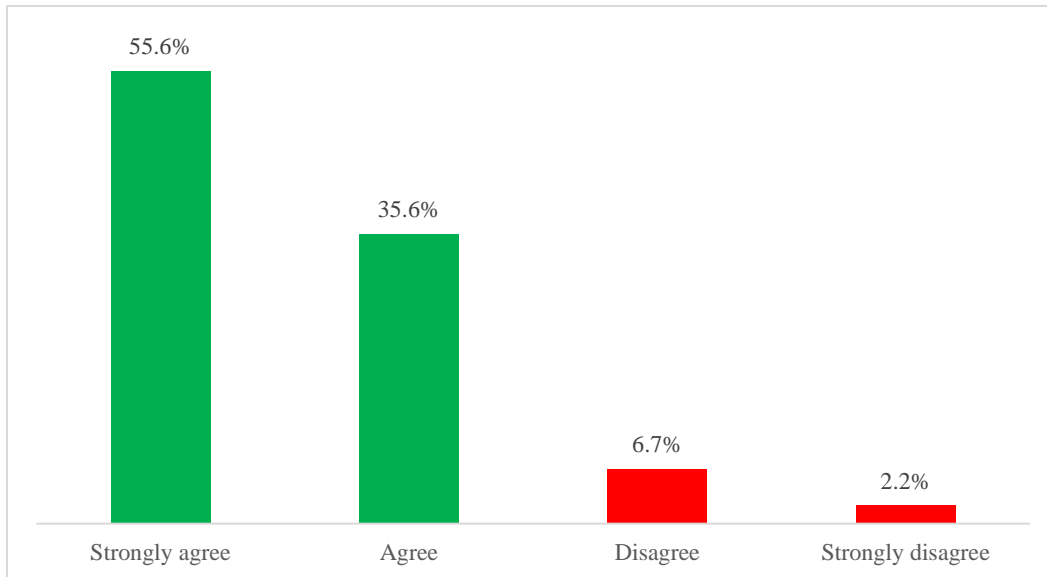
RA01. I think that the military command has the responsibility to ensure the army is protected from cybercrime.



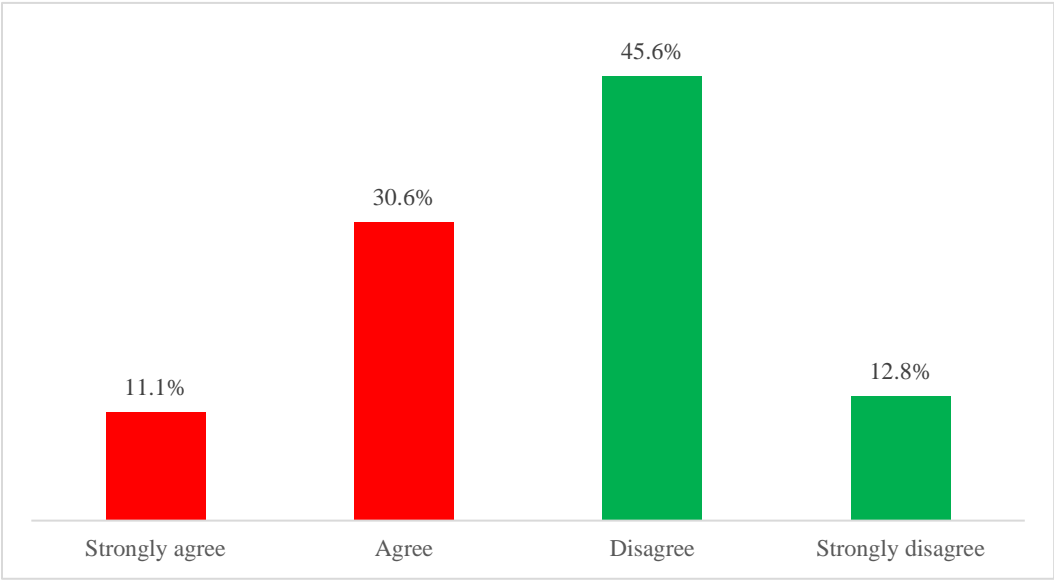
RA02. I am aware of my role in keeping the army protected from potential cybercriminals.



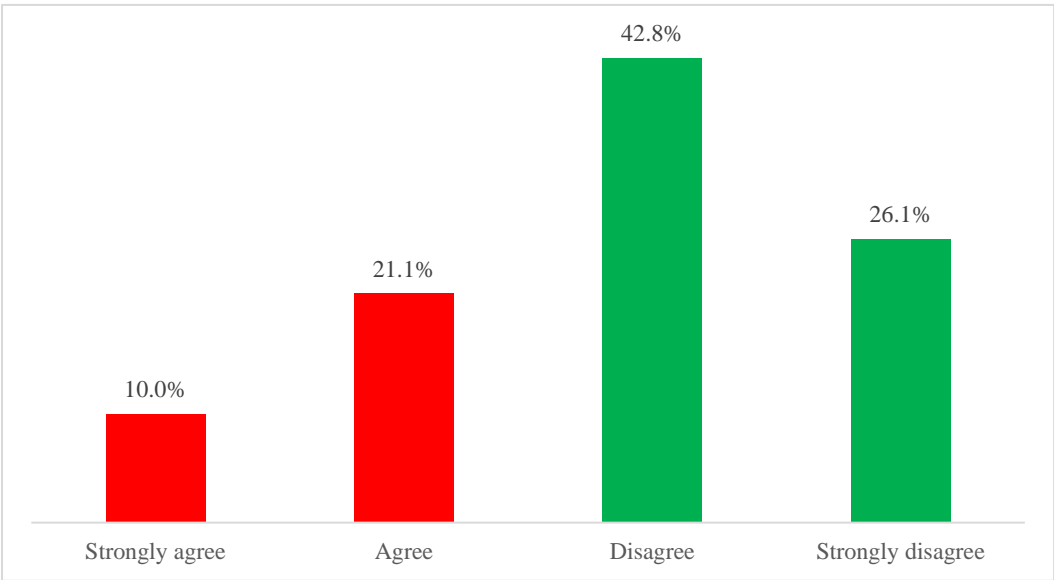
RA03. I believe everyone in the army has a role to play in protecting against threats from cybercriminals.



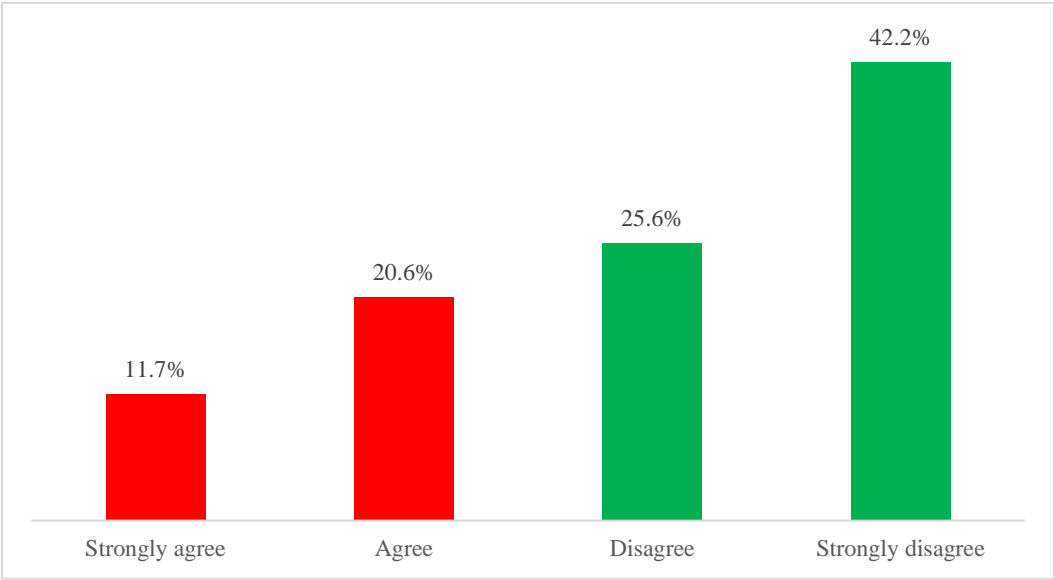
RA04. It is hard to know how I can help protect the army from cybercrime.



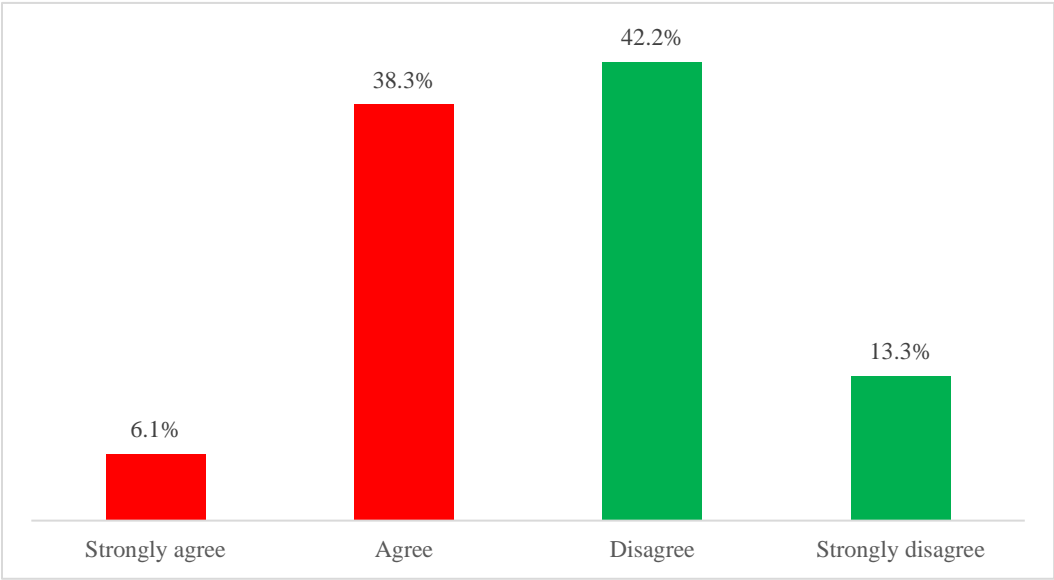
RA05. I don't have the right skills to be able to protect the army from cybercrime.



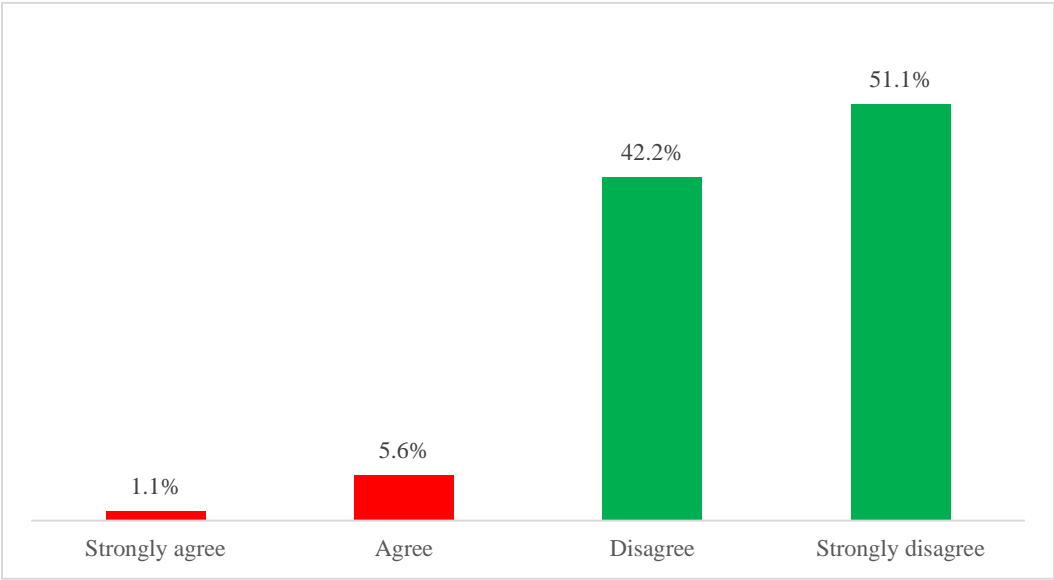
RA06. I do not feel that IT security is a priority within the army.



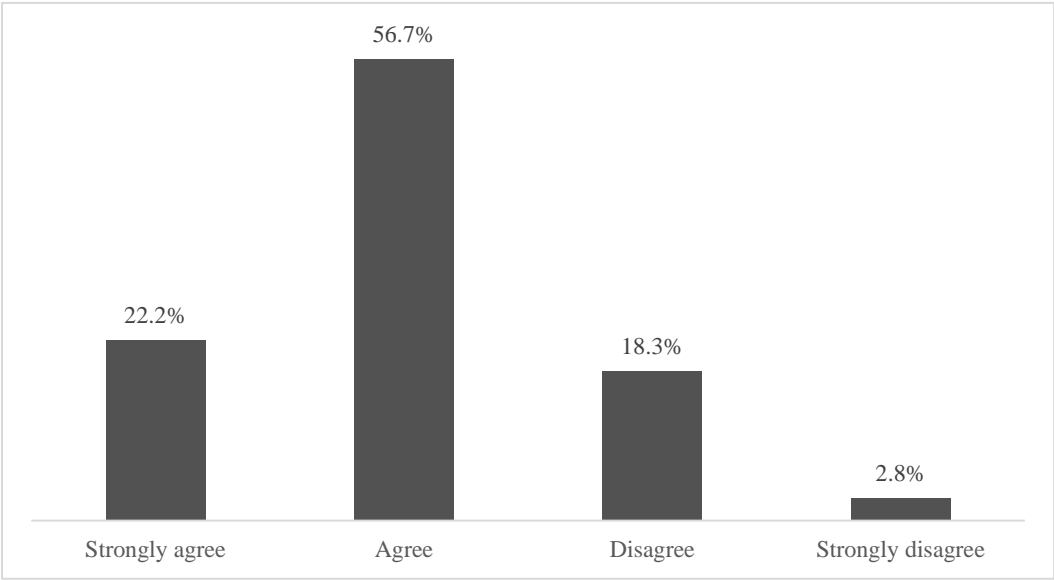
RA07. Computer systems provide all the protection the army needs.



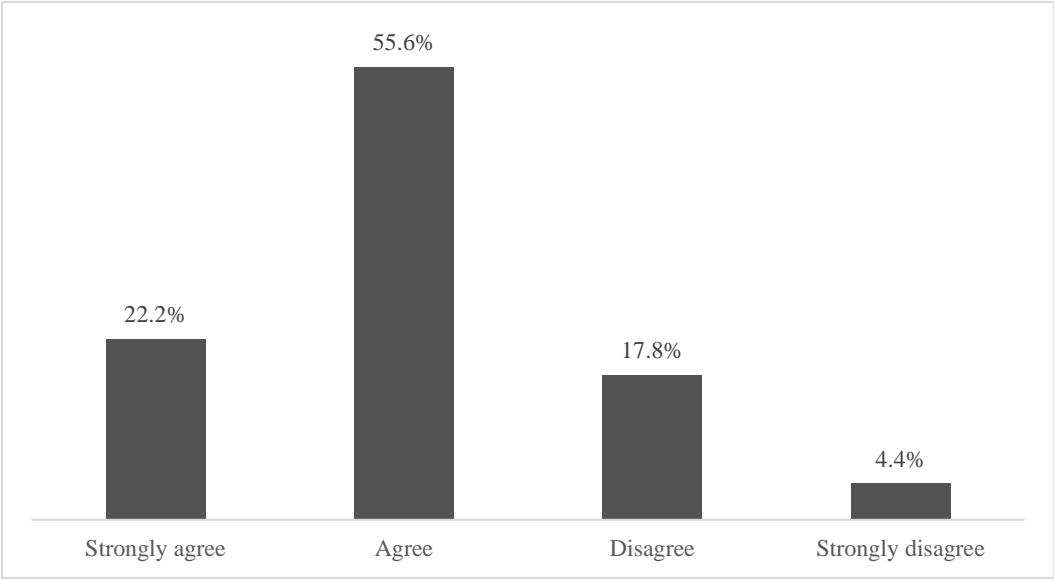
RA08. I think that reporting cybercrime is a waste of time.



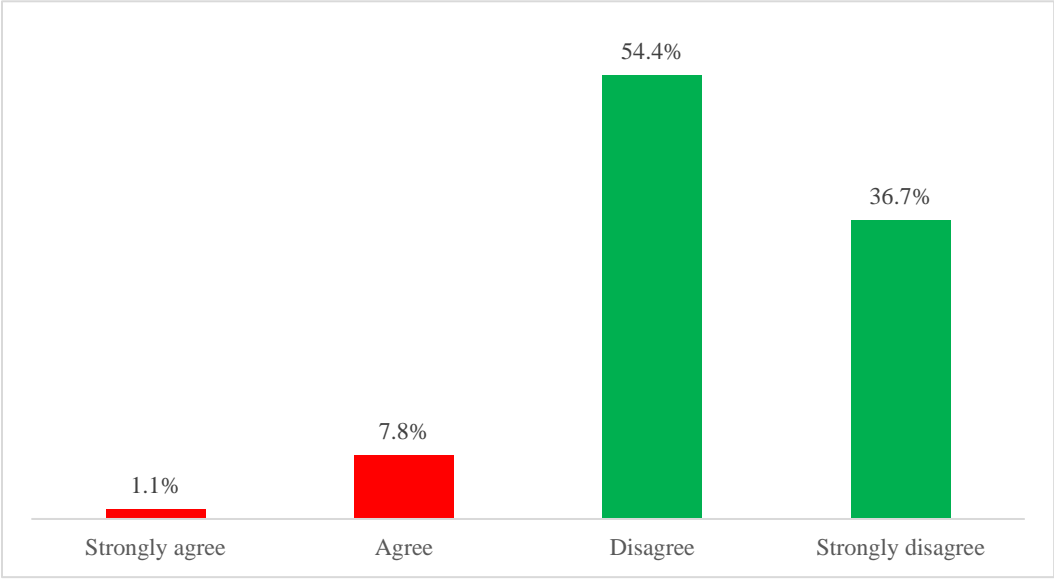
RA09. The Police lack the capacity to deal with cybercrime effectively.



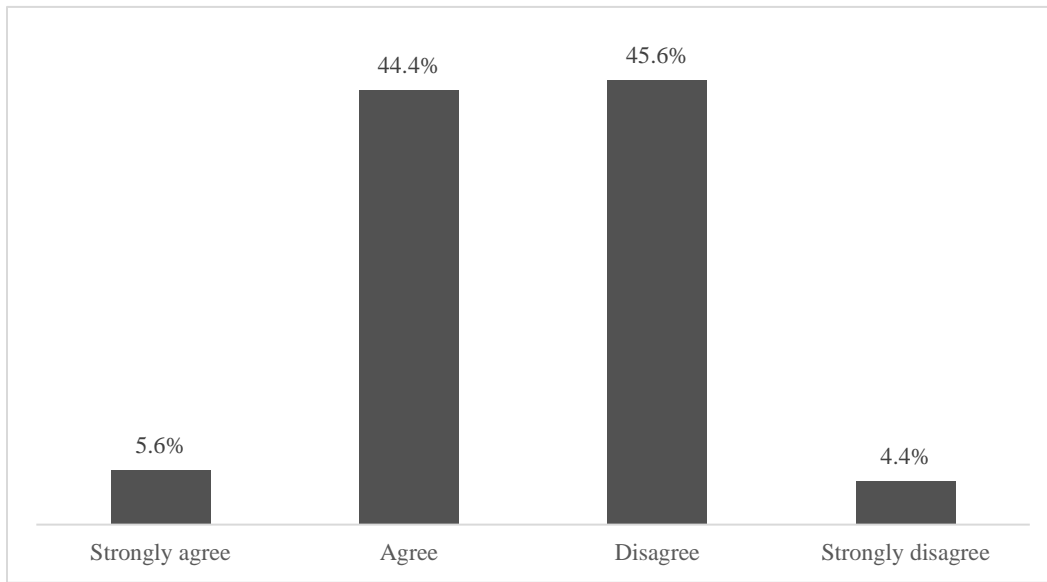
RA10. I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.



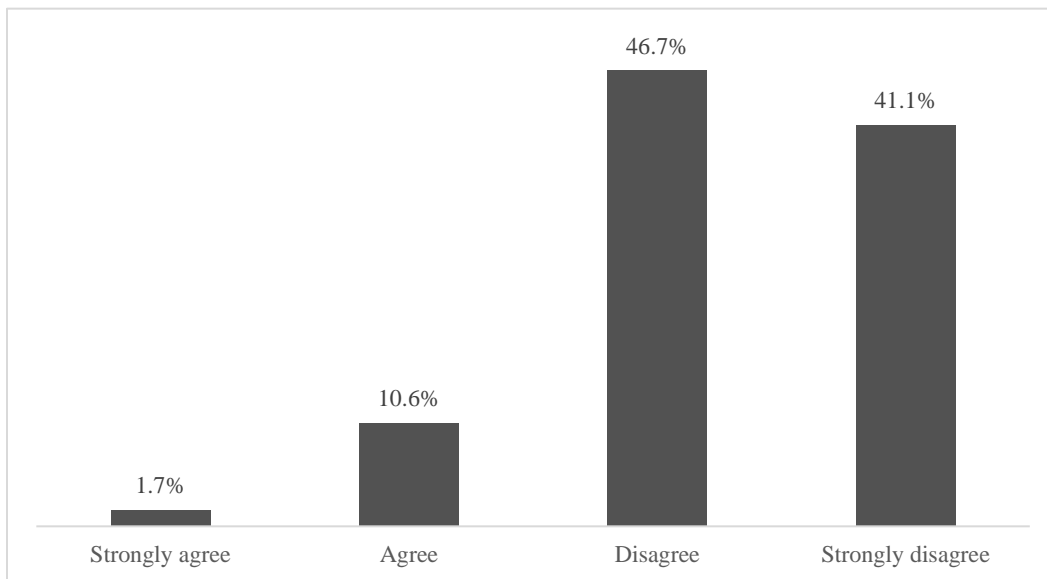
RA11. I think that information provided by the Government and Police on cybercrime is not relevant to the army.



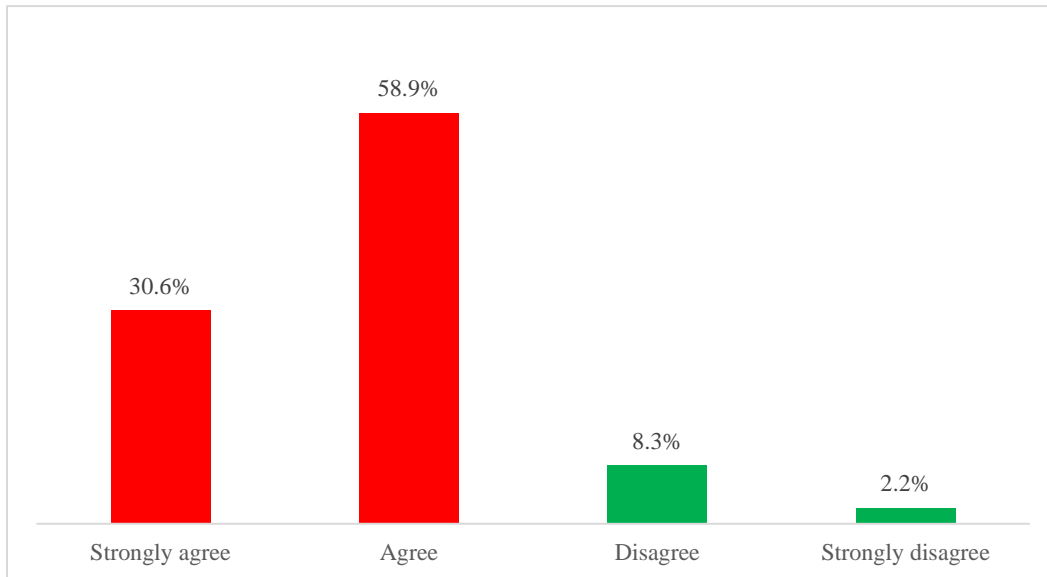
RA12. I feel that the Police are far too busy to deal with cybercrime.



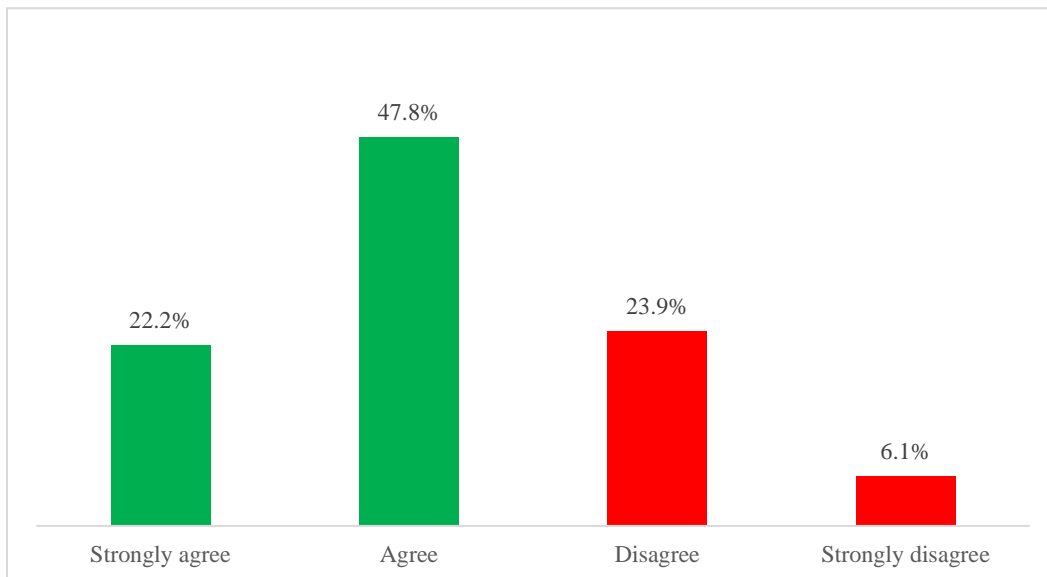
RA13. I worry that if I report a cyberattack to the Police it might damage the reputation of the army.



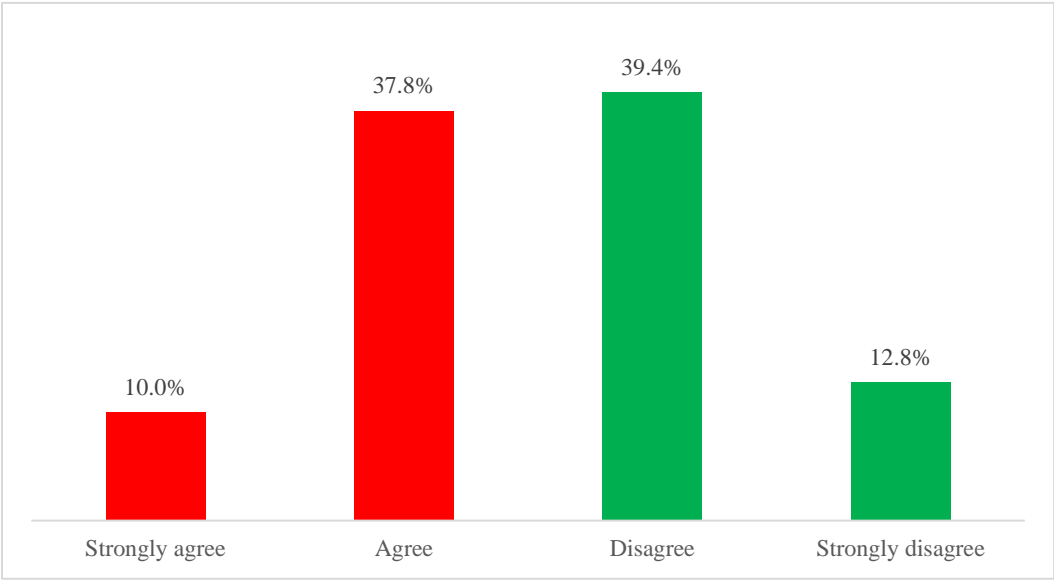
RA14. I think more could be done to communicate the risks from cybercrime to individuals in the army.



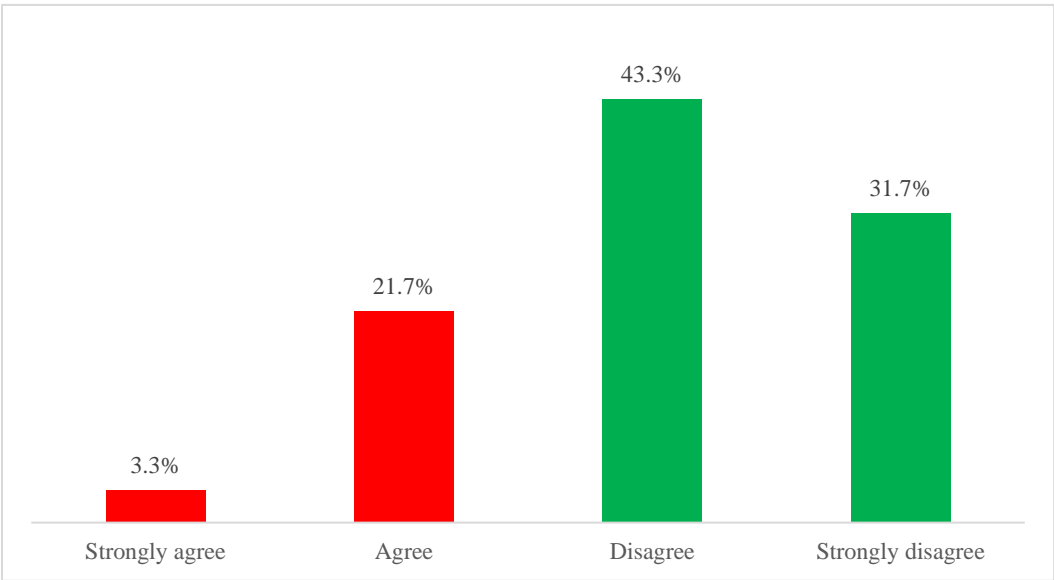
RA15. I am aware of the army's IT use policy and attempt to follow it.



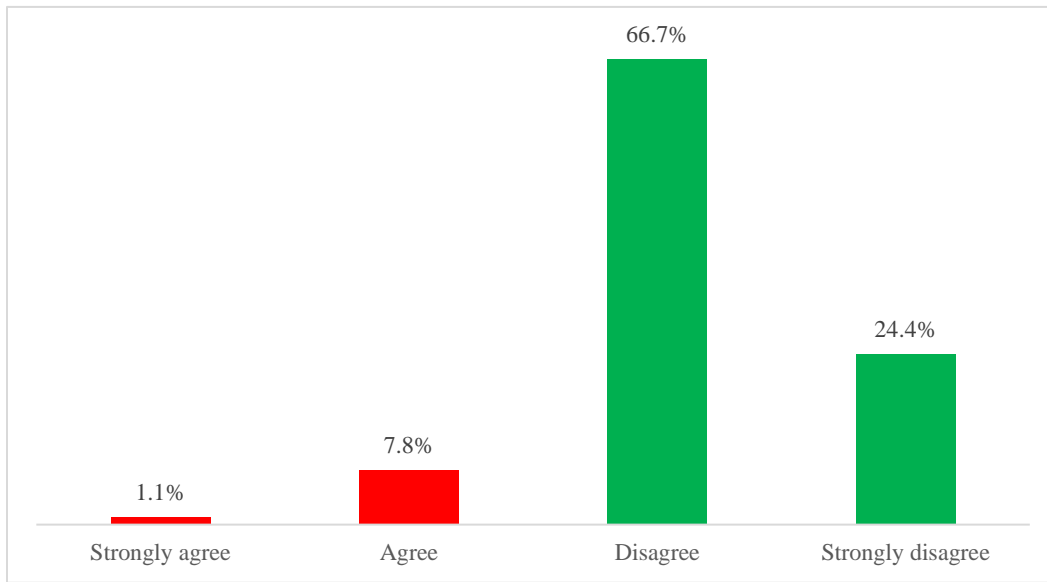
RA16. I would not know how to report a cyberattack if one happened.



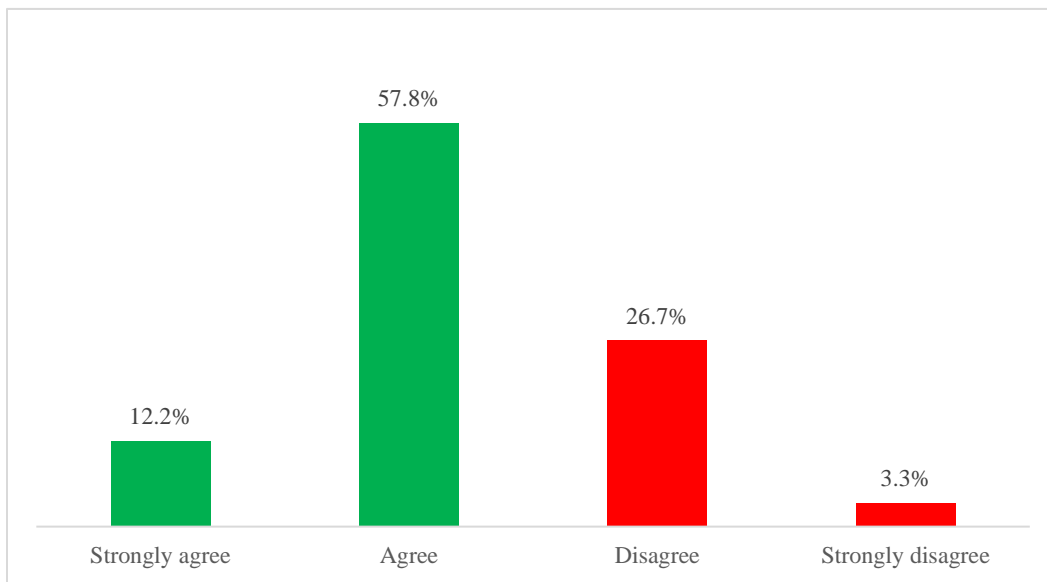
RA17. I don't think that reporting a cyberattack on the army is my responsibility.



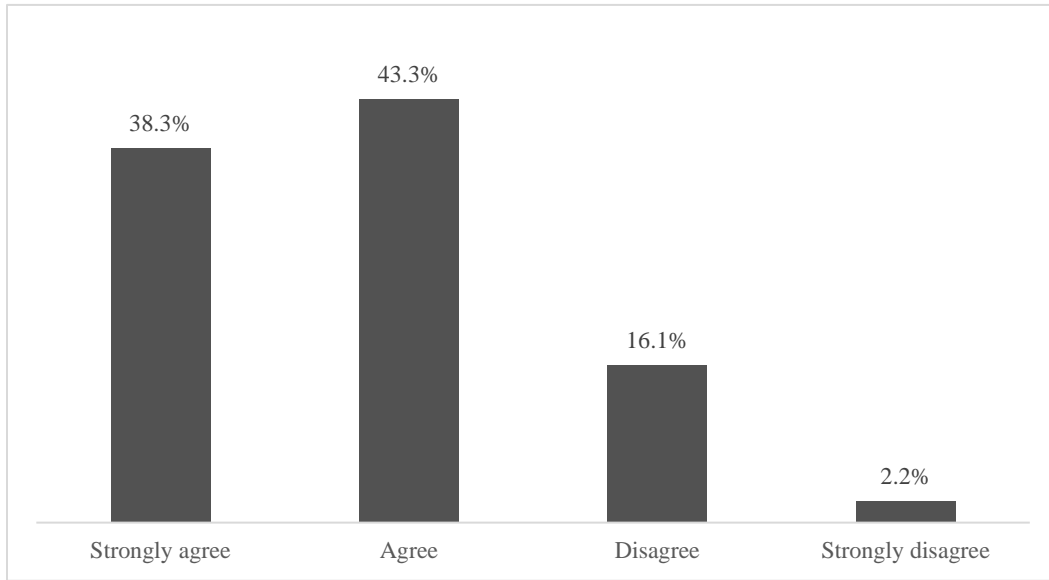
RA18. I don't pay attention to army material about the threats from cybercrime.



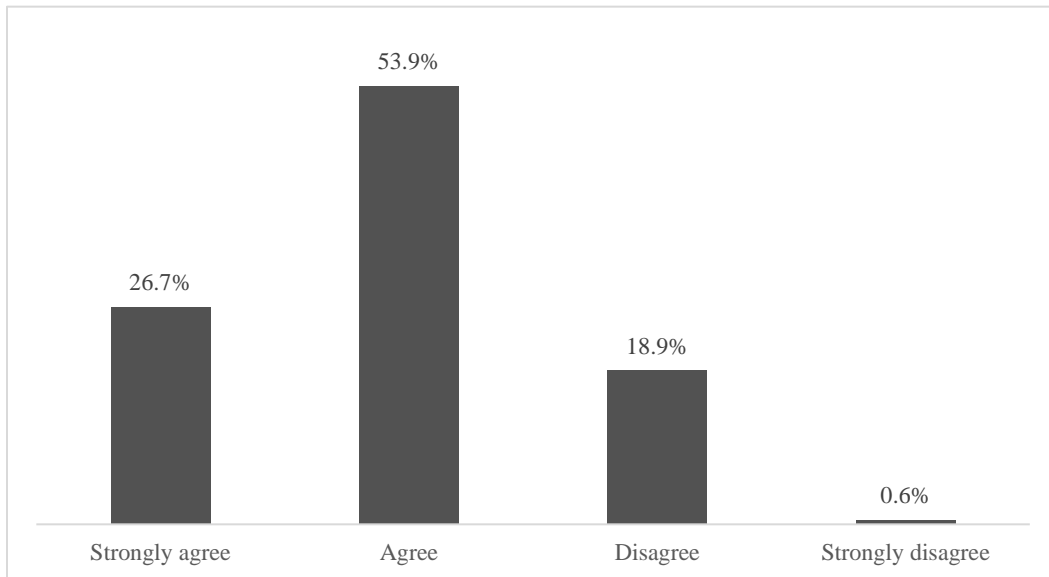
RA19. I am confident that I would be able to spot the signs of a cyberattack.



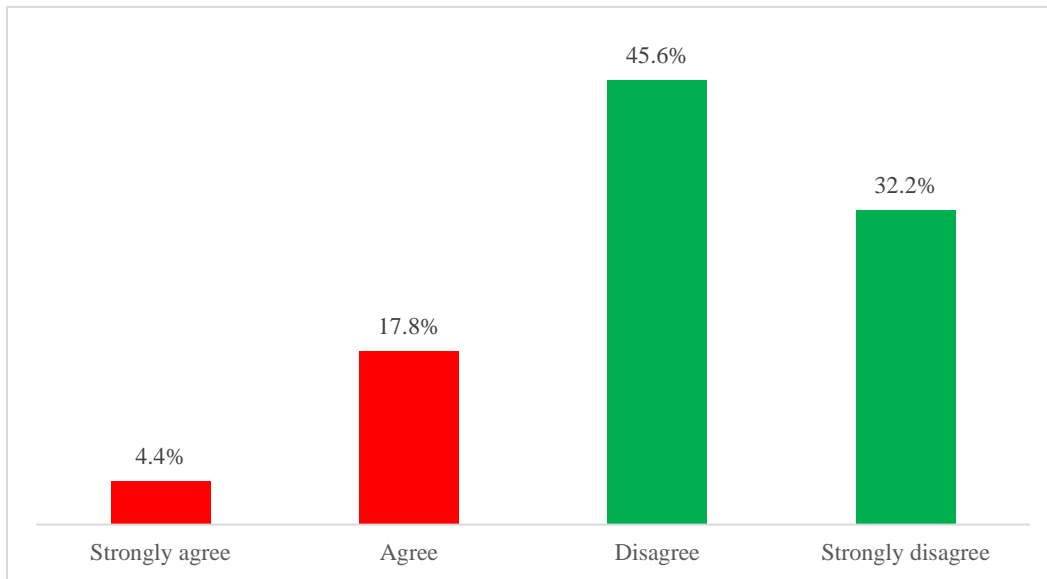
RA20. I think the biggest threat for IT systems comes from people within the army.



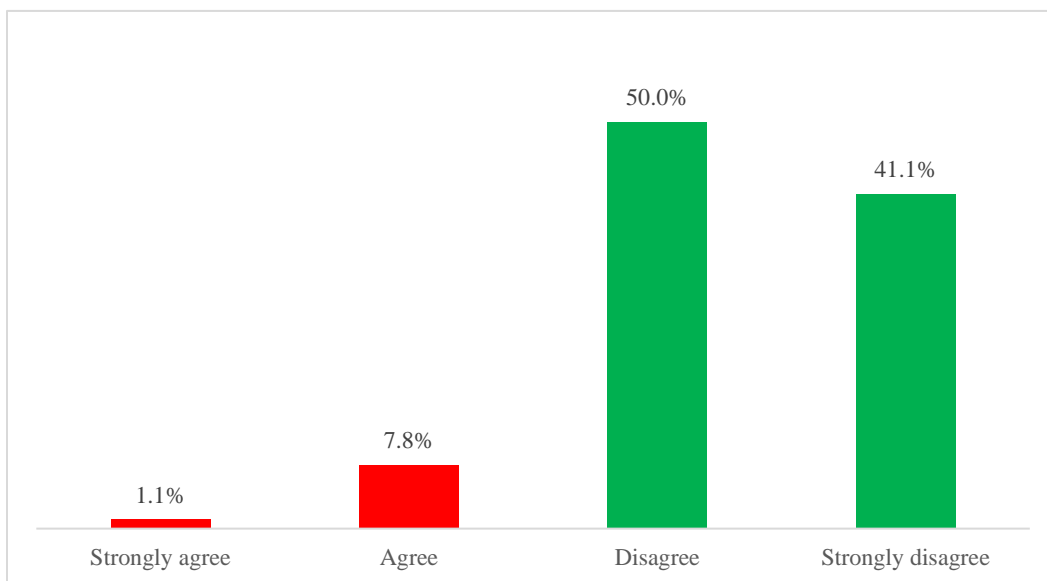
RA21. I feel that any individual within the army are at risk of manipulation from confidence tricksters.



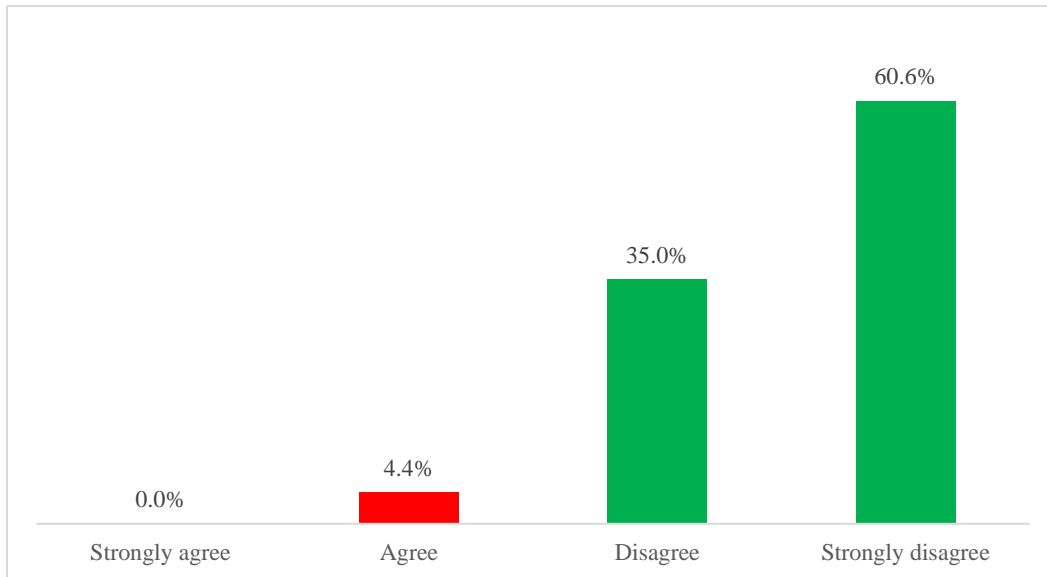
RA22. I think that cybercriminals only target the army when there is a substantial financial gain.



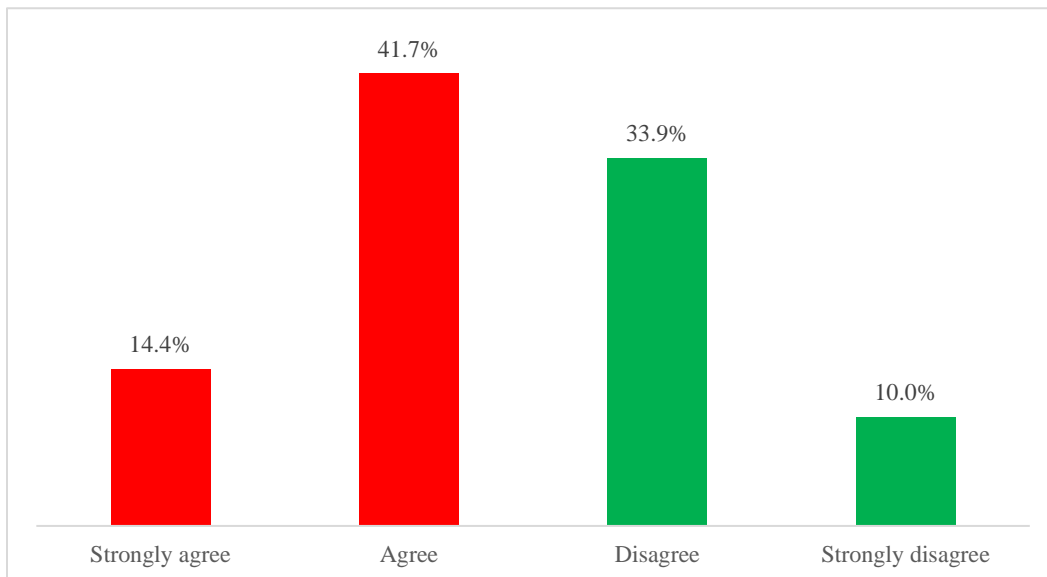
RA23. I believe only large organizations are targeted by hackers and cybercriminals.



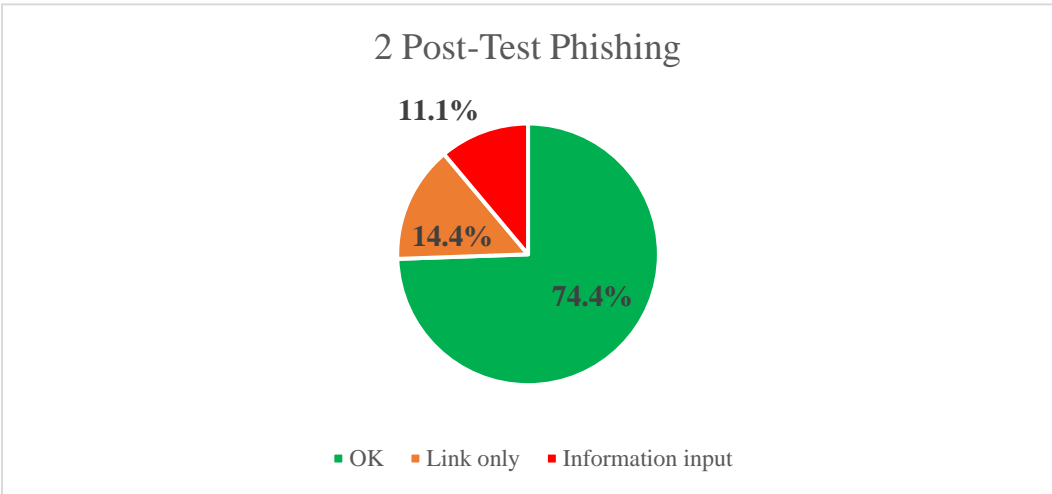
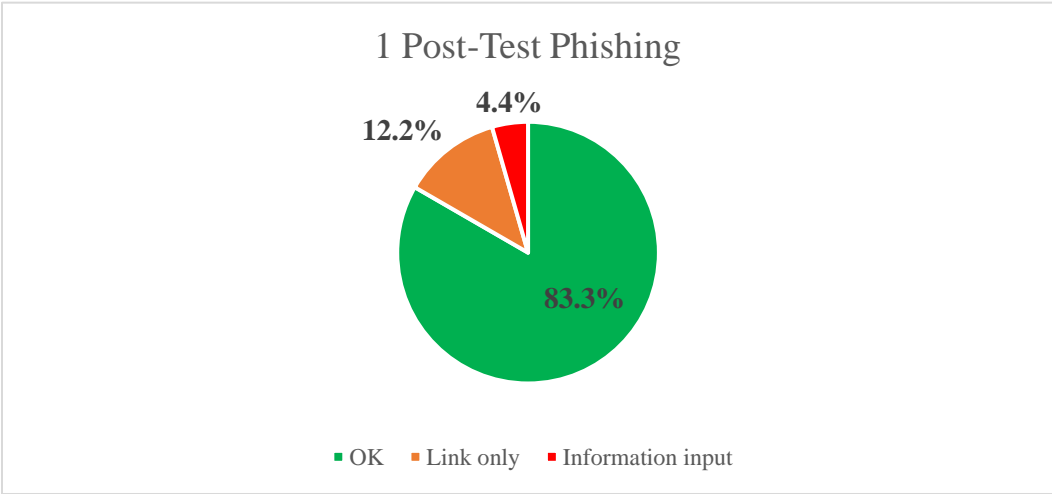
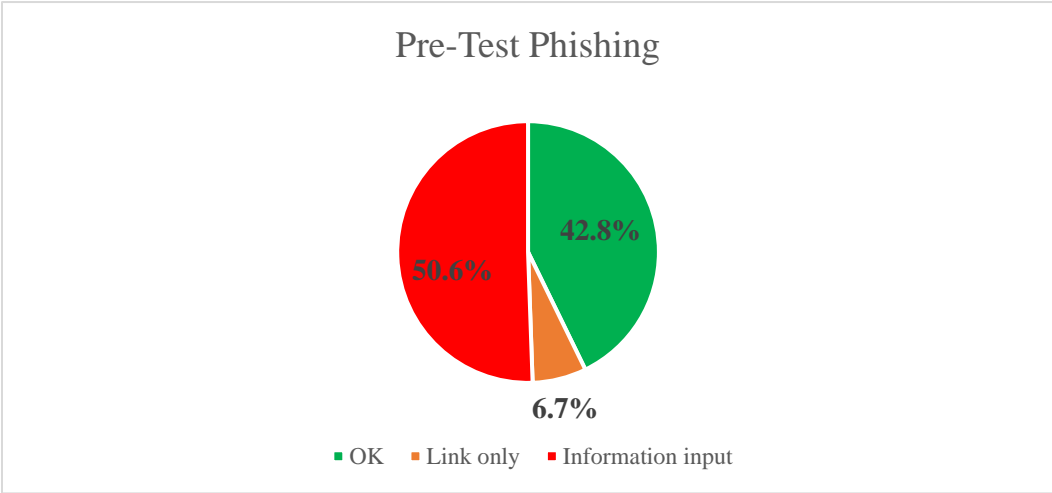
RA24. I feel that only organizations that take payments using online systems are at risk of being victims of cybercrime.



RA25. I don't think I know who is responsible for protecting the army from cybercrime.

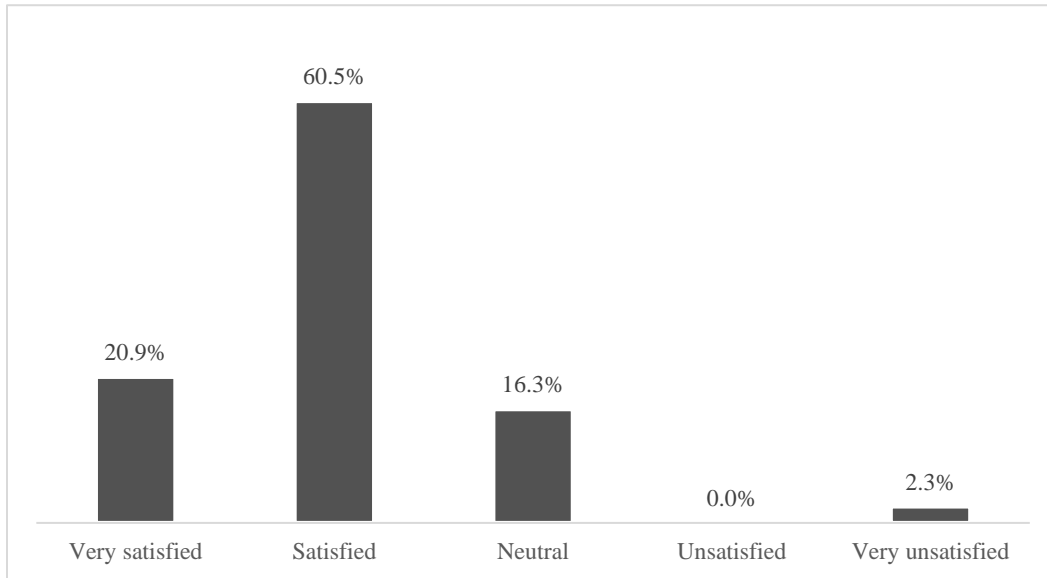


2. Phishing results

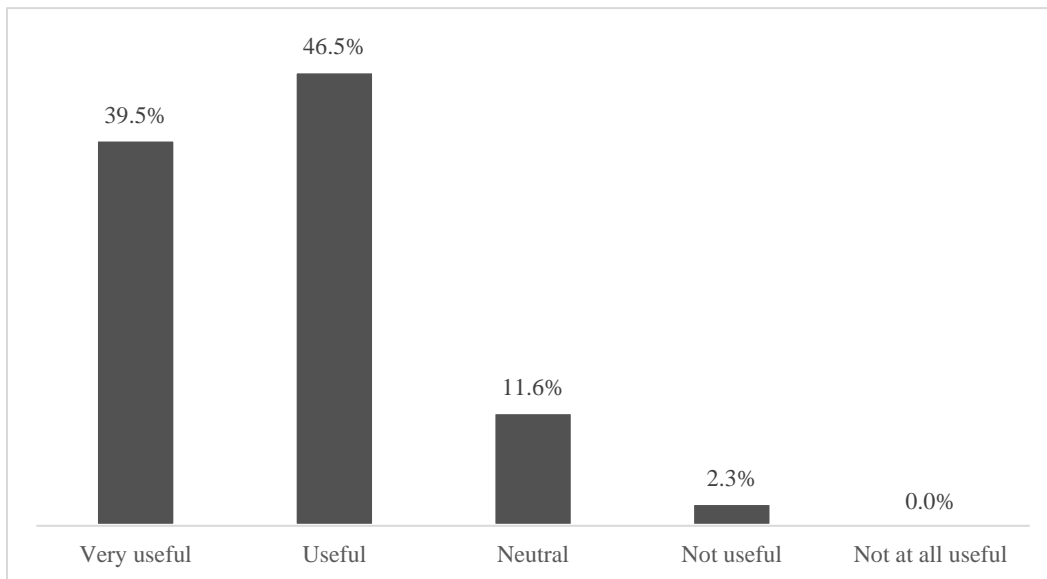


3. Post Serious Game Survey Results

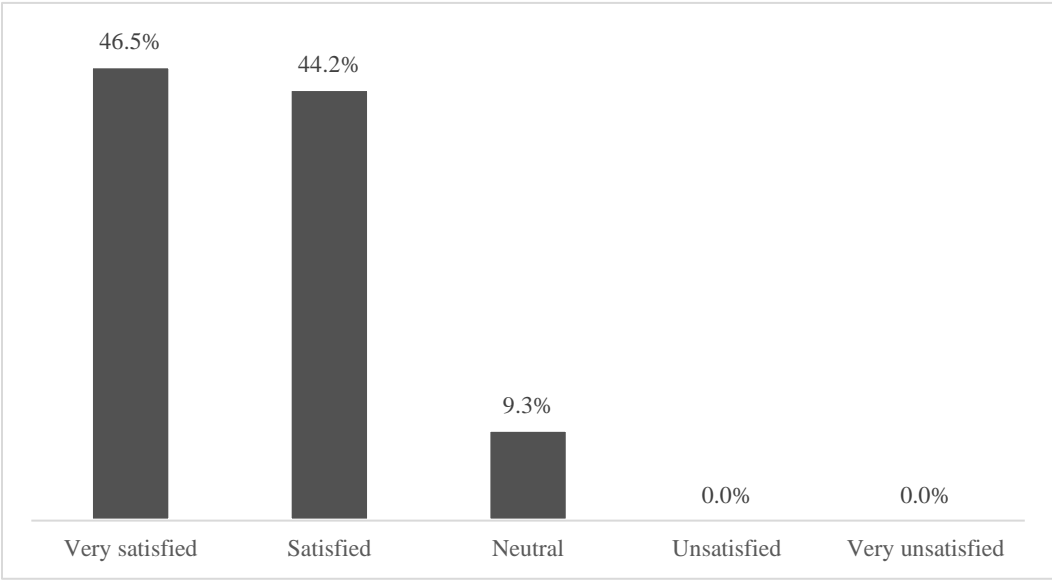
D2. How satisfied are you with the whole event?



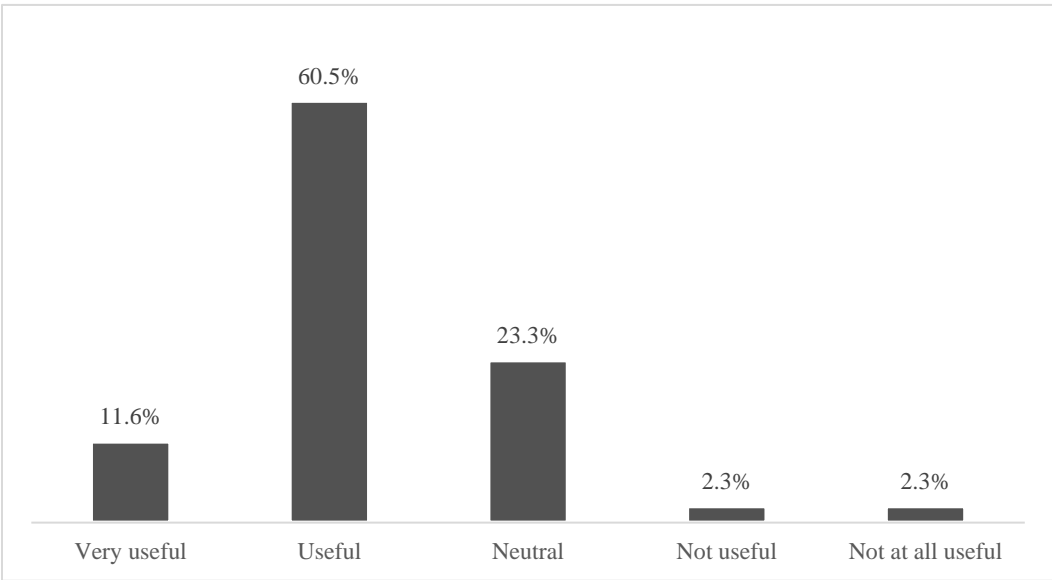
D3. How useful do you consider the introductory presentation?



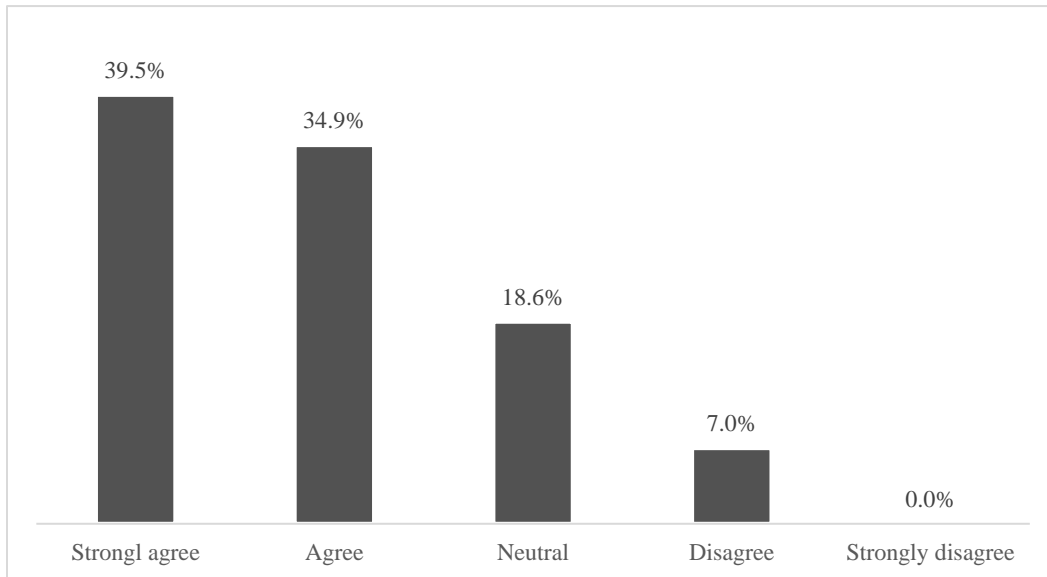
D4. How satisfied are you with the game master of your table?



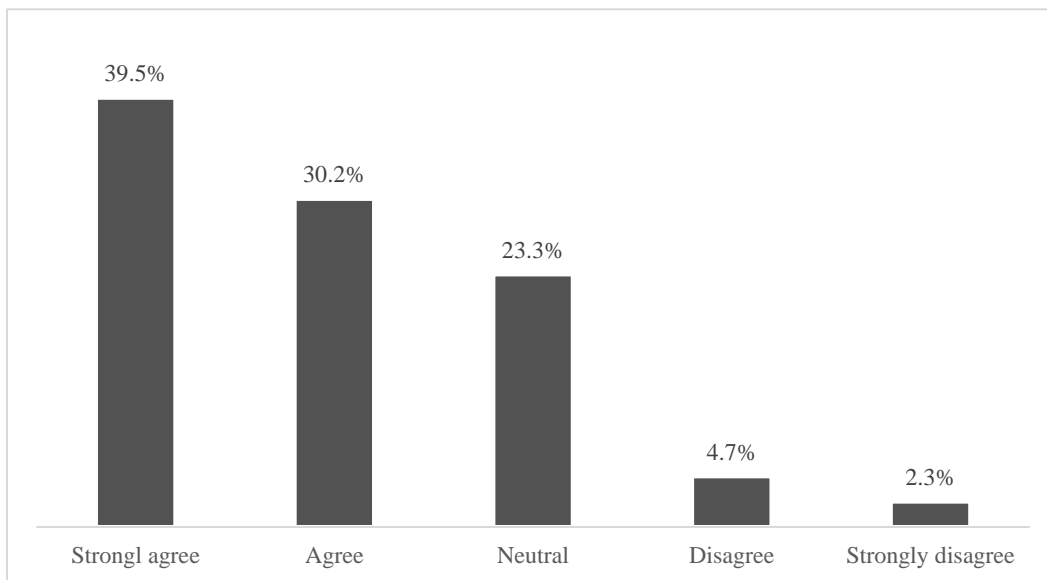
D5. How useful was the interactive serious game to you?



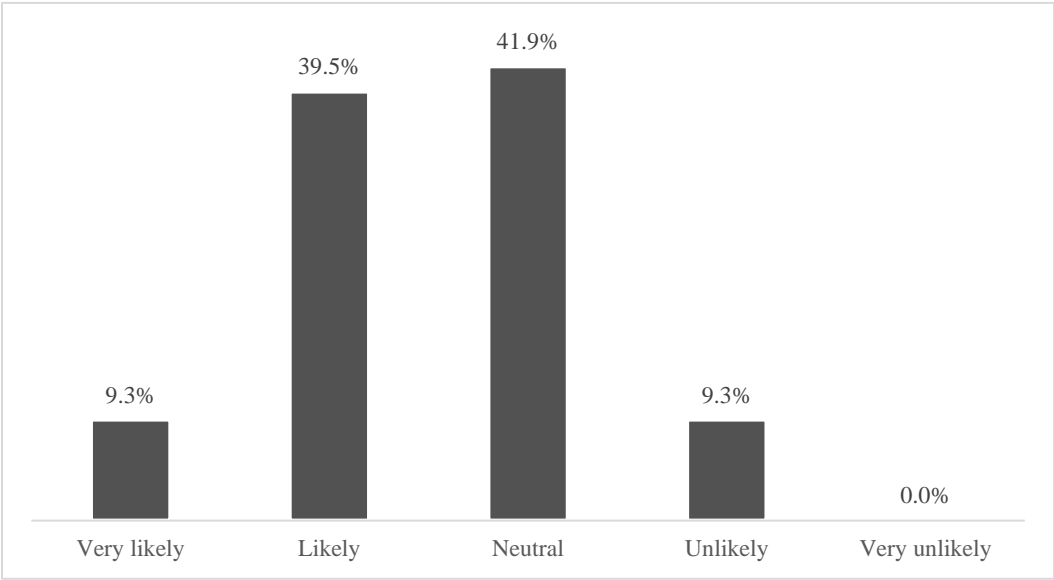
D6. How much do you agree with the following statement: The serious game has contributed to my knowledge about social engineering?



D7. How much do you agree with the following statement: I am now more aware of the threats posed by social engineering than before the event.



D8. How likely is the event to help you avoid becoming a victim of social engineering?



D9. Do you have any suggestions for improvement?

