COPING WITH CYBERCRIME VICTIMIZATION: AN EXPLORATORY STUDY INTO IMPACT AND CHANGE

Jurjen Jansen
NHL Stenden University of Applied Sciences[1]

Rutger Leukfeldt
The Hague University of Applied Sciences

Abstract

An increasing number of Internet users are dealing with cybercrime victimization. In order to find out whether victims adequately recover from cybercrime incidents, it is important to gain insight into its effects and impact on users. However, as it stands now, there is not much literature on the impact of cybercrime. We address this gap by qualitatively examining the impact of two types of cybercrime, namely phishing and malware attacks targeting online banking customers. We used the coping approach as a framework to study how victims deal with the negative events they have experienced. In order to study the impact of cybercrime and how victims cope with it, 30 cybercrime victims were interviewed. We observed that, next to financial damage, victims described different forms of psychological and emotional effects. Victims also reported various kinds of secondary impacts, such as time loss and not being treated properly when handling the incident. In addition, the interview data provided insight into cognitive and behavioral change, which potentially offers opportunities for cybercrime prevention. Our study demonstrates that the level of impact varies among cybercrime victims, ranging from little or no impact to severe impact. In addition, while some victims were only affected for a few days, some were still feeling the effects. The effects and impact of these fraudulent schemes on victims should therefore not be underestimated. We conclude that the coping approach provides a useful framework to study the effects and impact of cybercrime victimization and how victims recover from it. The results of our study provide a steppingstone for future studies on this topic.

Keywords: Cybercrime, financial impact, psychological and emotional impact, secondary impact, cognitive and behavioral change, coping theory

INTRODUCTION

The advances of technology provide opportunities for individuals, such as business and leisure activities, but they also offer opportunities for criminals to commit crime (Bossler & Holt, 2009; van Wilsem, 2011). In 2015, 5% of Dutch citizens aged 15 and over were victims of hacking, 4% of marketplace fraud, and 1% of identity fraud (Statistics Netherlands

[1] Corresponding author details: NHL Stenden University of Applied Sciences, Rengerslaan 10, P.O. Box 1080, 8900 CB Leeuwarden, the Netherlands. Telephone: +31 6 2830 3830. Fax: +31 5 8251 1950. E-mail: j.jansen@nhl.nl.

[CBS], 2016). Furthermore, the Crime Survey for England and Wales reported 3.6 million fraud incidents in the year prior to the study (Office for National Statistics [ONS], 2016). Of these, 1.9 million were cyber related. Additionally, about 2 million computer misuse incidents were reported, including malware and unauthorized access to personal information. Cybercrime therefore poses serious risks to society. Besides financial damages, the effects of cybercrime may lead to reputational damage and loss of goodwill and trust.

Because a substantial number of people have to deal with these types of crime, it is important to gain insight into their effects and impact on victims. However, victim perspectives on cybercrime are an underexposed topic in the literature. In addition, we need to understand whether victims adequately recover from, or effectively cope with, cybercrime incidents. Green, Choi, and Kane (2010) stressed that a better understanding of factors related to adaption after a crime event is crucial, primarily for victims' well-being. We contribute to this understanding for a particular type of cybercrime, namely online banking fraud.

This paper examines online banking fraud victimization and how victims recover from it. More specifically, we study the effects – financial, psychological, emotional and secondary victimization – and impact of phishing and malware attacks on online banking customers, two common fraudulent schemes affecting online banking in the Netherlands (Jansen & Leukfeldt, 2016). Phishing is the process that uses deception, i.e., impersonation, to retrieve personal information (Lastdrager, 2014). Phishing often starts with a deceptive e-mail, but fake websites and fraudulent phone calls are also used to intercept user credentials. Malware is defined as malicious software designed to infect a device, including viruses, worms, Trojan horses, and spyware. In this case, the malware targets online banking. Although malware can be considered a type of technical engineering, in some cases human action is necessary for such an attack to succeed; for example, by opening an infected attachment in an e-mail.

Research that considers online and offline fraud and the psychological impact on its victims is scarce (Button, Nicholls, Kerr, & Owen, 2014b; Schoepfer & Piquero, 2009; Whitty & Buchanan, 2016). When online fraud is studied, the focus is often on prevalence, financial impact, and victim characteristics (Kunst & van Dijk, 2009). Moreover, there is little research available that involves speaking with online fraud victims about their experiences (Cross, Richards, & Smith, 2016).

Button, Lewis, and Tapley (2014a) argued that the public perception of (online) fraud is often that of a victimless or low-impact crime. For example, the public may believe online fraud is instigated by credit card fraud in which victims tend to be financially compensated for their losses, or committed against larger companies who have adequate resources to compensate for the damages. However, they exposed this as a myth by showing that some of the fraud victims that they interviewed and surveyed reported devastating impacts. The fraud scams that they investigated included identity fraud, boiler room fraud, investment fraud, and lottery fraud. We contribute to literature by studying the consequences of, and recovery from, online banking fraud victimization.

We believe that insight into cognitive and behavioral coping responses that fraud victims use might present opportunities for online fraud prevention. Extensive research on these aspects is currently lacking in the cybercrime domain. We take a critical (victimology) angle to broaden the scope of analysis to include a consideration of harm rather than crime, and social justice rather than criminal justice (McLaughlin & Muncie, 2005). Whereas criminal law is about doing justice, victims are interested in coping with injustice or the harm that is done to them.

The remainder of this paper is structured as follows. In Section 2, the theoretical background is outlined. We describe what is known in the literature about the effects and impact of crime and coping strategies related to victimization. Section 3 covers the methodology adopted in the current study and the results are presented in Section 4. The limitations and discussion are the central themes of Section 5, and the concluding remarks are addressed in Section 6. In sum, our study tries to answer the following research questions:

RQ1: What are the financial, psychological and emotional effects of online banking fraud victimization?

RQ2: What are the secondary victimization effects of online banking fraud victimization?

RQ3: What impact does online banking fraud have on its victims?

RQ4: What are the cognitive and behavioral coping responses to online banking fraud victimization?

BACKGROUND LITERATURE

The background literature provides theoretical insight into the effects and impact of crimes and coping strategies to deal with the effects and impact of crimes. This information will be used to reflect on our findings. Because the topic of interest belongs to a small field of work, the literature review was broadened to more general crime and victimization studies.

Effects and impact of victimization

Dignan (2005) described victimization as a highly complex process as it is made up of at least three different elements, two of which are discussed at the end of this section. The first element that he described is the interaction between the victim and the offender and the effects from that interaction or from the offense itself. Crime in general can have several possible effects on victims. The effects can be divided into the following categories: physical, financial (both direct and indirect), psychological and emotional (both short-term and long-term), and social relationships (Dignan, 2005; Lamet & Wittebrood, 2009; Shapland & Hall, 2007), and are also applicable to online fraud victimization (Button et al., 2014a; Cross et al., 2016). Furthermore, the effects can be felt by the social environment of the victim (indirect victimization), such as family, friends, and colleagues (Shapland & Hall, 2007).

A wide range of possible effects of crime victimization – both online and offline – are reported in the literature. Such effects include distress, irritation, anxiety, concentration problems, sleeping trouble, lowered self-esteem, posttraumatic stress disorder, and losing trust in online commerce (Cross et al., 2016; DeValve, 2005; Kirlappos & Sasse, 2012; Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2003). Additionally, victims lose the perception that they are invulnerable to victimization (Frieze, Hymer, & Greenberg, 1987). However, it is difficult to accurately describe the precise effects of certain types of crime as they can be similar to one another (Shapland & Hall, 2007). For example, Schoepfer and Piquero (2009) pointed out that victims of fraud – which can be considered as a type of non-violent financial crime – experience similar effects to those felt by victims of violent street crimes. Thus, fraud crimes may also have serious consequences for victims.

Dignan (2005) made an important distinction between effects and impact. According to him, impact relates to the perceived intensity of the effects plus their duration from a victim's (subjective) viewpoint. The precise effects and impact of victimization may differ from crime to crime, but can also differ for the same crimes, prompted by individual characteristics, including age, gender, and income (Button, et al., 2014a; Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Women, for example, often experience more or more severe psychological consequences than men, at least for offline financial crimes (Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Shapland and Hall (2007) also mentioned that domestic circumstances and certain life events can have an influence on how the effects of victimization are perceived. They concluded that it is "extremely difficult to predict which individual victim will suffer which effects to what extent" (p. 179).

Green et al. (2010) argued that victims make adjustments to the effects of crime on a continuous basis. Frieze et al. (1987) distinguished between immediate, short-term, and long-term reactions. According to them, the first stage lasts from hours to days and reactions typically include numbness, disorientation, denial, disbelief, and helplessness. The second stage lasts from three to eight months, and includes fluctuations in feelings such as from fear to anger, from sadness to elation, and from self-pity to guilt. In the last stage, the victims resolve the trauma they have experienced by adopting successful coping strategies. However, Frieze et al. (1987) also argued that long-term effects can be problematic for the victim's well-being, leading to depression, fear, guilt, low self-esteem, and relationship difficulties for instance, which has also been demonstrated in more recent studies (Denkers & Winkel, 1998; Hanslmaier, 2013). For instance, a study on white-collar crime victims by Shover, Fox, and Mills (1994) reported that victims suffered from psychological and financial harm even years after the incident. For online fraud victimization, anecdotal evidence is provided by Cross et al.'s (2016) study that reported long-term emotional effects of some of the victims they interviewed.

The second and third elements Dignan (2005) identified were victims' reactions to the offense and interactions of victims with other parties as a consequence of the offense. The former relates to changes in self-perception, attitudes, and behavioral responses (these changes are examined in greater detail in the next section). Within the current context, the latter deals with organizations such as banks and criminal justice agencies. Any negative impacts resulting from these interactions can be labeled as secondary victimization. These include not being treated properly when reporting the incident, inappropriate disclosure of status information, careless handling of sensitive information, and poor functioning of criminal justice (Kunst & van Dijk, 2009). Secondary victimization is important to consider as it can worsen the harm felt by victims (Cross et al., 2016), and hinder the victims' recovery from crime (Wemmers, 2013).

Coping with victimization

After an individual has been victimized and experienced some of the effects as explained in the previous section, he or she has to invest effort to overcome the situation. For this study, we use the coping approach as a framework to describe these efforts. Lazarus and Folkman (1984, p. 141) defined coping as "constantly changing cognitive and behavioral efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person." In other words, coping is a dynamic process of dealing with situations in which an individual is confronted with fear, stress, or threat. In the current context, we define coping as cognitive and behavioral responses against online

banking fraud and its impact, resulting in psychosocial adaptation to the stressful event. How stressful an event is depends on an individual's cognitive appraisal.

The coping process starts after two appraisal processes, which Lazarus and Folkman, (1984) referred to as primary appraisal and secondary appraisal. In short, appraisal processes comprise evaluations of the significance of what is happening in relation to one's well-being. These evaluations are affected by personal and situational factors and are often subjective in nature because individuals do not always have access to full information. Basic outcomes that are affected by appraisal and coping processes are functioning in work and social life, morale or life satisfaction, and somatic health (Lazarus & Folkman, 1984).

In the primary appraisal process, an individual evaluates why and to what extent the person-environment relationship is stressful (i.e., harm/loss, threat, and challenge). Note that a situation is not always evaluated as stressful; it can also be evaluated as irrelevant or benign-positive, respectively having no effect on or enhancing a person's psychological well-being (Lazarus & Folkman, 1984). When the situation is perceived stressful, an individual evaluates the options of how to deal with it in the secondary appraisal process. This is quite a complex process in which individuals not only need to consider coping responses, but also the efficacy of the coping response, one's self-efficacy related to performing the coping response, and the possible costs of the response (Lazarus & Folkman, 1984; Maddux & Rogers, 1983).

As our study deals with victims who are already confronted with a stressful situation, we are mainly interested in the coping process. Note that coping can take place before (threat anticipation), during, and after events (Beaudry & Pinsonneault, 2005). Frieze et al. (1987) divided coping strategies into cognitive and behavioral coping strategies. Another division that is made when dealing with stressful appraisal is problem-focused coping and emotion-focused coping (Lazarus & Folkman, 1984).

Problem-focused coping aims to solve an undesirable situation by tackling the direct cause of a problem or threat. Lai, Li, and Hsieh (2012) identify two types of problem-focused coping in the information systems context: technological and conventional coping. An example of the former is installing or updating anti-virus software to protect a device against future malware attacks. The latter deals with the behavior that an individual displays without using technology; for example, checking the account balance for inconsistencies. Lazarus and Folkman (1984) defined these as strategies directed at the environment and strategies directed at the self.

Emotion-focused coping aims to change undesirable feelings and emotions towards a problem or threat, such as stress, anger, fear, sadness, and helplessness without taking actions against the actual cause. Examples of emotion-focused coping include cognitive strategies such as avoidance, distancing, and selective attention, and behavioral strategies such as meditating, seeking emotional support, and having a drink (Lazarus & Folkman, 1984). Emotion-focused coping does not change the objective reality, but helps individuals to manage their emotions or control their emotional distress (Green et al., 2010), which is also important for effective coping (Lazarus & Folkman, 1984). However, such strategies can lead to a false perception of reality (Liang & Xue, 2009).

Emotion-focused coping is likely when an individual comes to the conclusion that nothing can be done about a situation, whereas problem-focused coping is more likely to be adopted when a situation is perceived to be changeable or controllable (Lazarus & Folkman, 1984). Liang and Xue (2009) stated that rational individuals are likely to use problem-focused

coping as a strategy because they probably have the required knowledge and the necessary skills to do so. However, if individuals do not find a solution to mitigate a threat or if they adopt an ineffective measure (e.g., anti-virus software that cannot detect new variants of malware), then they will have to use an emotion-focused strategy in order to maintain adequate levels of psychological well-being. Furthermore, these strategies are not opposites per se; they may also complement each other. For example, installing anti-virus software is a problem-focused strategy to mitigate malware attacks, but an emotion-focused strategy is applied as well, i.e., hoping that one will not contract a malware infection (Liang & Xue, 2009). Moreover, problem-focused and emotion-focused coping influence each other, which can be either facilitating or impeding (Lazarus & Folkman, 1984). Thus, although the problem-focused strategy appears to be the preferred one – since taking actions against a threat or harm seems more meaningful than changing relational meanings (Liang & Xue, 2009) – emotion-focused strategies are also very relevant for effective coping.

The extent to which a victim is able to regulate emotions can result in the victim denying, nullifying, or coping with victimization (Frieze et al., 1987). For coping to be effective, it is important that individuals (in time) move beyond seeing themselves as a victim. The extent to which victims perceive themselves as victims depends on whether the situation is cognitively evaluated as a harmful stressor or not. According to Matthieu and Ivanoff (2006), a stressful event becomes a stressor when it is perceived to have a negative impact on one's personal well-being. Thus, regardless of what is objectively defined as victimization, "victims" may not subjectively perceive themselves that way. Indeed, what some may consider stressful may not apply to others. This is primarily down to one's personal characteristics – some are more sensitive or vulnerable than others towards certain events – and the nature of the event (Lazarus & Folkman, 1984).

It is also important that victimization is recognized by others. However, this is not always obvious, because the offense itself might be evaluated as a victimless crime (Button et al., 2014a). Additionally, victimization might not be recognized because of the perceptions people hold about what constitutes being a victim. The "ideal victim," based on Nils Christie's definition, is likely to be female, sick, very young, very old, or disabled (or a combination of these attributes) (Dignan, 2005). When these attributes are not met, then the victim status will be less likely assigned, resulting in victims being given less recognition and/or being taken less seriously. In other words, the more innocent victims are perceived to be, the more likely it is for others to see them as victims. Similarly, if victims deviate from this image, i.e., when perceived to be not "ideal", this will be less likely.

Additionally, the circumstances play an important part in making an ideal victim according to Christie's typology. When victimization is perceived unavoidable, people are more easily assigned the victim status. This is also the case when it is believed that victims engaged in practices they thought were legitimate and, therefore, can be considered blameless for what had happened. An unknown attacker who is unambiguously evil is also of significance. Finally, victim status is more easily assigned when victims display the right combination of power, influence, and empathy (Dignan, 2005). The question is to what extent people believe online banking fraud victims to be truly innocent, as the victims – at least for phishing – adhered to what perpetrators demanded from them. However, the extent to which victims perceive themselves to be "victim" and their perceptions on how others viewed them is beyond the scope of the current study.

Coping efforts not only involve cognitive adjustments, but also taking action. Behavioral actions include locating the perpetrator (and demanding the stolen goods or

compensation for what was lost, but also retaliation for what was done), target hardening (e.g., self-defense lessons, being more cautious, installing alarm systems), avoiding social contacts (e.g., not leaving the home, moving to a new house, changing telephone number), seeking help from others (e.g., medical assistance, emotional support, assistance with physical tasks), and seeking help from the criminal justice system (Frieze et al., 1987).

Button et al. (2014a) reported changes in victims' behavior in a study of fraud. These included being more cautious when taking financial decisions, credit card usage and Internet purchases, and being less trusting of others. It also led to positive changes towards the threat because victims became more security aware and attentive to fraud prevention. Regarding behavioral coping, two effective strategies found in a study on identity theft by Sharp et al. (2003) were taking actions to resolve the issue and talking to family and friends. The latter was found to be an effective means of coping for victims of other types of offline crime as well (DeValve, 2005; Frieze et al., 1987; Lamet & Wittebrood, 2009). Frieze et al. (1987) argued that social support is effective in protecting victims from different pathological states, making it a vital aspect of successful coping. The extent to which online banking fraud victims use this and other coping strategies – as well as the effects and impact they have experienced – are inventoried by means of interviews, which are presented next.

METHOD

Semi-structured interviews were chosen as the research method to study the effects and impact of, and coping responses to, online banking fraud victimization. A topic list was developed based on a literature review. Although we tackled all of the topics in the interviews, the structure was modified in each interview to best fit the experience of the participant. The interviews were conducted face-to-face at a location decided by the interview participant. This was either at their home or at their working location.

Our aim was to identify the effects and impact of online banking fraud incidents and coping responses after the incident. The questions were newly developed for this study and included: What is your experience with online banking? What effects did the incident have on you? Did the incident result in emotional harm? Do you recall the amount that was stolen? Did your bank reimburse the financial damage? Have you taken new or additional precautionary measures since the incident? Furthermore, demographic characteristics of the participants were registered. During the interviews, participants were also asked about how the incident had unfolded, possible reasons for being targeted, and what protective measures they had in place. Outcomes of these particular questions are described in the work of Jansen and Leukfeldt (2016). The interviews lasted 52 minutes on average and were recorded using a digital voice recorder.

The participants were selected based on police reports and were contacted by a liaison officer working for the Dutch police to inform them about the study and to obtain their consent for voluntary participation in an anonymized interview. Of the 65 police reports selected from the Northern and Southern regions of the Netherlands, 29 participants agreed to be interviewed, nine declined the request, and 11 were not reached. Possible participants in the remaining 16 cases were not contacted because we obtained sufficient data to complete our study. One participant was recruited via a liaison officer at the Fraud Helpdesk, bringing the total number of participants to 30. The Fraud Helpdesk is a national organization for answering questions and collecting reports about fraud. The participants were interviewed between October 2014 and April 2015. The participants that were recruited based on police files were victimized in the year prior to the interview. The participant that was recruited via

the Fraud Helpdesk was victimized three years prior to the interview. In this study, participants were defined as victims when they actively or passively gave away their user credentials because of phishing or malware attacks. In addition, the reports were not made available to the researchers by these organizations, making it impossible to triangulate the data.

The ages of participants ranged from 23 to 89 years (M = 59, SD = 17). Thirteen women and 17 men were interviewed for this study. The distribution of their educational level – based on the grouping of Statistics Netherlands – was low (n = 3), medium (n = 15) and high (n = 12). The majority of participants were experienced users of online banking having used it for five years or more (n = 23) and using it at least once a week (n = 21). Their bank accounts were held at different banks in the Netherlands. In total, 17 phishing victims and 13 malware victims were interviewed – the cybercrimes of interest in this study.

The victim sample included private as well as corporate customers. For phishing, the distribution was 16 to 1. For malware, the distribution was 1 to 12. The corporate customers were primarily self-employed entrepreneurs and small and medium-sized enterprises. Two of the malware participants were not the actual victims. Instead, we spoke with the partner of a victim and a supervisor of an employee who was victimized. We decided to include their input in the analysis because their stories contained relevant information, such as the financial impact and changes due to the incident.

After the interviews were conducted, the recordings were transcribed and sorted into conceptual themes that we defined prior to the study. These were based on the research and interview questions, derived from general theoretical concepts, and include, for example, effects and impact. The interview data were analyzed using QualiCoder (Version 0.5), a type of computer-assisted qualitative data analysis software. Using this tool, we labeled the written information with analytical codes, which gave us the opportunity to separate the themes into more detailed categories (Ritchie, Lewis, McNaughton-Nicholls, & Ormston, 2014), such as psychological and emotional effects. Thereafter, the content within these categories was gradually specified into codes, including, feeling awful, stupid, and disbelief. Finally, the output was manually recorded in a Microsoft Excel file (which can be requested from the authors). A short summary of the interviews is provided in Table 1 of the Appendix.

RESULTS

In the following sections, we present damage amounts (rounded up to hundreds of euros) and incidence of particular views or experiences of participants. We do not claim that we are providing a representative reflection of online banking fraud incidents. That is not possible using this interview method nor was it the objective of our study. Rather, the study aims to provide insight into how coping phenomena vary among participants. Where possible, we make a distinction between the phishing and malware cases. Differences between phishing and malware are mentioned only when certain outcomes were reported for either one of the two fraudulent schemes. If only one participant mentioned a certain outcome, the response is not quantified, i.e., no “n” is indicated. Before we continue with the results, we provide a summary of a phishing and a malware case, because these give a good impression of what the interview participants have experienced.

Phishing attack – A participant received a deceptive e-mail containing a message to execute a security update for online banking. She clicked on the hyperlink that was included in the e-mail, which redirected her to a false website where she entered some personal details.

About two weeks later, she received a fraudulent phone call. During the telephone conversation, she followed the instructions of the caller and passed on user credentials by which the fraudster used to log in and make illegitimate bank transfers.

Malware attack – A participant noticed at some point that the online banking screen "shook" briefly when being used (interview 30). At a later date, the participant wanted to transfer money to the Dutch Tax and Customs Administration. However, in the background, the transfer was split into two transfers (adding up to the same amount), of which the largest amount was sent to an unknown account and a smaller amount to the administration service. During the execution of that particular money transfer, the participant noticed nothing out of the ordinary. The split-up money transfer was not visible in the payment summary screen when using the compromised device. Based on an investigation carried out by the Dutch police, we know that the malware was automatically installed on that particular device when visiting an infected website (Leukfeldt, Kleemans, & Stol, 2016).

Financial impact

Fifteen out of 17 phishing victims reported that the incident caused financial damage. The total damage that these 15 reported was 181,300 euros (M = 12,100; Min. = 900; Max. = 50,000). Seven of them were fully reimbursed by their bank. Three were fully reimbursed less a mandatory own risk excess of 150 euros, which one of the participants called a "fine" (interview 18). One participant received 1,000 euros from her bank, which was less than a third of the total damage of 3,600 euros. Four participants received no financial compensation, leaving a total damage of 58,700 euros. Two of the 17 participants reported no financial damage, as their banks were able to immediately stop the fraudulent transfer. The amounts that the fraudsters were attempting to steal were 2,000 and "over 10,000" euros.

We asked the participants who were not fully reimbursed about their opinion of this. The participant (interview 6) who got back 1,000 of 3,600 euros mentioned that, according to her emotional response, this amount was not proportionate. However, she thought that it may have been the maximum amount that could be refunded. In addition, she found the whole experience "a terrifying adventure," and so she made no further attempts to reclaim more money. "I was restless, frightened, tense. Maybe I should have stood up for myself?" Rationally, however, the participant stated that she understood why she was not fully compensated. "Not intentionally, but unintentionally, I was as stupid or as trusting as one could be." Because of the incident she had to cut her spending by not going on holiday for instance.

The participants who were not compensated at all expressed different views. Three of them respected the fact that they did not receive any compensation, stating that it was their own fault. One of them mentioned, "I did it to myself. So be it. I cannot turn things back. It is just silly, silly, silly" (interview 12). The second participant said, "It is the same as when you drive though a red traffic light. Then you get fined; it is your own fault. And that is also true in this case" (interview 13). She tried to minimize the impact by stating that, "It could have been more [money]." The third participant stated that he understood that he made the error, although he thought that the bank could have done more to trace the suspects.

The fourth participant (interview 15) who received no compensation was "very sorry" that she was not compensated, especially since "banks are so big." She felt that, because of the compulsory nature of online banking – "in particular for elderly people" – the bank could have shown more goodwill, also given the many years that she had been a customer of that

particular bank. However, her rationale was that the bank could not compensate her "because there are perhaps too many [phishing] cases." She also mentioned to have lost her security, i.e., having a monetary buffer, which affected her significantly. When talking about it with her husband, the impact was minimized for her because he made clear to her that they were still able to eat.

Twelve of the 13 malware victims reported that the incident caused financial damage. One participant did not mention the amount that was stolen. The other 11 participants reported a total damage of 52,800 euros (M = 4,800; Min. = 1,000; Max. = 10,000). All 12 participants were fully reimbursed by their bank. However, one participant claimed to have lost out on interest during the time that his money was not in his bank account. In one of the 13 cases, there was no financial damage because the bank was able to block the fraudulent transfer immediately. The participant explained that the amount that the fraudsters were attempting to steal was about a monthly wage.

Psychological and emotional impact

Most participants reported that the event had at least some psychological and/or emotional impact on them. However, four participants expressed no psychological or emotional impact. The supervisor of a malware victim stated, "It is all in the game. It is part of life, running those risks. […] And, besides, it is only money. If physical violence was involved, then it would have real impact" (interview 28). Three of these four participants indicated that they would probably have assessed the impact differently if they had not been compensated by their bank.

Eleven participants reported that the incident did have an impact, but that it was low. A malware victim mentioned that, "It is an administrative thing" (interview 21). Although he still felt "screwed," he did not worry about it, because he knew that the money would be back within a week. Another malware victim said, "You have a strange feeling, but nothing more. The intangible makes it difficult. With burglary, you see that things are broken and ransacked" (interview 23). Three phishing victims said that, although they did not experience any psychological or emotional impact or only to a small degree, they were annoyed by it.

Some participants compared online banking fraud with burglary (n = 2), while others believed that a comparison with burglary is not possible (n = 5). On the one hand, a phishing victim stated, "Strange people just enter your private life, and that is the most disgusting part of it. It does not matter if it is on your computer with money, or that people steal your belongings or are only sniffing around and turn things upside down. It just gets to you" (interview 2). On the other hand, the spouse of a malware victim indicated, "Hacking into your computer is a totally different experience. Burglary at home is a violation of your privacy. In this case, it is a technical thing" (interview 25).

Participants who experienced psychological and/or emotional effects said that, in general, they felt awful (n = 8), disbelief (n = 8), fear or shocked (n = 6), stressed or nervous (n = 6), cheated (n = 4), and insecure (n = 3). It also lowered their trust in banks and/or online banking (n = 8). Being misunderstood was an effect mentioned only by malware victims (n = 2). Effects that only phishing victims stated included feeling stupid (n = 8), shame or embarrassment (n = 5), angry (n = 2), devastated (n = 2), sadness, and feelings that things are deprived. Phishing victims also stated that the incident lowered their levels of trust in themselves (n = 3) and in people in general (n = 2). A participant pointed out that, "If you lose your trust, you lose more than your trust, you lose your certainties. […] I trust all people to be

honest and open. That trust has been given a big blow. When I say that I could cry again, since I find it that terrible. I still suffer from it" (interview 12).

Furthermore, phishing victims mentioned that the incident made them feel less safe online (n = 4) and offline. The participant who claimed feeling unsafe both online and offline said that these feelings were linked to a previous life event in which she was cheated. "Those feelings came back through this phishing incident. It really knocked me off balance. It certainly took a month. I was just really scared" (interview 6). She reported that the incident also affected her sense of safety in her home. She asked herself whether the criminals who had scammed her might have obtained her physical address. She indicated having had sleepless nights, wondering whether people would sneak into her home. "You don't know how far it may reach."

Other phishing victims also mentioned having suffered from physical effects. One participant (interview 17) spoke about having "a trauma" and indicated also having suffered from sleepless nights. "This was less about the money aspect, but more about the stupidity." The participant blamed himself that he fell for the scam. "You lose your self-confidence, because you can be so stupid." Contrary to this statement, four participants stated that the incident was something that befell them. A malware victim indicated that, "You must make sure that you don't blame yourself. You don't have control over it" (interview 30).

One of the phishing victims indicated that, "Its aftereffects are very bad. It has had a lot of impact and still makes me feel very sick" (interview 12). One aftereffect that she mentioned was that she experiences black outs from time to time. Another phishing victim claimed that she almost collapsed when the incident happened. She claimed having had heart palpitations when the bank e-mailed her with the message that she would not be compensated for her financial losses. She felt terrible and could not believe it. During the process of getting her money back, she became very insecure. "When I was using online banking for the first time after the incident, I was shaking all over" (interview 1). She reported being very anxious, mostly because she no longer felt in control. Furthermore, it influenced the work she was doing for a foundation. At the time of the interview, she was the treasurer of that particular foundation, but because of the incident she found it terrifying and wanted to resign from that role. "The idea that this [a successful phishing attack] would happen to me with other people's money makes me feel sick." Finally, a malware victim indicated that he was shivery using online banking after the incident, but that this feeling was subsiding as time passed.

The duration or timeframe of the effects was also mentioned in some of the other interviews. In total, four phishing victims stated that the effects were still (partly) present. For example, participants indicated that, although the incident had happened a while ago, feelings of uncertainty or distrust, especially with regard to digital payments, still existed. One participant claimed that she was trying to get over it, which she was confident about, as "time heals all wounds" (interview 6).

Seven participants reported that the impact goes away or at least goes into the background. A phishing victim reported that the impact lasted for two or three days. When things were back in order, she turned the page. Another phishing victim reported that feelings of shame and stupidity had subsided over time, but that it was not one of his favorite topics of conversation. "I don't talk about this topic at parties. It was quite an impactful experience" (interview 3). Two others also indicated not sharing the experience. However, some did (occasionally) talk about the incident within their social sphere (n = 13). Most did this for coping purposes, but five of them also did so to warn people about such schemes. In two out

of 13 cases, participants mentioned that the people they told about their experience tried to help them to get their money back and to locate the people responsible for the scam. Another participant indicated that the positive aspect was that her fellow residents from the elderly home and her family supported her really well, which helped her to cope with the incident.

Secondary impact

Some of the participants reported that the negative event also had secondary impact. This was often related to the handling of the incident. Obvious secondary effects were time loss due to reporting the incident to both the bank and the police, a blocked bank account and, consequently, not being able to having direct access to their own money. A malware victim indicated that the time between the incident and reimbursement of the bank was bothersome. "As a self-employed entrepreneur, you don't feel like spending hours on phone calls with your bank during the day" (interview 9). One phishing victim explained, "Especially as you get older, you don't want to be bothered by such things" (interview 4). Although this section mainly deals with negative experiences, nine participants explicitly indicated adequate levels of expertise among staff at the bank and/or the police, and mentioned that they took it seriously and were understanding and helpful. One of them argued that this attitude was very reassuring.

Other types of secondary impacts that were mentioned by participants from both fraudulent schemes included feeling mistreated (n = 6), bad communication (n = 4), and an uncooperative attitude (n = 3) on the part of banks. A phishing victim felt mistreated by her bank when reporting the incident. She got the impression that the bank employee sitting across her was thinking, "'Oh, you are so stupid.' He made that very clear" (interview 1). Participants also felt that they were being treated like the guilty one, or felt as though they needed to prove their innocence.

All of the participants went to the police to file a report. In 19 cases, participants were obliged or advised to do so by their bank. Eight reported having done so on their own initiative. Of the remaining three cases, we do not know what motivated them. Secondary impact related to the police were reported as follows: The police initially did not want to (or did not have time to) file the report (n = 5), have to wait for a few days until it was possible to file a report (n = 3), have to drive far to a police station, and a lack of expertise that was displayed by the particular police officer. The participant of the latter case – a malware victim – stated, "The person who filed the report did not understand any of it. You cannot blame that person for not knowing everything, but the police can significantly improve in this regard" (interview 21).

Two phishing victims mentioned that they received many payment reminders during the time their bank account was blocked, which they found annoying. Two malware victims claimed having to settle things because of the fraudulent transfer. One of them needed to settle things with the Dutch Tax and Customs Administration, because the participant's business received a formal warning. She had to rectify things by reporting that the late payment was unintentional, that it was due to a fraudulent attack. The other participant needed to settle things similarly with a do-it-yourself store.

Finally, five participants indicated that either the police or their bank updated them about the incident. In two instances, updates included a standard message that there were not enough leads to continue working on the case. In one instance, a malware victim mentioned being updated on the case by a police detective. This had a positive effect on the level of trust

that something was actually being done. Some of the participants that indicated that no updates made them feel that they were being left in the dark or gave them the impression that nothing was done about their case.

Behavioral change

We asked participants whether they had changed their behavior due to the incident in order to cope with the incident or to prevent future incidents. We have categorized behavioral change into three categories: 1) behavioral change related to devices used for online banking; 2) behavioral change related to online banking sessions; and 3) behavioral change beyond the online banking context. It is important to note that we have relied on self-reported behavioral change. We have no additional data that provides support for what the participants told us.

Behavioral change and devices. Seven participants told us that they had installed an additional anti-virus or anti-malware package, such as Malwarebytes and TDSSKiller. Four participants reported having changed their anti-virus software, of which one indicated that the device had no anti-virus software during the time of the incident. Another participant switched from a free package to a paid package, in order to prove to the bank that he is doing a good job. Three participants said that they updated their software more frequently. A phishing victim reported that her computer now updates every night and that she manually checks for updates once a week. This was not only due to the incident, she received messages from her bank stating that financial losses caused by phishing will not be reimbursed if software is out of date.

Other changes that were mentioned more than once were no longer using the device that was used during the incident (n = 2) and buying a new computer (n = 2). The latter was only reported by malware victims. One of them claimed that the police advised her to buy a new computer. This additionally led to the IT staff needing to reinstall all the (business) software. She indicated, “We have no insurance for that” (interview 30). Changes that were mentioned once included using a different web browser, switching from a Windows desktop to an Apple iPad (which was perceived to be safer), and replacing the hard drive of the compromised device with a new one.

Behavioral change and online banking. More than half of the participants indicated that they had become (extra) alert or more aware of phishing and malware attacks (n = 17). Participants also indicated that the incident was a good learning experience (n = 14). In addition, participants had changed their online banking practices. Both phishing and malware victims mentioned being more careful/meticulous or taking more time to properly check what they were doing during online banking and online purchases (n = 8), checking the account balance more regularly (n = 7), and checking the security certificate (n = 7, e.g., https, closed padlock).

Changes that were reported only by phishing victims include logging out of banking sessions instead of clicking away the window (n = 3), checking the web address (n = 2), using online banking less and traditional banking methods more when transferring money (n = 2), and not using online banking at home anymore. In this particular case, the participant visited a local bank once a month to conduct his banking activities. If he was not sure about something, he could ask a bank employee to help him.

A new online banking practice that only malware victims mentioned was taking screen shots of their online banking activities (n = 2). One of them indicated doing this, “To be able

to prove that you are doing the right thing" (interview 23). After about a year, both participants stopped doing this. Another participant explained that when she had to transfer large amounts of money, she would contact the bank by phone to find out if everything was in order. She attributed this to her insecurity that was caused by the incident. However, she soon stopped with this procedure because it was not practical.

Besides the duration of the new behaviors explained above, the timeframe of the new behavior was also mentioned in a few other cases. Three malware victims claimed that being extra alert or more careful was already waning. Two phishing victims who stated that they checked to see if there was a closed padlock revealed that they did this less frequently now or not at all during the time of the study. Finally, a phishing victim disclosed that she no longer checked the account balance regularly.

Behavioral change beyond online banking context. One frequently mentioned change in the behavior of phishing victims beyond the online banking context was that they became more suspicious about e-mails (n = 8); for example, not clicking on hyperlinks and checking whether e-mails are trustworthy. One also commented that it had become difficult to differentiate between legitimate and false e-mail messages. Other phishing victims indicated deleting all e-mails that were or seemed to be sent by banks (n = 4). Two also commented that if the message was important, the bank would have sent a letter.

Six phishing victims made changes to their bank accounts. Changes included removing the credit limit from the account (for overdraft protection), configuring the debit card so that it could not be used abroad; receiving a different bank account number from the bank (because fraudsters carried out new phishing attempts); closing a savings account (because that particular account was protected by a password only, which seemed to be unsecure); opening a savings account at another bank (since the checking and savings accounts had the same numbers, which was perceived to be unsafe); and opening several bank accounts (where specific amounts of money can be deposited, leaving only a smaller amount in the checking account). In this particular case, the participant commented, "In this way, third parties cannot get to the big money" (interview 16).

Four phishing victims said that they are more on guard when using mobile phones and receiving telephone calls. Three of them suggested that if the phone's display did not show a number, they picked up the phone without stating their name or they did not answer it at all. The other participant obtained a new phone number. Furthermore, two participants intended to leave their bank, but did not follow through.

Changes that were mentioned just once by phishing victims included not buying or signing anything anymore at the door, not writing down the PIN code in an agenda or on a piece of paper, not giving out their bank account number as readily as before, and not going on the computer when feeling sad (for this participant, safety was embedded in sadness). A participant who was phished while being the treasurer of a foundation indicated that the foundation had invested in making its website more secure.

Two malware victims commented that they had made changes beyond the online banking context. One of them indicated that business procedures and protocols were carefully reexamined in order to make sure that incidents would be adequately prevented or detected as soon as possible. Another indicated not sending information from business computers to the main business computer (used for online banking), i.e., not running any unnecessary risks.

DISCUSSION

Although we believe that our study provides a unique contribution to literature, it has its limitations. First, the results are not generalizable for all online fraud victims. We focused on victims who suffered from online banking fraud only. Furthermore, the participants were selected from police files. Therefore, we do not know what the effects are on victims who did not report the crime or how they cope with such events. Reasons for non-reporting include, for example, not knowing that they had been defrauded, feeling partly responsible, feeling embarrassed, and suffering low financial losses (Button, Lewis, & Tapley, 2009b). This limits generalizability as does low reporting rates.

For example, in 2015, 2% of all hacking cases, 20% of marketplace fraud cases, and 13% of identity fraud cases that Dutch people experienced were officially reported to the police (CBS, 2016). Perhaps in-depth interviews with respondents that follow a crime survey could be a way to address this limitation. Moreover, some potential participants declined the request to be interviewed. Perhaps these victims did not participate because they perceived higher or more problematic psychological and emotional impact than those in the sample. Another possibility is that these victims were not affected at all and therefore had no interest in participating. What becomes clear though is that victims vary in their characteristics and profiles. This concurs with previous research on fraud victimization (Button, Lewis, & Tapley, 2009a; Button et al., 2009b; Cross et al., 2016).

A possible limitation is related to the identification of psychological and emotional effects. Although we found that the participants talked openly about these and other subjects, the participants may have hidden some of these effects from the researchers because they felt too embarrassed about them. Dignan (2005) stressed that it is very difficult to measure such effects because the willingness and ability of people to talk about these issues, as well as about the experience itself, are highly subjective and partly cultural specific. This also counts for coping efforts because people are not always aware of what they are doing exactly (Lazarus & Folkman, 1984). The subjective nature of this study may therefore have led to the problem of method variance. However, Lazarus and Folkman (1984) nuanced the problems of validation by stating that subjective reports allow researchers to learn more about coping than any other single source. In order to make outcomes more comparable, regardless of their subjective nature, we recommend using other specific assessment tools in future studies; for instance, the “ways of coping” checklist (see Lazarus and Folkman [1984]). However, this would require a more quantitative research approach.

Finally, the current study adopts a retrospective approach, which has its limitations (Shapland & Hall, 2007). Participants may have forgotten certain details about the effects of online banking fraud and how they cope or coped with these. We have gained an impression of the short-term consequences, but we do not explicitly understand how victims’ coping strategies play out in the long term. For example, some participants mentioned that they were already using some behavioral coping measures less frequently. It would be interesting to find out whether individuals are consistent or variable in their coping strategies, and what their overall coping style is, as opposed to our more contextual focus on coping efforts (Lazarus & Folkman, 1984). Indeed, coping is not a one-off activity. Future studies could benefit from a longitudinal approach. Studying the effects and impact that victims perceive and their cognitive and behavioral responses at multiple points in time provide richer data with more potential. For instance, to understand how perceived effects develop and to better guide a victim through the coping process. Further research may also benefit from investigation of personal, psychological, and contextual factors that affect coping efforts.

The first research question we wanted to answer is: What are the financial, psychological and emotional effects of online banking fraud victimization? We start with the financial effects. Most participants experienced some financial damage – at least initially – from either phishing or malware victimization. Two thirds of the phishing victims and all malware victims whose bank accounts were affected were fully compensated for their financial losses. The fact that all malware victims were fully compensated probably has more to do with the type of the offense – that is the obscureness of the malware attack – than with the observation that most were corporate customers. Imaginably, the circumstances surrounding malware victimization appeal to the "ideal victim" typology.

Five participants – all phishing victims – were not or were to a minor extent compensated for their losses. Although the participants who suffered financial losses acknowledged that being victimized was to some extent due to their own wrongdoing, some expected more goodwill from their bank regarding compensation. Moreover, it would be interesting to investigate the banks' reimbursement policies on this matter: Why are some phishing victims compensated, be it in full or not, while others are not?

Besides the direct financial effects, indirect financial effects were also reported. These effects included loss of interest, buying a new device for online banking, and several types of loss of time that can be considered to have a monetary value, such as devoting more time to taking precautions (online) and going to a physical bank office to use banking services. Thus, the financial effects go further than only the (initial) damages caused by the fraudulent schemes.

We will now turn to the psychological and emotional effects. The participants that indicated that the event affected them psychologically and emotionally mentioned a range of effects, such as feeling awful, stupid, stressed, disbelief, and fear. It also affected their levels of trust, including trust in banks and/or online banking, people, and themselves. That such psychological and emotional effects follow victimization is consistent with other research on (online) fraud (Button et al., 2009a; Cross et al., 2016). Some participants even reported physical effects, such as having sleepless nights, getting heart palpitations, experiencing blackouts, and feeling shivery or shaky when using online banking.

We also found some evidence regarding the duration of the effects (Frieze et al., 1987). Most participants claimed that they had immediate reactions to the incident. The psychological and emotional effects were often at their most severe during this particular timeframe. Some of the participants indicated that the effects subsided after a few days. However, some reported that the effects or impact experienced lasted from about a month to still being present at the time of the interview. This is a similar pattern that is observed for (offline) violent crimes (Dignan, 2005), as well as for different types of online fraud (Cross et al., 2016).

The second research question was: To what extent do online banking fraud victims suffer from secondary victimization? Secondary victimization relates to negative effects other than those instigated by the incident itself. Negative effects often related to the way the incident was handled, such as time loss due to reporting the incident, not being able to access the bank account, and feeling mistreated. Feeling mistreated has a negative influence on coping because it does not address the victims' need for recognition.

In addition, most participants mentioned that they did not receive feedback from either the bank or the police on the incident and how it was being handled. Frieze et al. (1987)

argued that such information helps victims to relieve their fear and frustration, thus helping them in the coping process. In addition, victims may develop a positive attitude towards banks and the police instead of losing their trust and confidence in these organizations. The study of Button et al. (2009b) also found that fraud victims have a need for being held up-to-date on the process of the case. We believe that providing feedback, not only on the status but also on how the incident happened, can help victims to develop more effective defense strategies against future attacks.

Besides negative effects, some participants explicitly reported positive aspects in how their cases were handled. They mentioned that bank employees and police officers took them seriously, were understanding and helpful, and had adequate levels of expertise for the situation. Again, banks and the police stand to gain a lot if they respond in this way, not only reputation-wise, but also when it comes to helping victims to recover properly from online banking fraud victimization.

The third research question was: What impact does online banking fraud have on its victims? Although the financial *effects* of online banking fraud could objectively be defined as quite severe, the participants did not claim that the incident had a devastating financial *impact*, which is sometimes the case for other fraud victims (Button et al., 2014a). Therefore, we conclude that the direct financial impact of online banking fraud victims is low, most notably because the majority of victims were compensated for their losses. This differs from other types of fraud, where it is often more difficult or even unlikely to get restituted (Button et al., 2009b). Remarkably, some of the participants who were not compensated at all also felt that the impact was low. Three participants had no financial damage to begin with.

Regarding the psychological and emotional aspects, four participants said they felt no such impact. This was also mainly due to the fact that they were financially compensated for their losses, but also because online banking fraud was considered a technical or invisible phenomenon. These participants felt that their private lives had not been affected. About a third of the participants mentioned that the *impact* of the fraudulent attack was low, but did express some psychological and emotional *effects*.

Half of the respondents were – to some extent – overwhelmed by the situation. Thus, reimbursement could not prevent some of the participants from being psychologically or emotionally affected by the incident. Furthermore, we found some evidence that previous negative life events affected the impact of victimization. Our topic list, however, did not include questions about such events or prior victimization, which could be beneficial to add in future studies. Similarly, questions could be asked whether or not other accounts beyond banking were hacked, which may also have affected the impact experienced by participants.

The final research question was formulated as follows: What are the cognitive and behavioral coping responses to online banking fraud victimization? Regarding the participants who were not compensated or not fully compensated for their financial losses, we observed that they used a cognitive coping style of rationalizing it, thereby minimizing their victimization. They came up with an explanation that seemed to fit the situation in order to cope with the fact that they had lost their money.

Cognitive coping strategies were also observed regarding the psychological and emotional effects of becoming an online banking fraud victim. Examples include being at ease with the situation because reimbursement procedures were understood, and viewing an incident as being something that is part of life. Some participants tried to create a

"hypothetical, worse world" scenario in order to cope with victimization (Taylor, Wood, & Lichtman, 1983), for example, by thinking that the stolen amount could have been higher or that it would have been worse if it had involved physical violence. These strategies are effective for reducing emotional distress, but ineffective for tackling the actual problem.

Another cognitive coping response is that victims feel strengthened by the experience. Some indicated that the experience was a good lesson in that it made them wiser, which is also considered to be positive change in other studies (Button et al., 2014a; Whitty & Buchanan, 2016). Perhaps confronting online banking users with (controlled) phishing and malware attacks would be a good strategy as a way to teach them how to prevent such attacks.

A strategy that makes coping difficult was observed in a participant who blamed himself for being victimized (Whitty & Buchanan, 2016). Although self-blame can be considered a maladaptive response, which could for instance lead to hopelessness and depression, it can also be considered an adaptive response if self-blame is considered to be behavioral. If victims are able to link their own actions to victimization, they can avoid future victimization by adjusting these actions. On the other hand, if victimization is linked to character, it gives victims less confidence in their perceptions of avoiding future victimization because personality is hard to change (Frieze et al., 1987).

Some participants reported an opposite strategy towards self-blame, indicating that the incident was something that befell them, which helped them control their emotional state. In our opinion, this is not a strange – and perhaps the right – reaction, as the skills of fraudsters are often the reason why people fall for such scams. Individuals that are victimized are not stupid; they simply made a choice that was not a good one. For malware victims, it was out of their hands because their systems were infected automatically.[i] For these victims, the cases remained unsolved; they do not know how their systems were infected, nor how the fraudulent transfer(s) took place. They were surfing online in the wrong place at the wrong time. In general, this did not cause any distress, most probably because all were reimbursed – which might have strengthened their belief that they could not help it.

Respondents also applied behavioral coping mechanisms. The first behavioral coping mechanisms that they applied was reporting the incident to, and seeking support from, their bank. In addition, all participants filed a report with the police (which is logical given our selection procedure), either because the bank required them to or on their own initiative.

Some participants also sought support from their social environment, which was assessed as an effective means of coping. This is also identified in the literature as one of the most effective means for successful coping (Frieze et al., 1987). One of the participants mentioned after the interview that the conversation had a healing effect on her as she had not talked about it much. According to her, banks should provide aftercare in the form of having a conversation about the event after some time, helping victims to process it. Were banks to follow up on these incidents, it is essential that the person instigating the conversation adopts a supportive attitude, i.e., be unprejudiced, show empathy and understanding – not blame the victim, as the situation itself is difficult enough.

However, it can remain a difficult topic to address for some time. Perhaps these participants are assuming that others might find them stupid or that they would be angry with them because of the financial loss. Indeed, according to Cross (2015), there is a negative vibe surrounding online fraud victimization, although she found that phishing is a more acceptable type of fraud victimization, than, for instance, advance fee fraud and romance fraud. Whitty

and Buchanan (2016) argued that negative or non-supportive responses from the social environment can be harmful for recovery. We found no evidence that online banking fraud victimization affected social relationships, nor did we find any leads indicating indirect victimization by people within the victims' social environment. Perhaps this is the case, because the research participants were open to share these experiences with the people closest to them. Other fraud research has shown that when such events, for example, are kept secret, the impact on partners and family members can be more severe (Button et al., 2014a).

We also identified environmental strategies and strategies directed at the victims themselves. Environmental strategies included installing a different or additional anti-virus package and (more regularly) checking for software updates. A frequently mentioned strategy that was directed at the victims themselves was that participants became more alert to or aware of phishing and malware. Being more cautious after victimization is also found in the fraud studies of Button et al. (2009a; 2014a) and Cross et al. (2016). Online banking processes were also adjusted, such as being more meticulous or taking more time to check things, checking the security certificate, and checking the account balance more regularly. Furthermore, we observed that some participants adopted avoidance behavior, i.e., using (or wanting to use) online banking less and using traditional banking services more.

Some of the abovementioned strategies can be considered to be problem-focused coping as they are intended to prevent an online banking fraud incident from happening again. However, these strategies could also be adopted as a means to control emotions, for example, making them feel more confident about online banking. It is therefore difficult to determine whether certain responses belong to problem-focused and/or emotion-focused coping strategies (Lazarus & Folkman, 1984), so we have not labeled them as such. Follow-up research is required to clarify in greater detail how these strategies work.

Finally, we found that participants also performed behavioral coping strategies beyond the online banking context. One frequently mentioned example was that phishing victims reported being more concerned about or suspicious of e-mails. As a consequence, participants indicated that it was often difficult to differentiate between legitimate and false e-mail messages. This was also observed by Wang, Chen, Herath, and Rao (2009), who noted that phishing has a high impact on legitimate commercial e-mails. Other responses that phishing victims mentioned more than once included making changes or restrictions regarding bank accounts and being more on guard when taking telephone calls.

CONCLUSION

We agree with Button et al. (2014a) that, similar to other types of fraud, online banking fraud cannot be considered a *victimless* crime, not even when the stolen money is reimbursed (see also Whitty & Buchanan, 2016). The effects and impact of such fraudulent schemes on victims should not be underestimated. Regardless of the financial costs associated with online banking fraud, losing trust (e.g., in online commerce and people in general), and declining levels of safety and security are a much higher price to pay. However, the extent to which an individual perceives these effects and impact differs significantly. For some it was a temporary inconvenience only and they managed to get over it, whereas for the other it was (and sometimes still is) an overwhelming experience that changed them; they became more attentive, alert, and distrustful as a result. This means that individual differences should be acknowledged when helping victims to cope with their victimization. Hence, for help to be effective, one should take into account the interplay between personal characteristics and the environment (Lazarus & Folkman, 1984). They went on to state that effective help can only

be achieved if a process-oriented view is adopted. This would involve examining what happened and what is happening to that particular individual in terms of coping.

This conclusion has implications for banks and law enforcement agencies. Banks primarily have to deal with the incident and the damage resulting from the incident. Banks could probably improve their services by recruiting dedicated personnel who devote attention to the victims' coping process, employees who are able to assess how the victims' coping process is unfolding and who can support these victims in that process. These employees could have contact with the victim at multiple points in time depending on the specific needs of the victim. This may require a different set of skills than those that bank employees at fraud departments currently have.

Another strategy might be to cooperate with "victim support," a service that is provided to victims when they report a crime to the Dutch police. Another important implication for law enforcement agencies is that victims should be treated seriously as the impact they experience goes further than the money aspect only. It is crucial to do this right the first time victims come into contact with these agencies to report the incident because this might set the tone for the whole handling procedure. Moreover, as pointed out by Cross et al. (2016), a negative reporting experience can worsen the harm that victims already undergo. To evaluate whether this is done adequately, and to continually improve the support of victims, it is recommendable to map the customer experience in terms of fraud handling, which is already done by different banks in the Netherlands (personal communication, April 26, 2017).

Conclusively, we have contributed to the literature by increasing insight into the effects and impact of phishing and malware attacks and enhancing the understanding of adaption after online banking fraud victimization. These aspects are currently lacking in studies on cybercrime. More thorough analysis of coping strategies is required to deepen insight into the phenomena described in our study. This is not only needed to advance theoretical knowledge on this topic, but also to further shape the supporting role that banks and law enforcement agencies have, as presented in the recommendations above. We need more information about the factors that cause stress, how coping strategies are chosen, which strategies are effective and which are not, and how these function over time. Some coping efforts seem to work for awhile, but subside over time as they seem to hinder usability, cost too much time, and some perhaps do not work at all.

Acknowledgements

This study is part of the Dutch Research Program on Safety and Security of Online Banking.

This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy, and the Dutch National Police. We would like to thank the participants for telling their stories and our liaison officers at the Dutch National Police and Fraud Helpdesk for establishing the first contact with the interview participants.

REFERENCES

Beaudry, A. & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29*(3), 493–524.

Bossler, A.M. & Holt, T.J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Button, M., Lewis, C. & Tapley, J. (2009a). *A better deal for fraud victims: Research into victims' needs and experiences.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2009b). *Fraud typologies and the victims of fraud: Literature review.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2014a). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *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. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408.

CBS (2016). *Veiligheidsmonitor 2015 [Safety monitor 2015]*. The Hague: Statistics Netherlands.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187–204.

Cross, C., Richards, K. & Smith, R.G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice, 518,* 1–14.

Denkers, A.J. & Winkel, F.W. (1998). Crime victims' well-being and fear in a prospective and longitudinal study. *International Review of Victimology*, *5*(2), 141–162.

DeValve, E.Q. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. *Applied Psychology in Criminal Justice, 1*(2), 71–89.

Dignan, J. (2005). *Understanding victims and restorative justice*. Maidenhead: Open University Press.

Frieze, I.H., Hymer, S. & Greenberg, M.S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology: Research and Practice, 18*(4), 299.

Gale, J.-A. & Coupe, T. (2005). The behavioural, emotional and psychological effects of street robbery on victims. *International Review of Victimology*, *12*(1), 1–22.

Green, D.L., Choi, J.J. & Kane, M.N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment*, *20*(6), 732–743.

Hanslmaier, M. (2013). Crime, fear and subjective well-being: How victimization and street crime affect fear and life satisfaction. *European Journal of Criminology*, *10*(5), 515–533.

Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust*, Verona (Italy), pp. 24–31.

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Kirlappos, I. & Sasse, M.A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, *2*, 24–32.

Kunst, M.J.J. & van Dijk, J.J.M. (2009). *Slachtofferschap van fraude: Een explorerend onderzoek naar de impact van diverse vormen van financieel-economische criminaliteit [Fraud victimization: An exploratory study into the impact of diverse forms of financial crime]*. International Victimology Institute Tilburg (INTERVICT).

Lai, F., Li, D. & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363.

Lamet, W. & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers [Never the same again: The consequences of crime for victims]*. The Hague: Sociaal Cultureel Planbureau.

Lastdrager, E.E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1–10.

Lazarus, R.S. & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, 21–37.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90.

Maddux, J.E. & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Matthieu, M.M. & Ivanoff, A. (2006). Using stress, appraisal, and coping theories in clinical practice: Assessments of coping strategies after disasters. *Brief Treatment and Crisis Intervention*, *6*(4), 337.

ONS (2016). *Crime in England and Wales: Year ending Sept 2016*. London: Office for National Statistics.

Schoepfer, A. & Piquero, N.L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215.

Shapland, J. & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J. & Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Science*, *49*(1), 1–6.

Shover, N., Fox, G.L. & Mills, M. (1994). Long-term consequences of victimization by white-collar crime. *Justice Quarterly*, *11*(1), 75–98.

Taylor, S.E., Wood, J.V. & Lichtman, R.R. (1983). It could be worse: Selective evaluation as a response to victimization. *Journal of Social Issues*, *39*(2), 19–40.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127.

Wang, J., Chen, R., Herath, T. & Rao, H.R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems*, *48*(1), 92–102.

Wemmers, J.-A. (2013). Victims' experiences in the criminal justice system and their recovery from crime. *International Review of Victimology*, *19*(3), 221–233.

Whitty, M.T. & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims-both financial and non-financial. *Criminology and Criminal Justice*, *16*(2), 176–194.

Jurjen Jansen is a senior researcher at the Cybersafety Research Group of NHL Stenden University of Applied Sciences and the Dutch Police Academy. In 2018, he obtained his PhD in behavioural information security at the Open University of the Netherlands. His research interests include human aspects of information security, cybercrime, cognition and human-computer interaction.

Rutger Leukfeldt is senior researcher cybercrime and the cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Furthermore, Rutger is director ('lector') of the Cybersecurity & SMEs Research Group of the Hague University of Applied Sciences.

APPENDIX

Table 1: Short summary of the interviews

Interview	Gender	Age (years)	Level of education	Victim type	Fraud type	Damage (euros)	Reimbursed
01	Female	58	Medium	Private	Phishing	13,000	Yes
02	Female	79	Medium	Private	Phishing	2,000	Yes
03	Male	45	Medium	Private	Phishing	11,000	Yes
04	Male	89	High	Private	Phishing	2,000 (a)	N/a
05	Male	73	Medium	Private	Phishing	8,000	Yes
06	Female	59	High	Private	Phishing	3,600	1,000
07	Male	77	Low	Private	Phishing	10,000 (a)	N/a
08	Female	70	High	Private	Phishing	50,000	Yes
09	Male	36	Medium	Corporate	Malware	1,300	Yes
10	Male	68	Medium	Corporate	Phishing	900	Yes
11	Male	23	High	Private	Phishing	7,000	Yes
12	Female	74	Low	Private	Phishing	1,200	No
13	Female	73	Low	Private	Phishing	1,800	No
14	Male	80	High	Private	Phishing	4,800	Yes (-150)
15	Female	74	High	Private	Phishing	50,000	No
16	Male	67	Medium	Private	Phishing	2,500	Yes (-150)
17	Male	71	Medium	Private	Phishing	5,700	No
18	Female	61	High	Private	Phishing	20,000	Yes (-150)
19	Male	38	High	Corporate	Malware	M.w. (a)	N/a
20	Female	64	Medium	Corporate	Malware	6,900	Yes
21	Male	29	Medium	Corporate	Malware	10,00	Yes
22	Female	57	Medium	Corporate	Malware	5,000	Yes
23	Female	46	Medium	Corporate	Malware	4,700	Yes
24	Male	64	High	Corporate	Malware	3,000	Yes
25*	Female	56	High	Corporate	Malware	5,000	Yes
26	Male	31	Medium	Private	Malware	3,500	Yes
27	Male	30	Medium	Corporate	Malware	4,700	Yes
28*	Male	63	High	Corporate	Malware	5,000	Yes
29	Male	50	High	Corporate	Malware	3,700	Yes
30	Female	51	Medium	Corporate	Malware	N.t.	Yes

*Note. * = not the actual victim, a = attempt, m.w. = about a monthly wage, n.t. = not told, n/a = not applicable, -150 = minus mandatory own risk (i.e., 150 euros).*

[i] This articles includes both phishing and malware attacks, because they are basically two types of the same crime. Leukfeldt, Kleemans, and Stol (2017), for example, show that not only the goal of phishing and malware attacks is the same (i.e., to steal money from online bank accounts), but that the modus operandi of both attack types is quite similar too (intercepting login credentials, intercepting one time transaction authentication codes, wiring the money to money mule accounts and cashing the money). The biggest difference is that the malware victims in this study were not actively engaged in providing perpetrators their credentials. However, being fully responsible or not, it is still relevant to find out how the malware attacks affected participants and how they recovered from it. Furthermore, we had no information on how well the victims were protected against malware attacks before conducting the interviews. Personal responsibility could have been an issue when we had found that malware victims, for instance, had poor security protection installed. Moreover, in other malware cases, victims were more personally responsible, for example, by responding to a malicious pop-up window (see e.g., Jansen & Leukfeldt, 2015).