Forensic Science International: Digital Investigation xxx (xxxx) xxx

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

"Hello are you available?" Dealing with online frauds and the role of forensic science

Olivier Ribaux*, Thomas R. Souvignet

School of Criminal Justice, Faculty of Law, Criminal Justice, and Public Administration, Batochime, University of Lausanne, CH-1015, Lausanne-Dorigny, Switzerland

ARTICLE INFO

Article history:
Received 7 January 2020
Received in revised form
4 April 2020
Accepted 4 April 2020
Available online xxx

Keywords:
Online scam
Crime analysis
Digital forensics
Routine activities
Digitalization

ABSTRACT

On August 6, 2019, the 119 members of the School of criminal justice, forensic science and criminology at the University of Lausanne were the target of an online scammer. His/her modus operandi consisted of email masquerading as the Director of the School in an attempt to induce the victims to buy digital gift cards and to transmit the card usage code to the perpetrator.

The first author of this paper is the Director of the School, and the second is an expert in digital forensic science and a professor of the School. They worked together in real time to deal with the fraud. Because the fraud occurred in a School of forensic science and criminology, it raised many questions on a variety of overlapping dimensions. The objective of this study was, therefore, to draw lessons from this case from several perspectives ranging from forensic science to cybersecurity, and from practical to academic.

The response to the incident has been treated in four typical distinguishable phases: (1) fraud detection; (2) crisis management; (3) post-incident analysis; and (4) reporting to different communities.

We conclude this paper by taking lessons from the case to express the essential role of forensic knowledge and crime analysis in interpreting the information conveyed by digital traces to develop innovative cross-disciplinary models for preventing, detecting, analysing, investigating and responding to online fraud.

1. Introduction

Recently, the volume and variety of online frauds have been more clearly expressed through official crime statistics and surveys (BCS, 2016; Reep-van den Bergh and Junger, 2018). They describe the emergence of a new wave of crime or "cyber-volume crimes", perceptible to the public, which requires a rapid and structured response. By whom and how it should be organised between public and private stakeholders remains unclear, however (Dupont, 2017; Loveday, 2018).

Several professional and academic communities are developing integrative models for dealing with cybersecurity and potentially covering the issue. Their aim is to ensure better protection and resilience of infrastructures, as well as an effective response to computer security incidents, whether at individual, organisational or even national levels (Cichonski et al., 2012; CMM, 2016; NIST, 2018). They mainly adopt a technical and information technology risk management vision, but also incorporate legal or social aspects intrinsic to these problems. The inclusion of forensic science within incident response practices was also considered early in these models (Kent et al., 2006). At the same time, a "digital forensics" community was emerging, supporting the detection, collection and management of digital evidence in judicial processes (Pollitt, 2010). Beyond this traditional scope of forensic science, a forensic analysis approach has also proven to be essential to decipher the modus operandi of the attackers, and thus gather the knowledge to better protect an infrastructure (Casey and Nikkel, 2020). Cybersecurity and digital forensics are now routinely implemented as specialized departments in private and public organizations or as services. Digital Forensics and Incident Response (DFIR) is considered to be a sub-domain, which is involved in particular when a rapid response to incidents is required.

However, these developments are predominately technical and are primarily focused on high-profile cases such as major crimes, state-sponsored cyberattacks, and theft of large amounts of money

* Corresponding author.
E-mail addresses: Olivier.Ribaux@unil.ch (O. Ribaux), Thomas.Souvignet@unil.ch (T.R. Souvignet).

https://doi.org/10.1016/j.fsidi.2020.300978

or personal information. Although DFIR processes, practices, and tools play an important role in dealing with cybercrime, they are not sufficient for dealing with new forms of high volume crimes enabled by the technological infrastructures that have become ubiquitous in everyday life (Loveday, 2018). A wide variety of online frauds are among these crimes that have become part of a digitally transformed society in which human factors play the central role. The coronavirus has shown how suddenly new online modus operandi can appear when the social context changes and people's routine activities are disrupted.[1] Online fraud is therefore difficult to model and mitigate entirely using a DFIR approach. It is preferable to integrate a strong crime analysis component bringing new insights from criminology. A new stream of criminological research is attempting to better delimit the size of the problem and its forms (Button, Lewis and Tapley, 2009; Reep-van den Bergh and Junger, 2018), to adapt existing theories in an attempt to explain them (Leukfeldt and Yar, 2016), to characterize the phenomenon more specifically (Leukfeldt et al., 2017; Wall, 2010), study it from the victim's perspective (Button et al., 2014a; Button et al., 2014b; Cross, 2018; Whitty, 2019) or consider the kinds of possible responses (Holt and Bossler, 2016).

From a practical perspective, the police, in particular, are expected to respond in a professional manner to an increasing number of solicitations from the victims of these frauds. This is not only about creating new specialized structures. The whole organization has to adapt, from the field officers in charge of receiving complaints and communicating with the public, to a more central, specialized or managerial level (Loveday, 2018). New partnerships need to be created. Forensic science and crime analysis, both as disciplines and as structures, must also find their place in these changes (Rossy and Ribaux, 2020).

A practical case concretizes remaining challenges in combining different views and approach to online fraud, both from an R&D and a practical point of view. On August 6, 2019, members of the School of Criminal Justice at University of Lausanne, were the target of an online fraud consisting of email masquerading as the Director in order to obtain money from them in the form of digital gift cards. Both authors of this paper were directly concerned by the fraud. The first being the Director of the school, and the second as a professor of digital forensic science. They both worked together to deal with this fraud in real time.

This case-study is decomposed in four chapters, by similarity with typical incident response methodologies (Cichonski et al., 2012): (1) fraud detection; (2) crisis management; (3) post-incident analysis and (4) reporting to communities. Lessons learned from this case are eventually integrated into a broader discussion of the central role of forensic science and crime analysis in dealing with online frauds.

2. The detection

On August 6, 2019, the Director of the School of Criminal Justice (SCJ) at University of Lausanne was on holidays. It was a rainy day. A perfect day to work from the hotel on a paper in preparation. The mailbox was open on the computer, letting incoming mail through, mostly mixing spams with messages relevant to the organization (several dozen).

When scanning the emails quickly, one of them seemed unusual (message #1 - Fig. 1). This email was sent by a new employee of the School, who we will call Y for the rest of this article. It was the first sign that something was wrong. However, it did not trigger any action at that time. It just caused some surprise.

Time: 12:39 pm.

A little later, a second sign was perceived by the Director, through an email from a colleague, displaying his availability, but asking if his identity was not usurped (message #2 - Fig. 2).

Time: 12:45 pm.

Almost at the same time, the second author of this paper sent a WhatsApp message to the Director: “Hello, did you get hacked into your Gmail account?“. In fact, he had also received the message “Helloyou are available?” from the same wrong address. Another colleague then phoned the manager to inform him that he had received a strange “Are you available?” message. He replied, but felt uncomfortable.

Without any delay, the Director responded to message #2 (first colleague) to indicate that a fraud was probably in progress at the school, warning his colleague not to continue the dialogue with the sender of the email.

From these signs, it became clear that a fraud was now underway. The perpetrator(s)[2] of the fraud was claiming to be the Director in order to convince the employees to enter into his scenario. Beyond the fraud itself, it was emotionally difficult for the Director to imagine someone impersonating him and taking his position to demand a service from members of the School. He was therefore determined to take urgent action.

Time: 12:48 pm.

3. The management of the crisis

Although not a crisis management specialist, the Director adopted a usual structured approach in two steps: (1) assess the situation, and (2) consider urgent measures to mitigate the immediate development and impact of the fraud. When assessing the situation, it is necessary to identify the appropriate structures and people to be activated, according to their competencies (both as an authority and skills). Immediately five possibilities presented themselves:

1. The police
2. The University IT department
3. Google (because of Gmail)
4. Create an ad hoc crisis unit with a colleague, who communicated remotely via WhatsApp
5. Mobilize other members of the School

Immediately, the fourth solution imposed itself in the immediate situation: the police and Google were perceived as difficult to mobilize to deal with such an event in real time; before alerting the university, it was decided to observe the evolution of fraud. In the end, it was not considered reasonable to mobilize more people from the School during the holidays.

This was not an ideal setting for an ad hoc crisis management, as both were on holidays distant from each other. One of them was visiting a tourist site with his family.

The Director then entered into an intensive exchange of WhatsApp messages with a colleague, a digital forensic expert. Two different perceptions of what was happening emerged from this discussion: Hypothesis A: the fraud targets were all contacts of the Director, obtained in an unknown manner. Hypothesis B: the fraud only targets SCJ employees whose addresses were obtained in an unknown manner.

Hypothesis A was favored by the forensic expert. During his

[1] https://www.cyberthreatcoalition.org/(accessed 2nd of April, 2020).

[2] The hypothesis of a single fraudster or of a group of fraudsters is discussed below. In order to avoid overloading the text before, we will use the singular form, letting tacitly the hypothesis of several perpetrators open.

Please cite this article as: Ribaux, O., Souvignet, T.R., “Hello are you available?” Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

Fig. 1. First email received (message #1). It was an order for an iTunes card, for CHF 200 (approx. US$ 200). The sender of the email is a doctoral student from the School. In fact, this doctoral student (Y) had just arrived at the School. Her name had not yet been memorized by the Director. Without any context, the email went unnoticed in the daily flow of emails. Note that the email was sent to two different addresses: one on a Gmail address, and the other one at unil. ch, which is the institutional domain name.

Fig. 2. Second email received (message #2). "Hello Olivier, I'm back from lunch around 1:15 pm, and available. That's you "olivierribaux04@gmail.com" (see sender below), or someone is trying to use your identity? Best regards". Colleagues were supposed to know that the Director was on vacation. Note that the message transmitted ("Hello are you available?") is in English whereas the common language of communication between the members of the School is French.

career, he was repeatedly confronted with the type of fraud called "emergency scam" or "crying for help scam". In this typical type of fraud, a person's email contacts are stolen by various means and they are used to request assistance under many pretexts, in order to obtain something of monetary value.

Hypothesis B was preferred by the Director. He might be biased, because Hypothesis A would mean that his email account or computer was hacked and that all his contacts were stolen, which would have more serious ramifications for him and the university.

If Hypothesis A was true, the Director should immediately

Please cite this article as: Ribaux, O., Souvignet, T.R., "Hello are you available?" Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

enable two-factor authentication on all of his online accounts, inform his contacts of possible fraud, and contact his bank and government to check for any suspicious activity. These would be the minimum precautions he should take, and further actions could be necessary if the possible exposure was his computer or if there were subsequent indications of identity theft.

If Hypothesis B was true, the circle of possible targets was much easier to define and reach. At the same time, an institutional list of targets was more likely to have been obtained by some other means than by hacking an email account or computer. As the fraud seemed to have progressed gradually, a key success factor under this hypothesis was the speed of the incident response.

It was then that the Director decided to act by informing all the employees of the School (message #3 - Fig. 3).

Time: 12:57 pm.

This post created the progressive reaction of many members who provided information to the Director by email, or by other means of communication. One of them sent the following interesting message to the Director, bringing new information on the modus operandi. It was also a sign that some colleagues were currently responding to the initial message "Hello are you available?" (message #4 - Fig. 4).

In this message, two aspects mitigated the impact of the fraudster's message: the French used contained small mistakes. In addition, generally French uses either the polite form "vous" (you) or the more familiar form "tu". Here, the fraudster used the polite form, while among colleagues, the "tu" is generally preferred. Moreover, a time difference was apparent. The first message was supposed to have been sent at 12:26 p.m., while the colleague's response is traced at 11:51 a.m. There are many possible explanations about the time indicated in forwarded emails, but this discrepancy might be explained by a timezone difference between the place from where the perpetrator is acting and the place where the recipients are located.

It also appeared from the series of message received by the Director, that members of the School did not receive the messages at the same time: the fraudster did not send the messages all at once.

It was at this point that the connection with message #1 made sense. Indeed, from this moment, the modus operandi became much clearer:

- Many members of the School have received the 'Hello are you available?' message;
- The perpetrator gradually sends messages, with a low degree of computerization and relatively poor French;
- The fraudster enters into a real-time discussion with their targets, pretending to be at a meeting preventing any other form of communication than email. He is asking for urgent help to get iTunes cards (see Fig. 1);
- At least one doctoral student (Y) has fallen into the trap of buying such cards;
- Due to time difference traced in the emails, there are signs that the perpetrator is located in another country.

A specific message was sent to Y who had just realized that she had been the victim of the scam.

Time: 01:15 pm.

The Director then decided that it was time to alert the IT department of the University to the current situation, at least by an email to the helpdesk (this is how staff are required to communicate with the department). The sender of such an email immediately receives an automatic reply, certifying that the request will be taken into account. The message contains a ticket number. In our situation, this kind of response was very frustrating because time was critical for the immediate handling of the fraud. The Director tried to call the IT department but was unsuccessful, the employee insisting that he forwarded the request and rejecting the idea of creating a link with the person in charge.

Time: 01:37 pm.

At the same time, remote WhatsApp exchanges continued within the small crisis unit composed of the forensic expert and the Director. Hypothesis A continued to be confronted with Hypothesis B. The balance, however, tilted towards Hypothesis B, knowing that only members of the School had so far shown signs of having received the "Hello are you available?" message. However, the Director checked Hypothesis A in more depth by asking others in his email contacts if they had also received the message. As it was the holidays, he only received one negative response, 3 hours later.

The Director then attempted, by email, to inform an investigation service of the police specializing in the fight against cybercrimes. He has frequent contacts for research with this department.

Time: 01:58 pm.

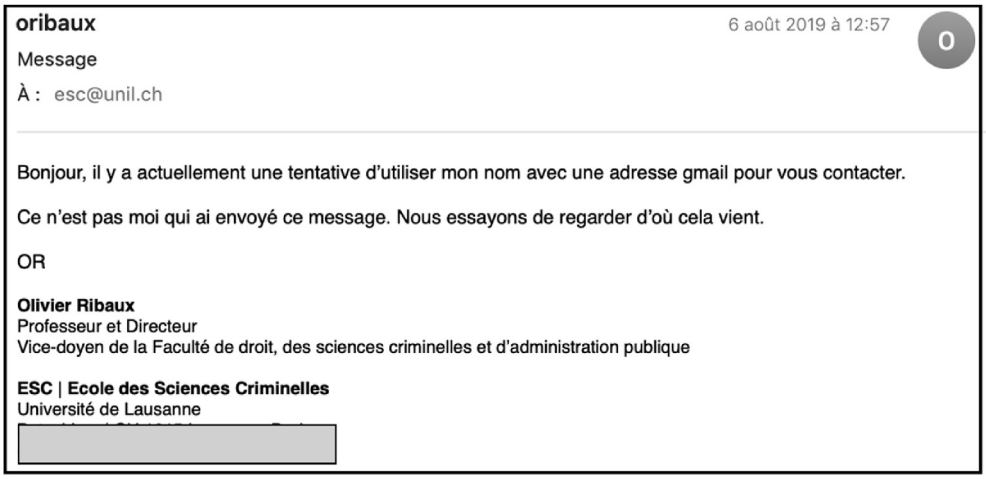

Fig. 3. The email sent to all the employees of the School (message #3). "Dear all, there is currently an attempt to use my name with a Gmail address to contact you. I did not send this message. We are trying to find out where it came from".

Please cite this article as: Ribaux, O., Souvignet, T.R., "Hello are you available?" Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

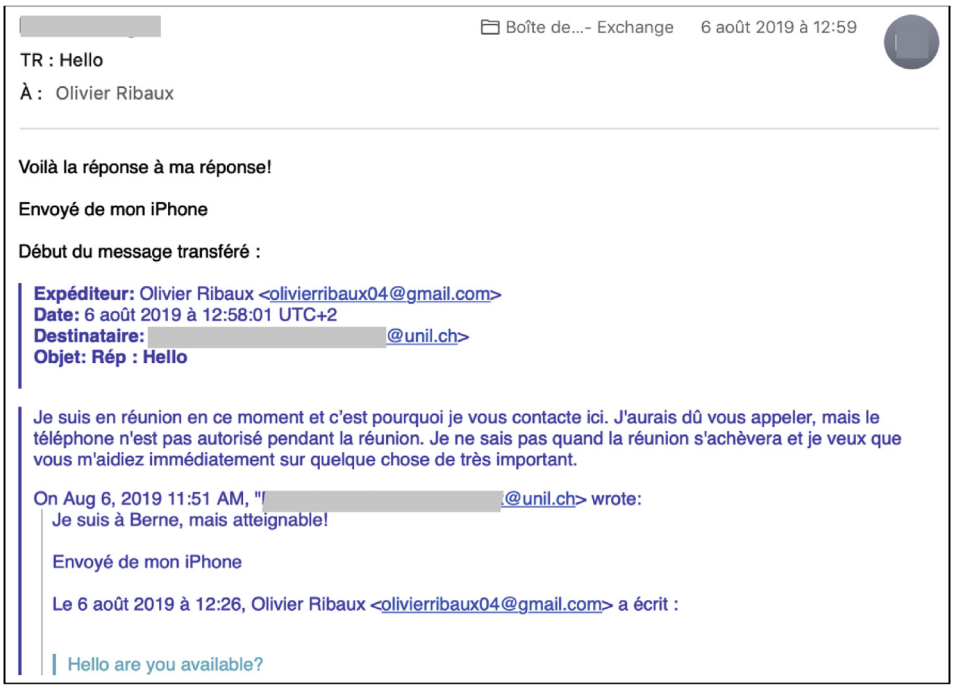

Fig. 4. Thread of a conversation with the fraudster (message #4). We translate. The colleague: 'I am in Bern, but reachable'. The fraudster: "I'm in a meeting right now and that's why I'm contacting you through here. I should have called you but phone is not allowed to be used during the meeting. I don't know when the meeting will be rounding off and I want you to help me out on something very important right away." Note the time difference of 1 hour between the sender and the receiver.

A little later, the IT department of the University eventually provided an answer with the following content (translated from French):

"Following your message, our team produced a script to intercept any mail sent to the "false" address."

We learned later that the script was already implemented at 1:44 p.m., 7 minutes after receiving the Director's message. This action considerably limited the possibilities for the fraudster to continue to deploy his/her fraud. The IT department then collected all the emails that were sent to the fraudster and warned the people concerned not to interact with him.

Time: 02:26 pm.

The next hour and a half was mainly devoted to:

- responding to the numerous messages sent by members of the School about the fraud;
- attempting to obtain the IP address of the fraudster's computer by trapping a message sent to him/her. This was before anyone knew that the IT department had redirected the messages sent to the fraudster from the School. Indeed, this specific trapped message was read by the IT department, providing a location of the IP number on the Campus. This misdirection created some confusion about a possible intervention on the Campus!
- continuing to weigh Hypothesis A versus B. The police cybercrime department eventually provided advice along the same lines as Hypothesis A (the same as the forensic expert). However, further inquiries and evaluation of available information made it clear that Hypothesis A had to be rejected in favour of Hypothesis B;
- discussing new information from the Computer Science Department, which mentioned that other departments of the University had been similarly victimized.

The fraud was finally considered to be over. At 03:58 p.m., a new message was sent to all employees of the School, mentioning the reality of the fraud and the measures that had been taken to secure the environment.

4. The post-incident analysis

A post-incident analysis was considered essential:

1. Meet with Y to address the potential psychological and financial impact of being victimized by fraud (message #1);
2. Determine if other members of the School were affected by the fraud. It was obviously very delicate, due to privacy and the fact that potential victims would not want to let it be known;
3. Learn more about the modus operandi, the extent of the fraud and the perpetrators would help assess the need to report the matter to the police for prosecution;
4. The School, as an organization, must constantly analyze its vulnerabilities and the effectiveness of its responses to incidents. Since the fraud may have concerned the whole University (and beyond), such an analysis would also be of interest beyond the School's structure;
5. The School shall deploy intensive research on crime transformations and how to situate the role of criminology and forensic science in their study and treatment. Such a case would also constitute relevant teaching material.

4.1. Method

During the two weeks following the fraud, six lines of actions were chosen to gain a more comprehensive understanding of the fraud and associated crime phenomenon and victimology:

1. It was decided to interview Y, in order to discuss the whole thread of the discussion with the aggressor, and address the potential psychological and financial impact on her;

2. An anonymous survey was quickly organized inside the school (one week later) to assess the number of people who received the message "Hello are you available?", when they received the email, if they have been victimized, if a category of employees has been specifically targeted, in what order. The response rate was 66% (N = 76);
3. Open source forensic data was analyzed to learn more about the modus operandi, trying to locate the offender(s), and to determine if the case was worth reporting;
4. A literature and open sources research was carried out to discover if similar modus operandi were already known, in which context and what kind of interpretations was available;
5. A meeting with the IT department was organized to discuss the fraud, its evolution, its interaction with the department during the event, to examine other available traces and possible future actions.

Due to the lack of time, resources and knowledge, it is not claimed that all of these dimensions have been dealt with in a sufficiently structured and comprehensive manner. However, they each illuminated different aspects of the problem which helped clarify its interpretation.

4.2. Results

The main result for the School that emerged from this analysis is that no one seems to have been ultimately victimized. Even Y, once informed of the fraud, finally succeeded in canceling the order.

The specific mechanisms of the fraud was investigated. They were mainly based on the traces, and email exchanges collected from the members of the School.

4.2.1. Pattern of activity

If the perpetrator had not obtained the email addresses of a member of the School, how did he proceed? The hypothesis that he or she visited the institutional site was naturally formulated. This website offers access to the individual page of each member of the School, containing the profile of each employee, including their email address, as well as their position. Another page describes the structure of the School with the name of its Director, its vice-directors, and administrative staff.

If the fraudster had visited these pages, then traces of such accesses should be detectable. Google analysis tools were installed on the pages concerned and could provide indications. However, the site of the School is usually accessed frequently. The feasibility of distinguishing the traces left by the crooks from those left by the usual accesses to the site was questionable. It is an elementary reasoning in forensic science. If a systematic scan of the page of each member of the School had taken place, this should be visible in the traces detected by the Google tool.

The result was particularly convincing. A clear pattern emerged. It indicated that something unusual happened at the site on August 6 and that vibrations had already occurred the day before (Fig. 5).

Finally, some indications on the origin of the fraud were also sought: many accesses to the site were traced by the Google analysis tool, pointing to Lagos, in Nigeria. These traces find no reasonable explanation other than the preparation and execution of the fraud. Why would a systematic access to all pages of the School's members from Lagos have occurred on that date and some of them the day before? The School has no specific agreement or collaborations with Nigeria. An access to the administrative page was also noticed in these traces.

According to the survey, all respondents reported receiving the first "Hello are you available?" email, and each at a different time. It was a strong confirmation that the fraudster had sent the messages one by one. From the more complete data processed by the IT department, it became clear that the fraudster sent from zero to four emails per minute (see also Fig. 6), by accessing the institutional page of each member of the School. This pace seemed to depend on the interactions he or she had with the people responding to their messages. The fraudster was then probably alone and doing the work by hand. In the exchanges of collected emails, it was clear that a time difference of 1 hour appeared systematically. This is exactly the time difference between Switzerland and Nigeria.

4.2.2. Specific thread

By studying specific threads of exchange, some interesting patterns emerged. Here is the thread concerning Y:

Fraudster(11:58 am): "Hello are you available".

Y (all the rest of conversation was in French, we translate – 12:00 pm): "Is it Prof. Ribaux? I don't recognize this email".

Fraudster (in French – 12:03 pm): "It is my personal email. I'm in a meeting right now and that's why I'm contacting you through here. I should have called you but phone is not allowed to be used during the meeting. I don't know when the meeting will be rounding off and I want you to help me out on something very important right away".

Y (in French – 12:06 pm): "Yes, of course. Today I was working from home but if you need I can come to the university in the afternoon without any problem. We can make an appointment for later if you wish. What do you think about it?"

Fraudster (in French – 12:12 pm): "You don't have to come to university. You have to help me get iTunes gift cards from the

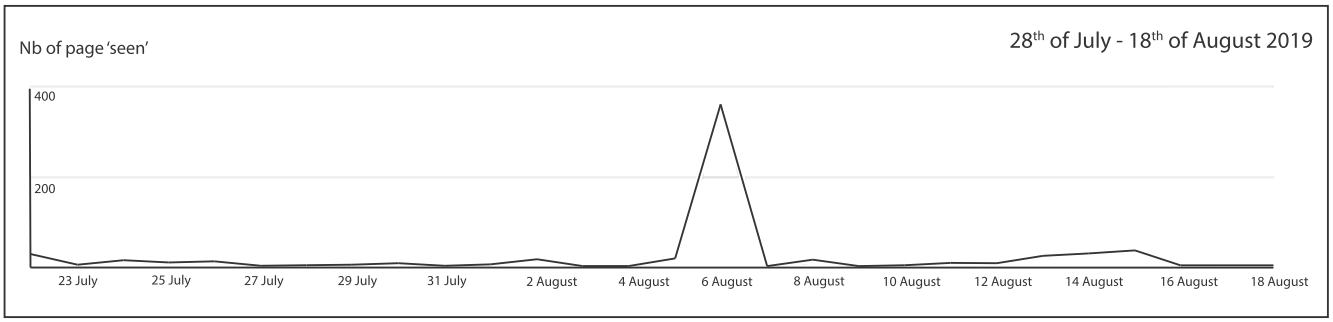

Fig. 5. Pattern of the activity. View of the number of individual pages "seen" (accessed) per day on the School's institutional site, a generated by "Google analytics". Beyond the obvious relevance of the pattern, the detailed concept of "pages seen" belongs to the google tool and should be understood as a third definition which is not entirely transparent to the authors of this article. An intuitive definition was, however, sufficient for the purpose.

Please cite this article as: Ribaux, O., Souvignet, T.R., "Hello are you available?" Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

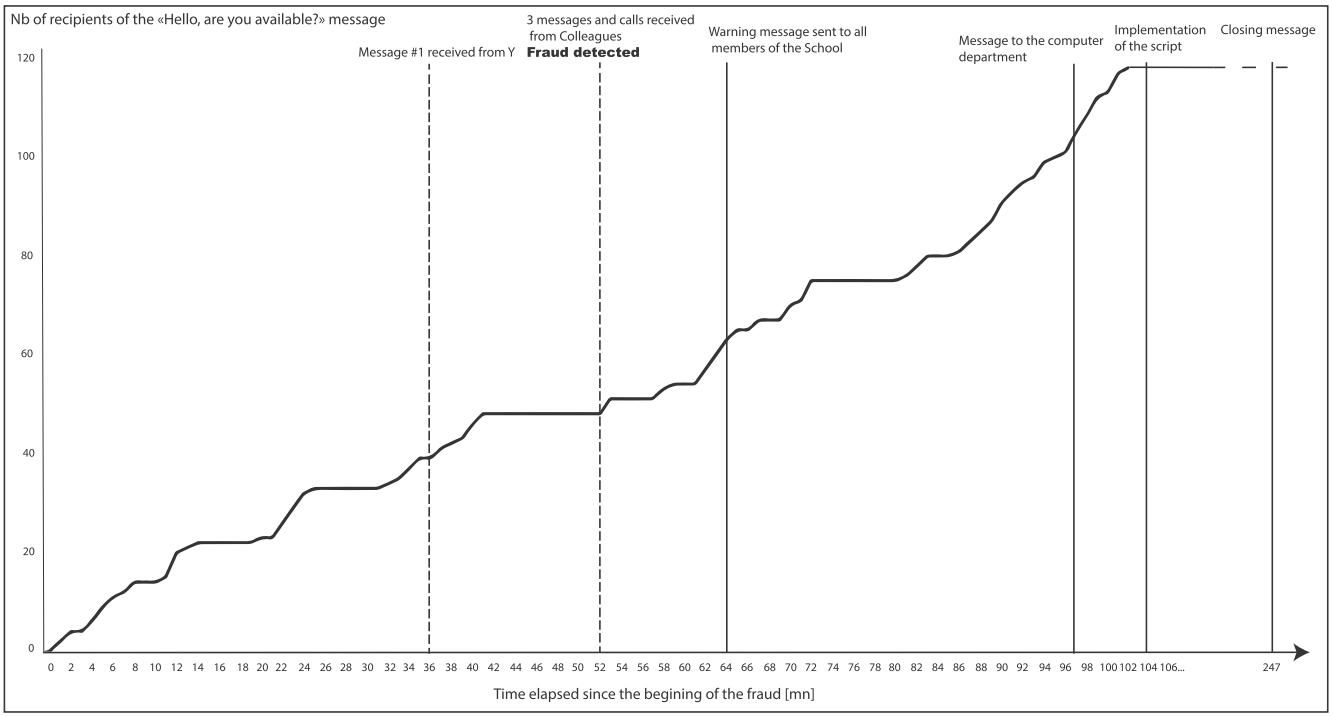

Fig. 6. Progress of the fraud and measures taken. A timeline showing the incoming flow of the "Hello are you available?" message that has been systematically sent to each member of the School. Fraud detection and actions taken are mentioned.

store and send them to me here, I'll pay you back, I'll have to send them to someone as soon as possible. »

Y– 12:16 pm): "Yes, of course, I can do it without any problem. Can you give me more details about this (amount, name of the recipient, etc.). - I have to put these details on the order."

Fraudster (12:24 pm): "I need you to get an iTunes card for CHF 200 and send it to al****ta@gmail.com"as the recipient. Thank you."

Fraudster (12:36 pm): "She wants physical ID cards from the store."

Fraudster (12:42 pm): "When you have them, scratch them, take pictures of the cards and attach them to this email, then send them to me here or to his email, okay."

Y (12:45 pm): "Isn't it the same as buying online? I'm sure you receive a code with which you can access it. Otherwise I can go to the store but it seems to me that it is the same process."

Fraudster (12:50 pm): "Go to the store and get a physical iTunes card. It can be 100 CHF in 2 pieces."

Fraudster (12:54 pm) "When you receive them, scratch them, take pictures of the cards and attach them to this email, then send them to me here or to al****ta@gmail.com."

Fraudster (01:19 pm): "Do you have the cards? I'm waiting for the cards"

Eventually at 01:39 pm, Y sent message 1 (Fig. 1) attesting that she had bought the cards, but online.

During the conversation, the fraudster showed some impatience. For unknown reasons, he/she insisted on receiving photos from the code of a real card, to be sent to another address (al****ta@gmail.com), rather than the code from an online order. This created confusion. The tone of the fraudster seems more and more imperative and authoritarian.

Another interesting aspect emerged from the collection of threads: when the first answer was in English, the rest of the conversation continued in English. When the first answer was in French, it continued in French. As a test, the first message was translated with "Google translation" (Table 1). If this tool was actually used by the perpetrator, this could have important consequences on the extent of the fraud, as will be discussed below.

4.2.3. Other data available on the fraud

The university's IT department informed us that other departments had also been affected before the school was. Subsequently, emails coming from other departments and further exchanges of information with the IT department showed that certain departments have been affected also after the School was.

Based on the survey, we were able to confirm that some members of the School responded to the first "Hello are you available?" message. Few of them continued the conversation, as they detected the fraud early on. This was confirmed by the IT department. Finally, on the basis of their data, they could determine that each member (except the Director) received the "Hello are you available?. The profile of the person who have answered the first emails distributed in:

- A new employee;
- Researchers who do not speak French, and are using English at the School;
- Professors having a strong daily interaction with the Director.

In addition, we were able to compare the number of people from the School who responded with the number of people from another department who responded to the fraudster (the name of this department is unknown to us) (Table 2):

This fraud is very global. On the Internet, it is very easy to find

Table 1
The text translated from English to French through the online available tool 'Google translation'[31] is exactly the text sent by the fraudster when the first answer of the message was in French. It contains some minor mistakes in French.

English	Automatic translation in French
I'm in a meeting right now and that's why I'm contacting you through here. I should have called you but phone is not allowed to be used during the meeting. I don't know when the meeting will be rounding off and I want you to help me out on something very important right away	Je suis en réunion en ce moment et c'est pourquoi je vous contacte ici. J'aurais dû vous appeler, mais le téléphone n'est pas autorisé pendant la réunion. Je ne sais pas quand la réunion s'achèvera et je veux que vous m'aidiez immédiatement sur quelque chose de très important

Table 2
Another department had also been targeted by the fraudster 20 days later, with the same modus operandi. The size of the department was much smaller, but the modus operandi seems to have had a greater impact.

	Shool of Criminal Justice	Other department
Number of members having received the « Hello are you available?" message	118	19
Number of people who responded to the first message	7 (6%)	15 (79%)
More than two exchanges	2 (1,7%)	4 (21%)
Date and duration	August 6, 2019, 1:53–15:38 (3h 45 min)	August 26, 2019 16:23–18:16 (1h 53 min)

examples of many institutional websites and IT departments of Universities, preeminently in North America, warning against such fraudulent activities throughout 2019. These reports show how the fraud has been persistent for at least one year. Bernstein (2019) also discusses some of the author's limitations regarding the language used, which is not meant to fit the style of an academic administrator. Beyond this, in a subsequent presentation (Perrig, 2019), it was learned that one of the most advanced laboratories in cybersecurity in the country had also been the target of the fraud, at the beginning of the year: 25% of the members of the department immediately rushed to the boss's office in reaction to the message "Hello are you available?". Eventually, a description of the fraud was found in the "Chronicle of higher Education".[4] This article highlights how expectations, desires and pressure on researchers can create a breeding ground for such frauds in universities.

4.2.4. *Synthesis of the modus operandi and victim profiles*

This analysis leads to assume:

- It is a global fraud, but it is specifically targeted at university departments;
- The perpetrator (alone), based in Lagos (NG), studied the structure of the ESC through the institutional site;
- He or she systematically sent the message "Hello are you available?", in order of appearance on the site. It took approximately 1 hour and 45 minutes to reach all members of the School;
- He or she was reactive, responding in the target language, using Google translation if necessary;
- He or she wanted to get codes for iTunes gift cards;
- He had estimated the reasonable amount to ask for CHF 200 (about 200 US$);
- He or she used progressively more authoritarian language;
- He or she planned to use a different address to manage the stolen codes. The monetization strategy remains unknown, however;
- The fraud had an impact on new employees and foreign doctoral students, who did not know the usual communication styles used. Also, professors who have a high degree of operational relationship with the Director.

[4] https://www.chronicle.com/article/Phishing-Scheme-Targets/245535, January 23, 2019, The chronicle of higher education.

The success of the fraud is strongly based on social engineering. It can be considered a priori as a fraud that is not really based on technology. However, it should be noted that everything relies on complex technological infrastructures fully integrated into daily life, and having radically changed the modes of communication and opened new opportunities for fraudsters. In addition, the possible use of an automatic translator, and therefore of artificial intelligence, has changed everything on the scale and the global potential of this fraud. Fraud was on the one hand very targeted (University departments), but, on the other hand, probably globalized on a very large scale through machine translation (see section 4.2.2.).

5. Lessons learned, reporting and possible plans of action

This case has the potential to raise many general questions about how high-volume online frauds are handled by professions, and studied by academia.

Several positions have been adopted here by the Director and the forensic expert having dealt with the case:

- as a manager, the Director felt responsible for what was going on; the fact that an unknown person tried to impersonate him to extract money from his colleagues worked as a powerful driver of this feeling;
- a manager is also concerned with the organization of the security of the establishment, in particular with the way in which it is protected against standard fraud and by its resilience in the event of a cyber-attack. The lessons learned from this situation are therefore of the greatest interest from this point of view;
- their experience in computer science, crime analysis and digital forensic science with police practice clearly guided their understanding of the situation and their reaction;
- they are, as researchers, particularly interested in the transformations of crimes by digitalization, and about the role of digital forensic science.

This fraud does not correspond to a high-level technological crime. Rather it belongs to these volume cyber-crimes that insert into daily life and routine activities (Felson and Boba, 2010). There is no existing "profession" that would adequately prepare for both the handling of this case in real-time, and for supporting its overall interpretation. This was made very concrete by the ad hoc manner in which the fraud was detected, the institutional vacuum that was faced during the management of the crisis, and the post-analysis of

the specific fraud, which was poorly treated in the scientific literature across disciplines.

This discussion is structured along four dimensions: (1) what worked and what did not work both in the detection and handling of the case, (2) general consideration about how this case can be situated in current research about online frauds, and (3) what was reported from the case and more global action taken, and (4) the role of forensic science.

5.1. The detection and the response to the situation

The timeline (Fig. 6) shows the progress of the fraud, its detection and the measures that have been taken. The fraud was detected when about 40% of the School's members had already received the message “Hello are you available?".

5.1.1. The detection and first measures

By a closer reading of the message from Y (message #1), the detection time could have been shorter.

This is a common problem in serial crime analysis: the detection of a previously unknown problem takes time, even when the relevant data are already available and systematically monitored (Grossrieder and Ribaux, 2019). In this particular case, the filtering system set up by the IT department did not detect the fraud and the anti-spam measures were ineffective. The early reaction of some colleagues triggered the detection, demonstrating a certain level of awareness within the organization. Once the problem was detected, retrospective analysis showed that it was already active before, and the readiness to recognize a future occurrence became much greater. This is also a very common mechanism in crime analysis.

The time elapsed since the message to all the employees was sent (12 minutes after the fraud was detected), could have been shorter. At that time, about half of the members of the School still had not received the message “Hello are you available?”. Most people reacted very positively to this warning. The difficulty of immediately recognizing the specificities of fraud and its targeted nature (Hypothesis A, known modus operandi against Hypothesis B, unknown modus operandi) explains the reluctance to send the alert message earlier. If the precise modus operandi of the fraud had been known earlier, the elapsed time would have been shorter.

The time that had elapsed since the University's IT department was alerted was also too long. For their part, the reaction time was very short. It only took, at lunch time, 7 minutes to implement a script to block outgoing mail. However, their accessibility in terms of tickets asking you to wait your turn is clearly not adequate in case of emergency. It is clear, however, that university IT departments are overwhelmed by the number of messages, of varying degrees of urgency, they receive. They must organize a request management system. Beyond, they are professionalizing their overall approach to cybersecurity, including incident response, and the monitoring of scams that reach and target universities. They are also seeking to raise the level of awareness in their organizations. However, there is a concern that their approach only draws on common-sense knowledge of criminology, intelligence and forensic science.

5.2.2. Reporting and subsequent measures

The knowledge gained through this case has obviously been of interest to the School, the University, and beyond that to all Swiss universities. There was no reason why the fraud should not spread further. As the modus operandi was known in detail, tailor-made prevention actions were relatively easy to determine.

The case was reported through different channels with the aim of making knowledge available to take repressive or preventive measures to be taken at a strategical or operational level:

- almost immediately, a presentation of the case was made in a meeting of all the responsible of IT security departments in universities;
- several presentations were provided to the management of the University, as well as to many colleagues under different contexts;
- an email prepared by the IT department was sent to all the departments one month later; as well as an article in the journal of the IT department[5] (four months later);
- a presentation in the form of a debriefing was organized specifically for the members of the School three months later;
- a presentation was organized for middle managers of the police at a regional level;
- a presentation is planned for the International Association of French-speaking Police Psychologists.[6]

Feedback received after such a dissemination indicate some impact of these measures. The debriefing at the School was obviously very impactive, because it was based on something vivid. This awareness raising initiative may even have exceeded a threshold of information saturation. This sensitization to the problem should significantly reduce the chances of successfully deploying similar online frauds in a near future.

From the traces collected, which show a clear pattern of access to the institutional site, it would certainly have been possible to develop a more technological approach to automatically capture the first signs of future attempts. This was not considered, mainly for privacy reasons, and also on the basis of the amount of effort to be made in balance with a subjective assessment of the impact of the fraud and the effectiveness of the measure.

The psychological impact of the fraud was not to be underestimated either. This point is much clearer in a new literature in criminology (Button et al., 2014a; Cross, 2018). Debriefing with those involved was considered a major objective. For the Director having been impersonated by the fraudster, the impact was not neutral at all.

Prosecution was ultimately a key point to address. Was it worth reporting? Indeed, it was not so clear whether, from the point of view of the criminal code, it was actually a crime. There was evidence of preparation and some attempts to commit fraud. If the activity was considered a crime, it is then not clear that the preparation and attempts would have been considered a crime. In imagining the likely origin of the fraud (Nigeria), it would have been doubtful whether all the investigative efforts across jurisdictions had been carried out for activities that are hardly considered a crime, without anything of financial worth being stolen.

Finally, digital traces available to the School were used extensively throughout the analysis or from a more investigative perspective. The evaluative strength of these available digital traces was low. However, if we consider the situation as a whole, this is a type of serial fraud and the perpetrators could act on a fairly large scale. There is a lack of knowledge to support the triage of online fraud activities between petty individual crimes and large-scale, organized serial crimes that are worthy of prosecution. Whatever these considerations, the case has been

[3] Translated the 22nd of September 2019, through https://translate.google.be/.

[5] http://wp.unil.ch/cinn/2019/12/lunil-victime-de-spear-phishing-une-arnaque-sur-mesure/(accessed the 30th of December, 2019).

[6] Cercle des psychologues francophones de la police.

Please cite this article as: Ribaux, O., Souvignet, T.R., “Hello are you available?” Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

transmitted to the police to contribute to their experience investigating fraudulent activities, and presented to middle level managers for training purposes.

6. Some more general considerations and the role of forensic science

The handling of this specific case was satisfactory, given its scope, impact and low severity. Some would even say exaggerated. Whatever these opinions, it was clear that members of the School, specially the persons who had to directly respond to the incident, were frustrated by the absence of institutional and structured approaches for dealing with the case. The response here was entirely constituted ad hoc. Whatever degree of structure is deemed reasonable to deal with such crimes, there is a long way to the current and usual structured treatment of typical high-volume crimes or the comprehensive and effective implementation of new incident-response methodologies in cybersecurity. In this area, institutions, professions and methods are not fully prepared to deal with such pervasive crimes.

This case completely confirms opinions calling for more coordination and collaboration between private and public institutions, as well as the community in general. It is also a matter, especially for the police, of taking distance from systematic prosecutions, as a main objective (Dupont, 2017), in order to adopt instead more comprehensive intelligence-led approaches, implement crime analysis systems (Rossy and Ribaux, 2020), and develop knowledge about what works and what does not work in terms of prevention and repression.

Many relevant academic works are now emerging, but within the typical silos of the disciplines. For example, cybersecurity is mainly considered at a technological level (CMM, 2016); data scientists are promoting big data analysis (Grossrieder and Ribaux, 2019); psychologists and criminologists scrutinize the methods used by the fraudsters and their capacity for social engineering, the profile of the perpetrators, the vulnerability of the victims and the psychological impact of the fraud (Button et al., 2014a; Reep-van den Bergh and Junger, 2018; Whitty, 2019); criminologists focus on how to measure the phenomena (Reep-van den Bergh and Junger, 2018) or how these new frauds can be explained by existing theories and what are their mechanisms (Leukfeldt et al., 2017; Leukfeldt and Yar, 2016; Wall, 2010); forensic scientists remain auxiliaries of the criminal justice system focused on the collection, evaluation and presentation of evidence (Pollitt, 2010); not to speak about the law community trying to define relevant judicial dimensions. All these works are highly relevant for interpreting parts of our case, and some might be relevant for designing a response. However, there is no cybersecurity methodology that integrates in a balanced way all of these factors for dealing with such concrete fraud campaign. There are many initiatives to advance interdisciplinary work in academia, but few successes in deriving practical methodologies for dealing with problems when and as they occur.

In this context, what kind of viewpoint can be developed in the field of forensic science? Casey (2019) first mentions that forensic science and digital forensics should be much better integrated in order to develop a structured and robust forensic ecosystem to deal with the new situation. In particular, it is about developing harmonized methodologies for forensic preparedness, exploiting forensic intelligence, improving investigations, strengthening evaluation of evidence, and lightweight agile retrospectives to enable rapid improvements (Casey and Nikkel, 2020). Concepts have to be worked out in order to avoid re-inventing knowledge already developed for years in forensic science. Rather, they need to be adapted to take better account of new digital environments with a change of scale in the variety and volume of available traces, as well as new challenges in evaluating their probative strength (Pollitt et al., 2018).

Such a vision also allows for the integration of physical and digital traces to extract the information they convey about the many forms of crimes that have been transformed by digitalization, but still have a strong component in the real world (e.g. stolen goods sold on auction sites or illicit drugs sold on the darknet).

Going further, the trace is considered by Boullier (2017) as the most elementary data generated by human activities which should constitute the main basis for studying sociological phenomena in a digitalized society. The study of traces (traceology) generated by unusual activities on different types of substrates (physical or electronic) can be combined with crime analysis and, more broadly, to certain theories in criminology, in order to constitute a focal point where methodologies dedicated to the study of and response to digitalized forms of crime should be discussed (Ribaux, 2019).

Is it not obvious that much of the handling of the “Hello are you available?” fraud was based on traces generated by the activity of the perpetrator, even though there was ultimately no prosecution.

Conclusion

In the many cases where this type of fraud has appeared in the world, it probably did not trigger “crisis management”, a coordinated response, and a lightweight agile retrospective. It is not considered important enough and gives the impression that everything is already known and that it is part of everyday life with no significant loss. It does not seem challenging in technical or forensic terms, because the modus operandi is heavily based on social engineering. It is up to the users of the Internet infrastructure to protect themselves. In any case, prosecution is still too difficult, slow or even impossible in such situations. It seems that we cannot do much more until legislation and cross-border evidence exchange has been harmonized and designed to make the investigative process more effective (Biasiotti et al., 2018).

A similar situation has occurred in the recent history of policing. Traditional high-volume property crimes that cross jurisdictions (e.g. burglaries or all sorts of thefts and frauds) were increasing dramatically during the eighties, and have required a strong reaction. It took a long time to gradually define new strategies and new policing style. The solutions found have been more proactive and intelligence-led (i.e., not prosecution-focused), incorporating crime analysis models based on crime concentrations, opportunities theories in criminology and the use of physical traces. Knowledge about what works and what does not work in terms of crime disruption or harm reduction has also increased considerably during this period (Ratcliffe, 2016; Ribaux et al., 2006). By analogy, we are now in the same situation with online frauds than in the past with traditional high-volume crimes. The difficulties in prosecuting globalized crimes should be an incentive to find alternative solutions in the same spirit. It is necessary to develop a new, well-balanced, interdisciplinary proactive vision integrating digital traces and their interpretation at the heart of the process (Rossy and Ribaux, 2020).

We are far from this point. Larger institutions seem increasingly better equipped, both technologically and in terms of cybersecurity, to deal with such cases and protect themselves from cyberattack that endanger or cause harms to their activities. However, what became clear in our case study was effectively that there was no comprehensive approach to policing online fraud, from data collection to the production of intelligence that would point the way to responses that are known to be efficient. Responsibilities are scattered into many structures and areas of competencies. The relevant expertise is focused on prosecution (the police) or cybersecurity (other stakeholders), and hard to mobilize for collective

Please cite this article as: Ribaux, O., Souvignet, T.R., “Hello are you available?” Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978

problem solving in today's context.

The common attitude of taking current organizational settings and professions as rigid silos should be abandoned. When confronted with real cases, the problem is the centre of interest, not a predefined structure or area of knowledge. From the problem, solutions, not restricted to prosecution or to technology, must be found in real time either by finding the best skills and tools in agile organizations. It was clear, in this case, that a generalist vision of forensic science, incorporating criminological knowledge, as well as a certain police practice were a solid basis for handling the case. In this sense, such a case study can pave the way toward approaches to policing online fraud fully integrating a reframed vision of forensic science around the study of the trace (traceology).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would especially like to thank Julien Furrer, Yassine Ghennai, Chrisopher Greiner, Sorcha Keating, Lorena Molnar, and Quentin Rossy for their support in collecting and processing the data, as well as all members of the School of Criminal Justice, University of Lausanne, who made possible this study. We owe special thanks to Eoghan Casey for his very useful comments on earlier versions of this paper.

References

BCS, 2016. Crime in England and Wales-Year Ending March 2016. Retrieved from. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2016.

Bernstein, A., 2019. Minding the gaps in lawyers' rules of professional conduct. Oklahoma Law Rev. 72 (1), 125–148.

Biasiotti, M.A., Mifsud Bonnici, J.P., Cannataci, J., Turchi, F. (Eds.), 2018. *Handling and Exchanging Electronic Evidence Across Europe*. Law, Governance and Technology Series, vol. 39. Springer, Cham.

Boullier, D., 2017. Big data challenge for social sciences and market research: from society and opinion to replication. In: Cochoy, F., Hagberg, J., Petersson McIntyre, M., Sörum, N. (Eds.), Digitalizing Consumption, Tracing How Devices Shape Consumer Culture. Routeledge, London and New York.

Button, M., Lewis, C., Tapley, J., 2009. Fraud Typologies and the Victims of Fraud: Literature Review. National Fraud Authority, London. Retrieved from. http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-typologies-and-victims.pdf.

Button, M., Lewis, C., Tapley, J., 2014a. Not a victimless crime: the impact of fraud on individual victims and their families. Secur. J. 27 (1), 36–54.

Button, M., Nicholls, C.M., Kerr, J., Owen, R., 2014b. Online frauds: learning from victims why they fall for these scams. Aust. N. Z. J. Criminol. 47 (3), 391–408.

Casey, E., 2019. The checkered past and risky future of digital forensics. Autralian J. Forensic Sci. 51 (6), 649–664. https://doi.org/10.1080/00450618.2018.1554090.

Casey, E., Nikkel, B., 2020. Forensic analysis as iterative learning. In: Keupp, M.M. (Ed.), *The Security of Critical Infrastructures*. International Series in Operations Research & Management Science. Springer, Cham, p. 288.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. *Computer Security Incident Handling Guide* (800-61 - Revision 2). National Institute of Standards and Technology.doi:10.6028/NIST.SP.800-61r2.

CMM, 2016. Cybersecurity Capacity Maturity Model for Nations (CMM). Global Cyber Security Capacity Centre. University of Oxford, Oxford.

Cross, C., 2018. Mis)Understanding the impact of online fraud: implications for victim assistance schemes. Vict. Offenders 13, 1–20. https://doi.org/10.1080/15564886.2018.1474154.

Dupont, B., 2017. Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. Crime Law Soc. Change 67 (1), 97–116. https://doi.org/10.1007/s10611-016-9649-z.

Felson, M., Boba, R., 2010. Crime and Everyday Life, 4ème édition ed. Sage, Washington.

Grossrieder, L., Ribaux, O., 2019. Towards forensic whistleblowing? From traces to intelligence. Policing: J. Pol. Pract. 13 (1), 80–93. https://doi.org/10.1093/police/pax039.

Holt, T.J., Bossler, A., 2016. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge, London & New York.

Kent, K., Chevalier, S., Grance, T., Dang, H., 2006. Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology. Special Publication - 800-86). National Institute of Standards and Technology (NIST). Retrieved from. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (accessed the 1rst of April, 2020).

Leukfeldt, E.R., Kleemans, E.R., Stol, W.P., 2017. Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. Br. J. Criminol. 57 (3), 704–722. https://doi.org/10.1093/bjc/azw009.

Leukfeldt, E.R., Yar, M., 2016. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behav. 37 (3), 263–280. https://doi.org/10.1080/01639625.2015.1012409.

Loveday, B., 2018. The shape of things to come. Reflections on the potential implications of the 2016 office of national statistics crime survey for the police service of england and wales. Policing: J. Pol. Pract. 12 (4), 398–409. https://doi.org/10.1093/police/pax040.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018.

October 2, 2019 Perrig, A., 2019. E-ID: Sécurité augmentée ou menace à la protection des données?. In: Paper presented at the Forum Sécurité Suisse, E-ID: l'homme de verre dans le cyberespace?, October 2, 2019, Aarau, Switzerland.

2010// Pollitt, M., 2010. A history of digital forensics. In: Paper Presented at the Advances in Digital Forensics VI, Berlin, Heidelberg.

Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., Gladyshev, P., 2018. A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence. OSAC Task Group on Digital/Multimedia Science.

Ratcliffe, J., 2016. Intelligence-Led Policing, second ed. ed. Willan, Cullompton, UK.

Reep-van den Bergh, C.M., Junger, M., 2018. Victims of cybercrime in Europe: a review of victim surveys. Crime Science 7 (1), 5.

Ribaux, O., 2019. Reframing forensic science and criminology for catalyzing innovation in policing practices. Policing: J. Pol. Pract. 13 (1), 5–11. https://doi.org/10.1093/police/pax057.

Ribaux, O., Walsh, S.J., Margot, P., 2006. The contribution of forensic science to crime analysis and investigation: forensic intelligence. Forensic Sci. Int. 156, 171–181.

Rossy, Q., Ribaux, O., 2020. Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. Eur. J. Crim. Pol. Res. https://doi.org/10.1007/s10610-020-09438-3.

Wall, D.S., 2010. Micro-frauds: virtual robberies, stings and scams in the information age. In: Holt, B.S. (Ed.), Corporate Hacking and Technologiy-Driven Crime: Social Dynamics and Implications. IGI Global, Hershey, PA (USA).

Whitty, M.T., 2019. Predicting susceptibility to cyber-fraud victimhood. J. Financ. Crime 26 (1), 277–292.

Please cite this article as: Ribaux, O., Souvignet, T.R., “Hello are you available?” Dealing with online frauds and the role of forensic science, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2020.300978