International Journal of Cyber Criminology
Vol 10 Issue 1 January – June 2016

Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization

Jurjen Jansen[1] **& Rutger Leukfeldt**[2]
Open University, NHL University of Applied Sciences, Police Academy, the Netherlands

Abstract

This paper explores factors that may explain online banking fraud victimization. The routine activity approach and protection motivation theory are used as theoretical lenses for this study. Based on 30 semi-structured interviews with phishing and malware victims, we found that suitable target factors from the routine activity approach have a marginal influence on victimization. About a third of the respondents were aware of the scam that they fell victim to prior to the incident. Most respondents had taken measures to protect themselves against online banking fraud. However, phishing victims were negligent and gave security codes to fraudsters. Several respondents reported having insufficient knowledge and skills regarding the safety and security of online banking and finding it difficult to assess to what extent protective measures help them to safeguard against fraudulent attacks. The results suggest, in line with the literature, that everyone is susceptible to some degree to online banking fraud victimization. From a customer perspective, both awareness of fraudulent schemes and training in how to apply protective measures are critical in keeping online banking safe and secure. Future research is needed to assess how customers can be trained to effectively mitigate phishing scams and whether customers are the right unit of analysis to target with interventions for combating malware attacks.

Keywords: Online Banking Fraud, Phishing, Malware, Customer Behaviour, Protection Motivation Theory, Routine Activity Theory.

Introduction

This paper describes an in-depth analysis into the behaviour and characteristics of bank customers leading to victimization caused by phishing and malware attacks, the most common crimes involving online banking fraud in the Netherlands (NVB, 2013). Phishing is "a scalable act of deception whereby impersonation is used to obtain

[1] PhD Candidate, NHL University of Applied Sciences, Rengerslaan 10, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands. E-mail: j.jansen@nhl.nl
[2] PhD Candidate, NHL University of Applied Sciences, Rengerslaan 10, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands. E-mail: E.R.Leukfeldt@nhl.nl

information from a target" (Lastdrager 2014, 8). Malware is the infection of a computer by malicious software, which includes viruses, worms, Trojan horses and spyware. In both cases, the aim of the fraudsters is to deceive the customer or the system used for online banking in order to obtain user credentials and/or to gain control over customers' devices. Fraudster use user credentials to access a victim's online bank account and to validate money transfers on behalf of the victim. Phishing and malware scams, however, are significant across the world and go beyond the online banking context. The Anti-Phishing Working Group reported in their Phishing Activities Trends Report of Q4 2014 that nearly 200,000 unique phishing reports were submitted to them and that an average of 255,000 new malware threats (including variants) emerged each day (APWG, 2015).

A number of recent studies try to shed light on how and why people fall victim to these crimes and others do not (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Vishwanath, Herath, Chen, Wang, & Rao, 2011). Jansen and Leukfeldt (2015), for example, carried out an exploratory study into how customers become victims of online banking fraud and demonstrate that customers have a specific role in their own victimization. Customers provide fraudsters with information, such as credentials, which fraudsters can use to steal money from their bank accounts. A study into phishing victimization shows that everybody is at risk when it comes to this type of crime (Leukfeldt, 2014). Additionally, Leukfeldt (2015) claims that this also largely holds for malware victimization; merely spending more time online, carrying out various kinds of activities, increased the risk of a malware infection.

Both of Leukfeldt's studies (2014, 2015) – which are based on an online survey – conclude that in-depth studies are necessary to increase knowledge about why customers are victimized. It is not sufficiently clear if certain individuals are more prone to being at risk for online banking fraud than others, and how it can be explained. Therefore, this study qualitatively explores, by means of interviews, what factors explain online banking fraud victimization. Crossler et al. (2013) mention, that, the interview is a valuable method to better understand the actual motivations and behaviour of individuals.

Theoretical background

For this study, two theoretical perspectives are in place. First, we take a routine activity approach (Cohen & Felson, 1979) to study victim characteristics and behaviours that influence victimization. This approach is also central to the studies of Leukfeldt (2014, 2015) making it possible to assess whether our qualitative study has added value to the quantitative studies in this context. The routine activity approach holds that victimization is influenced by a combination of a motivated offender, a suitable target and the absence of a capable guardian in a convergence of time and space. We study the two latter aspects of routine activity approach, namely the suitability of targets and the capability of their guardians. Guardians can, for example, be technical security measures such as anti-virus software.

Over time, elements regarding suitability have been added to the routine activity approach. Two acronyms that often emerge are CRAVED, which stands for concealable, removable, available, valuable, enjoyable and disposable and VIVA, which stands for value, inertia, visibility and accessibility. Sutton (2009) compared the two acronyms and concluded that they deal with identical attributes. Furthermore, he argues that VIVA elements relate to characteristics that attract attention, while the additional elements of

CRAVED are related to characteristics that make an object attractive for criminals. As this paper is about characteristics of victims that make them appeal to a motivated offender, we adopt the VIVA acronym.

Value means that fraudsters are interested in individuals who, for the purposes of online banking, have large sums of money in their bank account. Cyber crime studies have shown a correlation between victimization of identity theft and households with higher incomes (Anderson, 2006; Harrell & Langton, 2013). We have excluded inertia from our study because, in the context of cyber crime, it refers to the volume of data and technological specifications of computer systems (Yar, 2005). Visibility is operationalized as online activities. Cyber crime studies show that such activities, e.g., downloading and spending time on social media, make targets become suitable since these increase visibility (Bossler & Holt, 2009; Hutchings & Hayes, 2009; Pratt, Holtfreter, & Reisig, 2010). Lastly, accessibility refers to weaknesses in software that can be used by fraudsters to attack customers. Although these three factors do explain victimization for some cyber crimes, Leukfeldt's study (2015) did not provide evidence for this related to online banking fraud victimization. We assess this outcome by using a more in-depth methodology.

The routine activity approach is used in numerous studies (e.g., Bossler & Holt, 2009; Hutchings & Hayes, 2009; Ngo & Paternoster, 2011; Prattet al., 2010; Reyns, Henson, & Fisher, 2011; Van Wilsem, 2011a, 2011b). However, a critical note we need to make relates to an issue introduced by Yar (2005) who argues that it is problematic to convert the routine activity approach from real space to cyber space. Leukfeldt and Yar (2016) show, that, the significant impact of the routine activity theory elements differs greatly between different types of cyber crime. Therefore, we applied the interview method in order to overcome the issue of relying too much on analytic truths that is, measuring a limited number of (predetermined) items.

Protection motivation theory (Rogers, 1975), henceforth PMT, is used as the second theoretical perspective. PMT is a social cognitive theory that predicts behaviour (Milne, Sheeran, & Orbell, 2000) and seems applicable to online banking (Jansen, 2015). In PMT, two cognitive processes are central: threat appraisal and coping appraisal. The first process evaluates vulnerability to and the impact of a threat. This is continued by the second process that evaluates possible strategies to cope with a threat. This evaluation is based on response efficacy, self-efficacy and response costs. Both processes influence protection motivation, i.e., the intention of taking measures to protect online banking. We assume that not taking adequate protective measures, or not having capable guardians in place, might influence victimization. To be more precise, we do not qualitatively test PMT, rather its constructs are used as possible additional indicators explaining online banking fraud victimization.

Methods

We conducted 30 semi-structured interviews with online banking fraud victims. The goal was to unravel how and why they became victims of online banking fraud. The interviews took place between October 2014 and April 2015, were recorded using a digital voice recorder and lasted 52 minutes on average. Sample questions include: What is your experience with online banking? How did the phishing/malware incident unfold? Do you have any idea why you were targeted? What protective measures did you have in place to prevent phishing/malware attacks from occurring?

Respondents were recruited based on a selection of 65 police reports from the northern (N =31) and southern (N =34) regions of the Netherlands. A liaison officer working for the Dutch police first contacted the victims by telephone to inform them about our study and ask their permission to be approached to participate in an anonymized interview. Of the northern cases, seventeen respondents agreed to be interviewed, five declined the request and nine were not reached. Of the southern cases, twelve respondents agreed to be interviewed, four declined the request and two were not reached. The remaining sixteen interview candidates were not contacted because we gathered sufficient data to complete the study. One participant was recruited via a liaison officer at the Fraud Helpdesk, a national organization for answering questions and collecting reports about fraud.

We interviewed seventeen phishing and thirteen malware victims. The mean age of the respondents was 59 years (SD = 17) and ranged from 23 to 89 years. Thirteen respondents were female and seventeen were male. Respondents had different levels of education; low (N =3), medium (N =15) and high (N =12). Most respondents can be considered to be experienced users of online banking, having used it for at least five years (N =23) and using it on a daily or weekly basis (N = 21).

For phishing, we interviewed sixteen private customers and one corporate customer (treasurer of a foundation). Malware victims consisted of one private customer and twelve corporate customers (e.g. self-employed entrepreneurs and small and medium-sized enterprises).In two malware cases, we did not speak with the actual victim. In one case, we interviewed the partner of the victim and in the other case the supervisor of the employee who was victimized. We have, however, included the information they provided because both were closely involved in handling the incidents. We believe that their stories contribute to studying the research problem. The private and corporate bank accounts were held at different banks in the Netherlands.

The recorded interviews were first transcribed. The transcriptions were directly sorted into the conceptual categories we defined prior to the study. In order to analyze the interview data, we used QualiCoder (Version 0.5), a type of computer-assisted qualitative data analysis software. The data within the initial categories were labelled with analytical codes to separate the data into theoretical themes (Ritchie, Lewis, McNaughton-Nicholls, & Ormston, 2014). After that, we reviewed the data extracts.

The results of private and corporate customers are presented together because there is no clear distinction between their stories. In nine interviews, we discussed whether corporate customers behave differently with respect to online banking when engaging in work-related banking activities as opposed to their private use of online banking services. Three respondents mentioned that their private and corporate use of online banking is the same. One of them mentioned, "In both cases, you deal with money. In either case, it would be a shame when something goes wrong." Six respondents mentioned minor differences. Differences regarding corporate use of online banking include dealing with larger amounts of money, using online banking more frequently and using an accountancy system. One respondent mentioned being less precise when verifying individual payment details in a business context, "It should be consistent with bookkeeping."

Results

In the following sections, we present frequencies of particular views or experiences of respondents. However, we do not claim that this provides a representative image of all online banking fraud victims since that is not the objective of the current study nor is it possible using this method. Rather, enumeration provides insight into how phenomena may vary among respondents.

1. Anatomy of Phishing and Malware Attacks

The anatomy of the phishing attacks described by the respondents is in line with what is known from literature (Hong, 2012; Jansen & Leukfeldt, 2015). An attack starts with a potential victim receiving an e-mail or phone call designed to deceive them. Then, the potential victim takes the suggested action, such as giving away user credentials, which is followed by the fraudster using the stolen information to obtain money.

Of the twelve respondents who received a phishing e-mail as point of entry for the scam, nine were called afterwards in order to obtain additional information. The contents of the e-mails were related to security and authentication issues surrounding online banking. In total, thirteen victims were called by a fraudster, four of whom believed this to be the starting point of the scam. The content of the phone calls focused on security as well, sometimes accompanied by the caller mentioning that the recipient should check or complete a procedure that was put in motion by the recipient of the call through an e-mail response. One phishing victim was unaware of how his information was phished. The respondent, however, mentioned being aware of the numerous places where people's personal information is stored, "You have to leave your personal data everywhere." In addition, phishing respondents often reported that the fraudulent story was perceived to be trustworthy and/or that they just were not alert enough to counter the scam.

Malware attacks take place using a similar three-stage approach, except that no direct interaction between the victim and fraudster was required. Interestingly, victims themselves were unable to reconstruct the fraud process. Six victims reported not having noticed anything when the attack was carried out. The online banking process proceeded in the way they were accustomed to. A respondent stated, "There was nothing out of the ordinary. Nothing in particular which makes you think 'Huh?' afterwards."

Seven malware victims reported having observed an anomaly, of whom four mentioned having seen a glitch on their screen. The remaining respondents indicated that the browser stopped operating, that the payment instruction disappeared and that there were problems logging in. One of these respondents indicated that the anomaly occurred "quite some time" before the actual incident took place. The respondents who observed an anomaly did not, however, relate these events to a malware attack. One respondent stated, "It is associated with the inscrutable ways of the internet. […] It is science fiction to me."

We are able to make the claim about the anatomy; however, since the malware attacks were part of an investigation completed by the Dutch police. The Dutch police completed an investigation of a series of malware attacks in which infected websites were used to automatically install malware on the customers' device when visiting these websites (Leukfeldt, Kleemans, & Stol, in press). When the customer transferred money online using the compromised device, the largest transfer was modified. The amount was split into two, whereby one amount was sent to the original recipient and one amount to the bank account of a money mule, a person responsible for transferring illegally acquired

money to fraudsters. The customer approved the transaction because the fraudulent modification was not visible on screen. Moreover, the fraudulent transfer was hidden in the payment summary screen. It could only be observed when logging on to the online bank account with a device that was not infected with malware.

2. Suitability Factors

Suitability factors from the routine activity approach do not seem to have any influence on victimization. Hence, the majority of victims think that the fraudster selected them randomly. A malware victim added that thinking this way is possibly for the best, "Otherwise you might believe that someone is watching over your shoulder all the time." A phishing victim mentioned that she had the feeling not being chosen for who she is, but because she belongs, "to a club of fools who have clicked on a link."

Most victims do not relate *value* to victimization. A phishing victim said, "I do not consider myself to be a perfect victim. There are people with much higher amounts of money in their bank accounts that it would have been better to pick." However, one phishing victim and three malware victims think that the value criterion might be related to victimization. The phishing victim may be targeted because of where she lives, i.e., suburb and type of house. The malware victims considered value to be a possibility, since their businesses deal with large cash flows.

We could not directly find any evidence for the *visibility* criterion being a risk factor. One malware victim opted that he might have accessed an unsecure website. Two phishing victims mentioned that they never logged out of their online banking sessions, but instead clicked away the window. However, they were not certain whether this had anything to do with their victimization.

During the time of the incident, all respondents were using a desktop computer or laptop for their online banking activities. Except for two Apple users, all respondents used some version of Microsoft Windows. Most respondents were not aware of any weaknesses in their technical infrastructure that may have led to victimization. Therefore, we cannot conclude that the *accessibility* criterion is of importance. Two phishing victims stated, however, that this could be a possibility. One respondent mentioned that his security subscription needed to be extended and one suspected that his computer had been hacked. Two malware victims also linked a security flaw to victimization. One of these respondents explained that one of the business computers was not equipped with anti-virus software. The other mentioned that it could be associated with a Java update he continuously declined to install. He stated, "A message from Java constantly appeared on my screen wanting me to install an update. I have never clicked on this message because Java sounded like something illegal." However, all four respondents were not sure if the security issue they mentioned is the (true) cause of victimization.

Some respondents came up with *other reasons* for why they might be considered a suitable target. Several phishing victims indicated that their (older) age might be a possible explanatory factor. Additionally, two phishing victims pointed out that they became suitable targets after the incident had occurred. Both had the idea that they were in a "victim database", because at a later date, they became scam targets again. One of them said, "Maybe I am on a list of interesting addresses where there is something to be had."

We asked respondents if they thought that a similar incident would happen again in the future in order to assess whether they considered themselves to be suitable targets now

they have been victimized. Five phishing victims were adamant that it would never happen again. A respondent stated, "I have learned the hard way." The other twelve mentioned hoping or expecting that it would never happen again. Some of these respondents indicated, however, that there is always a possibility.

Malware victims responded similarly. Nine respondents indicated that the chances of being victimized again are slim, but do exist. A respondent replied, "It is the same as winning a lottery. There is a small chance that it will happen again, but it is possible." The remaining four respondents were not able to give an explicit answer. One respondent blamed the obscureness of the incident for this. The others stated that if it can happen once, it can happen again, "It is a fifty-fifty chance."

3. Capable Guardians and Protective Factors

Because we did not find strong support for the suitability factors explaining victimization, we will now examine the extent to which capable guardians were in place. In this study, we define "capable guardians" as the precautionary behaviour of respondents regarding the safety and security of online banking. Where appropriate, results regarding capable guardians are supplemented by statements from PMT.

Before asking respondents what protective measures they took, we first asked to what extent they were aware of the threat that they were victimized by prior to the incident. Nine respondents indicated that they were not aware of phishing prior to the incident, or stated that they were unfamiliar with the modus operandi used to scam them. A phishing victim indicated that he was, "not in a position to know there could be something wrong" because he believed that his bank did not inform him about the threat. Five respondents reported that they were aware of the existence of phishing. However, four of them also mentioned not knowing how phishing schemes manifest in practice. In the case of malware, five victims knew they could be victimized in such a fashion, although some were under the assumption that it would not happen to them. One respondent mentioned, "The same is true for burglaries; you always think it will happen to someone else." Furthermore, six malware respondents indicated not having heard of the threat they fell victim to. This topic was not discussed in the interview sessions with the remaining four respondents.

We went on to ask respondents how they protect themselves against threats aimed at online banking. We did so using an open-ended question first and second by letting respondents fill out a list with protective measures. In general, most respondents take precautions to keep online banking safe and secure. Protective measures that were mentioned most are: having good security on the device for online banking (N = 21), such as anti-virus software and the latest updates, checking the money transfer details before finalizing the transfer (N = 8), deleting suspicious e-mails or e-mails from unknown sources (N = 6), and checking whether the internet connection with the bank's website is secure (N = 5), for example by checking for https and a closed padlock. On the open-ended question, three respondents indicated that they did not take any measures. A phishing victim said, "When I am using online banking services, I do not immediately think about crime. I have no idea how I should protect myself against it."

After answering the open-ended question, respondents could score their use of protective measures that we presented to them with "yes", "no" and "do not know". The measures we included were based on uniform safety rules for online banking, which are defined in the general terms and conditions of all banks in the Netherlands. These rules

and subsequent responses are as follows: 1) keep you security codes secret (N =29); 2) make sure your debit card is not used by other persons (N =26); 3) secure the devices you use for online banking properly (N =29); 4) check your bank account information at least every two weeks (N =29); and 5) report incidents directly to your bank (N =30). Although most respondents indicated that they comply with the rules set by banks, most phishing victims admitted that they had been negligent once with respect to sharing security codes.

The respondents were also asked why they take protective measures. Twelve respondents indicated that the measures they take effectively assist in protecting them against fraud or that they hope that they do so. A malware victim stated, "I think I am maximally protected. However, there is always a risk. There is no such thing as one hundred per cent security." A phishing victim added, "If criminals really want something, they will probably achieve their goal. However, you should not open the door for them. I believe that I have locked the front and back doors." Respondents also mentioned that they like to act according to the rules (N =3), and to take the bank's terms and conditions into account so that they can get reimbursed (N =2). Other respondents did not have a clue whether the measures are effective in protecting them against online banking fraud, often because they do not know how security works. One phishing victim questioned the efficacy of protective measures, "In some instances, only one password is needed. The security is much too limited."

Another means to gain insight into respondents' perceptions on *response efficacy* is to ask them if they could have prevented the incident. Five phishing victims thought that the incident could not have been prevented. One respondent indicated, for example, that he took the same actions and measures before, during and after the incident. Another respondent mentioned, "There are always moments when you just are not alert and that is when something can happen. This is not exclusive to online banking, it is true for a lot of other things."

Other phishing victims mentioned that the incident may have been prevented if they had been more alert when reading the phishing e-mail, if they had not performed the actions fraudsters asked them to, if they had listened to their instincts, if they had been aware that banks do not conduct such procedures via e-mail and if they had been aware of the level of sophistication of criminal schemes. In addition, a respondent indicated that it is a difficult issue, "People are insecure, vulnerable, do not know exactly what the procedures are. When a message appears about IBAN [International Bank Account Number, which had just been introduced for domestic payments in the Netherlands], for example, things can easily go wrong."

Because it was unclear to most malware victims how the incident had happened, they were virtually unanimous that they did not know whether the incident could have been avoided (N =9). Additionally, respondents reported not having received any feedback from the police or their bank on how the incident unfolded. Two malware victims mentioned that installing a (better) virus scanner might have prevented the incident. Another respondent mentioned that installing software updates might have made a difference, and yet another one stated that she may have been able to prevent the incident if she had checked whether the internet connection between her device and the bank was secure.

Eight respondents experienced *response costs* when taking protective measures due to lack of knowledge and/or low *self-efficacy* when taking precautionary measures. Some mentioned that security is just too complex for them. Two illustrations of this given by phishing victims, "Someone needs to tell me exactly what to do, for example, where to click for software updates. I do not know much about computers, which makes it difficult. You are already down 0-1." And, "I wrote down everything on paper in order to arrange security. This is due to my age: one day you know it, the next you do not. It does not stick."

It is noteworthy that sixteen respondents indicated that they had security assistance available or that they completely outsourced security, for example, to a family member or a security company. These respondents do so because they have no knowledge or not enough about security-related issues, or that they lack the necessary skills. Outsourcing security is a means to overcome the barriers or response costs they experienced. Consequently, these respondents completely trust that their security is well organized and so they feel safe. Two illustrations by malware victims, "I do not know what is done in order to secure my PC, but I am confident that it is good." and, "I imagine I am safe because I use a corporate security package provided by[provider]. I trust it completely."

Three respondents consider protective measures a hassle, annoying or irritating. However, half of the respondents claim to experience no response costs that hinder the usage of protective measures; it is part of their routine. A malware victim added, "You need to be alert, like in traffic. Then you also have to pay attention to red lights and putout your hand when you turn." Another malware victim stated that he is willing to adopt additional measures if necessary, "I am not bothered by it. I prefer to make a little more effort knowing it is safe."

In sum, capable guardians are in place in most cases, with the exception of four instances as reported in the suitability factors section. However, some respondents mentioned difficulties with regard to the PMT variables of response efficacy, self-efficacy and response costs.

Discussion and Conclusion

The current application of the routine activity approach is not adequate for distinguishing characteristics and behaviours of respondents that explain why they have been contacted and/or have become victims of online banking fraud. This is a typical since most cyber crime studies paint a different picture (Anderson, 2006; Bossler & Holt, 2009; Pratt et al., 2010). However, it is in line with the results of Leukfeldt (2015). Our study concurs with his statement that it seems that everyone is at risk.

The above holds that for online banking fraud: there is simply no such a thing as a suitable target. Becoming a victim appears to be simply a coincidence in this regard, a contextual phenomenon. Victimization seems to occur because fraudsters continually adjust their modus operandi according to recent events, because they gain the trust of customers or because customers simply do not pay sufficient attention. Ngo and Paternoster (2011) claim that the routine activity approach is perhaps not the best framework for studying online threat victimization at the individual level. If we challenge this conclusion, the question then is what does make these respondents suitable targets? Future research could make use of different research approaches or theoretical perspectives. Studying customers' actual computer and internet behaviour, for example by analyzing logfiles, might provide evidence for what makes them suitable targets or

increases their chances of becoming fraud victims. Another possibility is to use other predictor variables in quantitative studies, for example personality factors from the Big Five Inventory.

For phishing, additional possibilities for future research might involve studying in which databases or on which social network sites victims' e-mail addresses are stored. Perhaps phishing victims were targeted because fraudsters obtained personal information by buying e-mail addresses used for spam mailings or by hacking certain databases that are poorly protected. If this is the case, updating the security of databases could provide a barrier to stop fraudsters from obtaining these details. After all, this is how the crime script for phishing often starts. Another possibility for preventing phishing e-mails from appearing in people's inboxes includes technical solutions, like e-mail filters. However, accuracy and usability are challenges for these (Hong, 2012).

We do know, based on police intelligence, that most devices of malware victims were automatically contaminated with malware when visiting ordinary websites with outdated security. This raises the question of whether customers are the right unit of analyses or the right target group for interventions to counter malware victimization. Maybe we should target website owners and hosting companies in our efforts to reduce malware victimization.

Regarding protective measures, we found that malware victims generally take adequate measures to protect the security of their technical infrastructure. Our study found no concrete evidence that malware victims were grossly negligent about security, except for two respondents: one who had outdated software and one who had no anti-virus software. Therefore, it is not possible to provide recommendations for improving security on the customer side– apart from having basic security software installed (Choi, 2008) and making sure all software packages are up to date. This backs the recommendation we presented above about debating the issue of which actors should be addressed in combating malware attacks. Having said that, in this study we rely on self-reports. It might be interesting for future research to study the actual devices of customers (who have been victimized) to establish how they are secured.

Phishing victims were negligent because they gave security codes to fraudsters. We believe that awareness about this threat can be raised further. In addition, online banking processes should be more transparent, e.g. customers need to know what security codes entail and what happens when they fall in to the wrong hands. Although a third of the respondents were aware of threats, they often did not know how these threats manifest in practice. We believe that if customers are more aware of threats, they will recognize them more easily and take actions accordingly. Experimental research could provide evidence for this suggestion. Furthermore, banks and police could play a role here, for example, by providing victims with feedback on how the attack unfolded. If victims do not understand what had happened, it is difficult for them to prevent bad things from happening again.

What also became clear is that respondents were unable to properly assess the effectiveness of measures to mitigate threats. Although it may be difficult to prove a measure's efficacy, it is important to not only communicate to the customer what to do and how to do it, but also what a certain measure aims to address. Hence, PMT posits that response efficacy is an important predictor for precautionary behaviour. Because security is a difficult and obscure subject for many respondents, communication about this subject must be expressed as simply as possible. When customers understand the need for

protective measures and gain more insight into the underlying principles, we expect that they will be more willing to apply these measures.

While most respondents perceived no response costs or barriers to taking measures, we noticed that a number of respondents found it difficult to do so, often because of a lack of knowledge and self-efficacy or skills. Therefore, it is important to train customers how to apply security measures. Although some respondents mentioned having outsourced security, they are still the ones that perform transactions and money transfers. Furthermore, training is important since customers are attributed with more responsibility regarding safety and security of online banking (Anderson, 2007; Davinson & Sillence, 2014). This is illustrated by the fact that some of our phishing respondents were not reimbursed by their bank. This raises the question of whether customers can be held responsible when something goes wrong if they are not properly taught how to apply protective measures.

The challenge lies in what is the most effective way to train customers. It would seem obvious to offer courses on safe online banking. In the Netherlands, we note that various banks and special interest groups already offer such courses. Moreover, a special website has been set up to warn customers about online threats and to tell them how to deal with these threats (www.veiligbankieren.nl). Banks could also consider letting their customers take a test in order to see whether they are capable of using online banking safely. However, this recommendation is probably not realistic since it is more cost-effective for banks to offer online banking instead of traditional banking methods. Besides, banks would not be keen to lose customers to other banks that do not implement tests. Therefore, a more effective way would be to explore using embedded training (Jansson & von Solms, 2013; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010) that is integrated within the online banking environments. This way customers receive relevant information in a relevant place and on a relevant time, namely when they are actually using online banking –without interrupting the payment process too much needless to say. It is claimed that learning is more meaningful when rooted in the social and physical context in which it is used (Brown, Collins, & Duguid, 1989). It is also important to periodically repeat this kind of training. Research on cardiopulmonary resuscitation (CPR) skills retention, for example, shows that not only participants' skills, but also their knowledge, already decrease after a two-month interval (Einspruch, Lynch, Aufderheide, Nichol, & Becker, 2007).

Although a smooth online banking experience is critical, it is essential to identify the best solution for educating and training customers. Future research may seek evidence for this suggestion. Furthermore, it is important to answer the question of whose responsibility it is. Is it a duty for banks in particular because they offer online banking services? Or is it a problem for society – one that falls within the scope of online safety and security in general – and one that the government should be dealing with?

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 respondents 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

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171.

Anderson, R. (2007). Closing the phishing hole - Fraud, risk and nonbanks. *Proceedings of the Payments System Research Conferences,* 1–16.

APWG [Anti-Phishing Working Group] (2015). *Phishing activity trends report: 4th quarter 2014*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf.

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.

Brown, J. S., Collins, A. & Duguid, P. (1989). Situated cognition and the culture of learning. *Educational Researcher*, *18*(1), 32–42.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588–608.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

Davinson, N. & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), 154–168.

Einspruch, E. L., Lynch, B., Aufderheide, T. P., Nichol, G. & Becker, L. (2007). Retention of CPR skills learned in a traditional AHA Heartsaver course versus 30-min video self-training: A controlled randomized study. *Resuscitation*, *74*(3), 476–486.

Harrell, E. & Langton, L. (2013). *Victims of identity theft, 2012*. Washington DC: Bureau of Justice Statistics.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81.

Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the net? *Current Issues in Criminal Justice*, *20*, 433–451.

Jansen, J. (2015). Studying safe online banking behaviour: A protection motivation theory approach. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance*, 120–130.

Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Proceedings of the 5th Workshop on Socio-Technical Aspects in Security and Trust*, 25–31.

Jansson, K. & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 7:1–7:31.

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

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering, 4*(5), 26–32.

Leukfeldt, E. R., Kleemans, E. R. & Stol, W. P. (in press). From low tech locals to high tech specialists: A typology of phishing networks. *Crime, Law and Social Change*.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis, *Deviant Behavior*, *37*(3), 263–280.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Ngo, F. T. & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

NVB [Dutch Banking Association] (2013). *Position paper rondetafelgesprek online betalingsverkeer: 30 mei 2013 [Position paper on online banking: May 30, 2013].*Amsterdam: Nederlandse Vereniging van Banken.

Pratt, T. C., Holtfreter, K. & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Reyns, B., Henson, B. & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169.

Ritchie, J., Lewis, J., McNaughton-Nicholls, C. & Ormston, R. (2014). *Qualitative research practice: A guide for social science students & researchers*. London, UK: SAGE Publications Ltd.

Sutton, M. (2009). Product design: CRAVED and VIVA. In B. S. Fisher, & S. P. Lab (eds.), *Encyclopedia of Victimology and Crime Prevention*. Thousand Oaks: Sage.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.

Wilsem van, J. A. (2011a). 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.

Wilsem van, J. A. (2011b). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2),168–178.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.