CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 17, Number 8, 2014

DOI: 10.1089/cyber.2014.0008

Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization

E. Rutger Leukfeldt, MSc

Abstract

This article investigates phishing victims, especially the increased or decreased risk of victimization, using data from a cybercrime victim survey in the Netherlands ($n = 10{,}316$). Routine activity theory provides the theoretical perspective. According to routine activity theory, several factors influence the risk of victimization. A multivariate analysis was conducted to assess which factors actually lead to increased risk of victimization. The model included background and financial data of victims, their Internet activities, and the degree to which they were ''digitally accessible'' to an offender. The analysis showed that personal background and financial characteristics play no role in phishing victimization. Among eight Internet activities, only ''targeted browsing'' led to increased risk. As for accessibility, using popular operating systems and web browsers does not lead to greater risk, while having up-to-date antivirus software as a technically capable guardian has no effect. The analysis showed no one, clearly defined group has an increased chance of becoming a victim. Target hardening may help, but opportunities for prevention campaigns aimed at a specific target group or dangerous online activities are limited. Therefore, situational crime prevention will have to come from a different angle. Banks could play the role of capable guardian.

Introduction

DIGITAL PAYMENT SYSTEMS play a crucial role in our society. In 2012, in the Netherlands, more than 8 out of 10 Internet users (82%) used online banking with the percentage rising to 92% for users aged between 25 and 45 years.[1] The number of Dutch people shopping online grew in 2012 to 9.5 million. According to the Dutch Home Market Monitor, online consumer spending totaled more than €9.8 billion.[2] This flow of digital finance attracts criminals. According to the annual report of the Dutch Association of Banks, a major portion of total fraud costs (€82 million) in 2012 is attributable to phishing (€35 million—equivalent to 2011).[3] In other countries, there are similar damages. In England, the loss in 2012 was €46.2 million.[4]

Phishing is the process aimed at finding out users' personal information by posing as a trusted authority using such digital means as e-mail.[5–8] Routine activity theory explains changes in crime brought about by technological developments,[9] including the behavior of victims, as the reason why crime occurs.[10] This article aims to contribute to the knowledge about the groups that are at increased risk of phishing victimization and, in turn, provide insights into opportunities for prevention.

Suitable Targets: Expectations Based on Routine Activity Theory

According to routine activity theory,[10] opportunity structures influence the prevalence of deviant behavior. The combination of the presence of a motivated offender and a suitable target, and the absence of a capable guardian influences these structures. Felson and Clarke suggest four elements that determine the extent to which a victim appeals to a motivated offender: value, inertia, visibility, and accessibility.[10] This section zooms in on these four elements and draws hypotheses for the four elements in relation to phishing victimization.

Value

Offenders are particularly interested in goals to which they assign value for whatever reason. A popular brand of laptop, for example, is easier to sell than an unknown brand, even if their monetary value is about equal. Value can be operationalized in several ways. In phishing, the size of a bank account may be interesting, as the profit potential is higher. Households with higher incomes are more at risk of becoming victims of identity theft.[11,12] In our study, respondents were

Cyber Safety Research Group, NHL University of Applied Sciences and Dutch Police Academy, Leeuwarden, The Netherlands.

not asked directly how much money they had in the bank. However, with data from Statistics Netherlands, financial assets and income could be linked to respondents. These factors are used as an indication of the level of bank accounts. The first hypothesis is:

H1: Victims have significantly higher income and financial assets than nonvictims.

Inertia

Felson and Clarke describe inertia simply as the weight of the item.[10] Small electronic goods, for example, are easier to steal than heavy cumbersome objects, unless the latter is provided with wheels or is motorized. Van Wilsem argues that this factor is less important in criminal forms of identity fraud such as phishing.[13] With material goods, the removability of the property is a relevant criterion for target selection (and one reason why many new portable technologies, such as smart phones and laptops, are so theft sensitive). In the case of information theft, this seldom applies (only with extremely large databases, at most). Therefore, the multivariate analysis excluded inertia.

Visibility

Visibility refers to the conspicuousness of objects criminals want, for example expensive items in a living room that can be seen from the street. Empirical studies into cybercrime show that visibility of someone online can also provide an increased risk of victimization. For an offender, degree of visibility is linked to the degree to which a person is a suitable target. The activities that predict higher risk of victimization differ in the literature. This is unsurprising considering the studies deal with victimization in various cybercrimes. Hinduja and Patchin, for example, showed that computer proficiency and the time someone spends online are factors for victimization in bullying.[14] Holt and Bossler found in their study of online harassment that spending time in chatrooms increased risk of victimization.[15] Van Wilsem showed that risk of fraudulent bank payments is greater among students, as they share more personal information on social networking sites.[16] Other studies show that downloading free games and music from unknown Web sites, opening attachments in e-mails from strangers, and clicking on pop-up messages also increase the risk of online victimization.[17,18]

Clearly, these studies show online activities contribute to making someone a suitable target, simply because they increase visibility. In the case of phishing, the question is which (and to what extent) online activities actually provide suitable targets. Respondents were asked to indicate what activities they conducted online (and how frequently). Eight activities can be classified in two categories of behavior: activities with a high or low level of online visibility. Activities with low visibility are e-mail, targeted browsing, and using direct messaging platforms such as MSN and Skype. Activities with high visibility are untargeted browsing, using online chatrooms, online gaming, actively using Internet forums, active social networking, and twittering. The hypothesis that follows is:

H2: Victims conduct significantly more highly visible online activities than nonvictims.

Accessibility

According to Felson and Clarke, accessibility is related to the construction of communities, placing goods in easily accessible locations, and other features of everyday life that make it easy for offenders to come into contact with their target.[10] Accessibility in the offline world can be translated into the online world. Users need software such as operating systems and web browsers to enter the online world. Motivated offenders abuse holes, gaps, or leaks in software to attack users (e.g., infect them with malware). Popular, commonly used operating systems and web browsers are attractive to motivated offenders. They can attack millions of users at once, just by abusing one weakness in the software. A relatively large group of motivated offenders is constantly trying to find new weaknesses in software and shares information on (potential) holes on forums (different studies describe these forums[19–23]). Indeed, so much is known about abusing weaknesses in popular software that users of popular platforms are more accessible to criminals than users of less popular software. Obviously, the user's operating system and web browser can influence victimization.

H3: Victims use popular (commonly used) operating systems and web browsers significantly more often than nonvictims.

Software can also protect users. A user becomes less accessible to a criminal when he takes protective measures by installing and updating antivirus software. Known holes in software abused by criminals disappear, protecting users against malware attacks. The use of antivirus software may thus affect victimization. Studies show varying results. Choi indicates a protective factor[17] while the studies of Holt and Bossler and of Marcum show no effect.[15,18] Based on the theory, however, it is expected that:

H4: Victims have significantly less up-to-date antivirus software than nonvictims.

Technical knowledge might also be a protective factor against victimization by phishing. Technical knowledge ensures that a potential victim is less accessible to a motivated offender.[24,25] The less users know about the software and equipment they use, the less they know about the risks they run. Phishers exploit this and, for example, try to trick users into believing something went wrong in their last online banking session. They then approach the user with the solution for this so-called problem, which has to be fixed as fast as possible to prevent further damage (e.g., ''Click on this link to log onto the secure website of Bank X''; for the use of social engineering, see Mitnick and Simon[26]). Thus, it follows that:

H5: Victims have a significantly lower level of computer literacy than nonvictims.

An offender may also gain access to a victim through the victim's own actions. After all, one way to gain the identity of users is by infecting a computer with malware. The studies by Choi and Marcum show that activities such as downloading free games and music from unknown Web sites increases the risk of online victimization.[17,18] Downloading may increase

the risk of infection with malware. By downloading files (which might be infected with malware) from unknown platforms (which might be infected with malware), the victim makes himself accessible to the motivated offender. Thus, it follows that:

H6: Victims download significantly more often than nonvictims.

The victim's awareness of risk may also determine their accessibility. Internet users who are aware of the risks they run online are better able to anticipate risk and are therefore less likely to become victims. The studies by Choi and Marcum show, for example, that opening attachments in e-mails from strangers and clicking on pop-up messages increases the risk of online victimization.[17,18] Respondents were asked about their awareness of online risk. The hypothesis that follows from the above is:

H7: Victims have a significantly lower level of risk awareness than nonvictims.

Data and Methods

To determine the factors that play a role in phishing victimization, a secondary analysis of a data set of cybercrime victims in the Netherlands was conducted.[27] The representative sample included 21,800 Dutch citizens aged 15 years and older, of whom 10,314 (47%) responded. This analysis involved 9,163 respondents (89%) who reported using the Internet.

To gain insight into the financial situation of respondents, data from the Social Statistical Database (SSB) of Statistics Netherlands was linked to the data set of cybercrime victims. The SSB contains more than 40 linkable and mutually matched records on various subjects. Various government agencies such as the police, IRS, and social welfare agencies provide the initial data; see Arts and Hoogteijling for a detailed description.[28]

The dependent variable—phishing victim—was coded dichotomously (1 = ''victim''; 0 = ''no victim''). Respondents were asked about phishing attacks that resulted in financial damage in the last 12 months. Of the 9,163 respondents who reported using the Internet, 53 were victims of phishing (0.6%).

The independent variables were: (a) sociodemographic traits such as gender, age, marital status, educational level (coded in eight categories from ''no education'' to ''university education''), and employment (12 hours per week or more); (b) additional financial data (personal income, household income, value of financial assets, amount of savings), added in collaboration with Statistics Netherlands; (c) frequency of online activities, rated by respondents on a 4-point scale; and (d) accessibility factors, such as computer skills (a composite variable of knowledge about the used operating system, Internet connection, web browser, and antivirus software) and risk awareness (a composite variable of 10 propositions, such as: ''I open attachments or files from unknown senders'' and ''I use different passwords for different accounts''). Other factors include type of operating system, web browser, and possessing up-to-date antivirus software.

Suitable Targets: Risk Factors

Table 1 shows the multivariate analysis of phishing victims. The results are divided according to the elements that determine the extent to which a victim holds appeal for a motivated offender: value, visibility, and accessibility.[10] Inertia is also one of Felson and Clarke's elements, but as it was not possible to translate it well in the online context, inertia was excluded from the analysis.

Personal characteristics are also included in the model (Table 1). However, none of the personal characteristics seems to play a role in phishing victimization. Given the way phishers work, this is perhaps not strange. The phisher's tactic is to approach large groups of potential victims through, for example, spam.[5,6,8] They can reach anybody with an Internet connection and an e-mail account. Indeed, phishers do not need to select a specific group based on the personal characteristics of potential victims. The advantage

Table 1. Multivariate Analysis of Phishing Victims

	B	SE
Constant	−10,685	3,176
Background characteristics		
Gender (Man = ref)	−0.297	0.310
Age	0.010	0.012
Education level	0.039	0.096
Work (12 hours per week or more)	0.540	0.365
Financial characteristics		
Personal income	0.000	0.006
Household income	−0.002	0.007
Financial assets	0.000	0.001
Financial possessions	0.000	0.001
Savings	0.000	0.002
Online activities		
Frequency of Internet use	0.231	0.498
Online activities with high visibility		
Targeted browsing	0.519*	0.253
Direct communication: e-mail	0.197	0.199
Direct communication: MSN, Skype	0.066	0.151
Online activities with low visibility		
Chatting in chat boxes	0.187	.208
Online gaming	−0.006	0.167
Active on online forums	−0.132	0.261
Active on social networking sites	0.135	0.153
Twitter	−0.024	0.229
Downloading	−0.331	0.174
Targeted browsing	0.016	0.144
Buying online	0.159	0.369
Accessibility		
OS: Windows	−0.122	0.649
Browser: Internet Explorer	−0.115	0.383
Browser: Google Chrome	−0.072	0.360
Browser: Firefox	0.0353	0.356
Browser: Opera	0.491	1.049
Browser: Safari	0.128	0.636
No antivirus software	0.255	0.562
Computer knowledge	0.643	0.504
Online risk perception	−0.145	0.266
Nagelkerke R^2: 0.050		
$N = 8,379$		

*$p < 0.05$.

of carrying out such a large-scale attack is that even a small percentage of actual victims can provide significant gains. However, the fact that phishers use this trawling method does not mean that the risk of victimization is actually the same for all kinds of people involved in the trawl. The analysis shows that the probability of being a victim is the same for men and women of all ages and from all educational levels. If phishers do use trawling, the risk of becoming caught in the trawl is equal in all these groups.

Value (hypothesis 1)

Financial characteristics of respondents do not seem to play a role. The reason for this is less obvious. Previous studies into identity theft showed households with higher incomes are more at risk of becoming victimized.[12,13]

Phishers, however, do not plunder just the victims with large bank accounts. An unemployed person on a shoestring budget or a director of a multinational company: everyone has an equal chance of becoming a victim. There seems to be no evidence for so-called spear-phishing attacks on specific targets with lots of money.

Visibility (hypothesis 2)

We expected online activities with high online visibility would increase the risk of phishing victimization. However, these activities do not appear to increase risk. Only one variable in the ''low online visibility'' category did show increased risk of phishing victimization: targeted browsing.

In other studies, this element of the routine activity theory did increase risk of victimization regarding a broad range of cybercrimes (from online harassment and threat to online consumer fraud and malware infection).[9,14–19] Why this does not apply to phishing remains unclear. Perhaps the nature of a phishing attack is different from that of other cybercrimes. Indeed, offenders of consumer fraud, threat, and bullying all focus their attacks on a limited number of victims. Other studies show offenders and victims of cybercrime often know each other.[7,29,30] As mentioned at the beginning of this section, phishers work in a different way: they use a trawling method to catch as many potential victims as possible.

Another explanation may lie in the fact that phishers use two ways to obtain identity information: (phishing) e-mail and malware. The latter could also happen if a user is contaminated with malware by visiting an infected Website. For instance, in the Netherlands, the popular news site nu.nl was contaminated in 2013[a] when one advertisement was infected. All visitors to this Web site ran the risk of infection with malware, regardless of their online visibility. Internet users who search more than the average for information on the web and view all kinds of (legitimate) sites are at greater risk.

Accessibility (hypotheses 3–7)

Factors in relation to accessibility do not have a risk-increasing effect. This applies to both online accessibility (use of popular operating systems and web browsers) and protective measures to reduce accessibility (up-to-date antivirus software).

Accessibility can be applied to the online world: users need software such as operating systems and web browsers to enter the online world. Although it is known that motivated offenders are constantly trying to find new weaknesses in software and share information on (potential) weaknesses on forums (different studies describe these forums[19–23]), our analysis shows the type of operating system or browser someone uses does not influence the risk of phishing victimization. Apparently, in the case of phishing, the technical accessibility is not of great importance.

Another technical aspect without any effect on victimization is the use of antivirus software. The studies of Choi, Holt and Bossler, and Marcum showed different outcomes regarding antivirus software as protective factor.[15,17,18] The results of our analysis correspond with the latter two studies (no effect). That current antivirus software as a technically capable guardian has no effect on victimization is possibly because this tool works only against malware infections. Antivirus software cannot guard against mail that persuades users to provide personal information. In the case of malware attacks, the constant evolution of malware may play a role. Antivirus software only identifies malware that is already known. New variants are not detected (yet). Antivirus software also does not protect against criminals who abuse zero-day exploits (a flaw in software for which there is no patch at a certain moment).

Discussion: Opportunities for Crime Prevention

The analysis did not recognize any one, clearly defined group of users with an increased chance of becoming a victim (e.g., the elderly with big savings accounts). In addition, most online activities do not play a role in victimization. There are few opportunities to aim prevention campaigns on a specific target audience, or a particularly dangerous online activity. Future campaigns should be directed at all citizens.

Crime prevention will have to come from a different angle than target hardening alone. According to routine activity theory, capable guardians also play an important role. The banking sector might be the right actor to fulfill that role, for example by increasing the chance of catching phishers or intercepting unjustified transactions on time. Two possible strategies that match this endeavor are always initiating criminal prosecution of offenders (report offenders to the police, start civil proceedings against straw account holders), and investing in preparatory investigative work in conjunction with the police and justice department. In the second case, it is actually about stopping an attack during the attack itself. You cannot stop a motivated offender from gaining control over a victim's account, but you can stop the offender's attempts to transact money from the victim's account to the accomplices' (straw men) account. You can achieve this by monitoring transactions, and stopping and analyzing suspicious cases. This may frustrate criminals, whose ultimate goal is not to gain information from victims (the phishing process) but to gain money.

Notes

a. See, for example, www.nu.nl/blog/3494164/korte-tijd-malware-verspreid-via-advertentie-nunl.html (in Dutch; accessed Jan. 10, 2013).

Acknowledgments

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 (NVB), the Police Academy, and the Cybercrime Program of the Dutch police.

Author Disclosure Statement

No competing financial interests exist.

References

1. Centraal Bureau voor de Statistiek. (2013) *ICT, kennis en economie 2013* [ICT, knowledge, and economy 2013]. The Hague: Centraal Bureau voor de Statistiek.
2. Blauw Research. (2013) *Thuiswinkel Markt Monitor 2012* [Online shopping monitor]. Rotterdam: Blauw Research.
3. NVB—Nederlandse Vereniging van Banken. (2013) *Jaarverslag 2012* [Annual report 2012]. Rotterdam: Media-Center.
4. Financial Fraud Action UK. (2013) Decline in fraud losses stalled by rise in deception crime aimed at consumers. www.financialfraudaction.org.uk (accessed May 23, 2014).
5. Ollmann G. (2004) The phishing guide (part 1). Understanding and preventing phishing attacks. www.technicalinfo.net/papers/Phishing.html (accessed June 30, 2014).
6. Watson D, Holz T, Mueller S. (2005) Know your enemy: phishing. Behind the scenes of phishing attacks. www.honeynet.org (accessed May 20, 2012).
7. Leukfeldt ER, Domenie M, Stol WP. (2010) *Verkenning cybercrime in Nederland 2009* [Cybercrime in the Netherlands]. The Hague: Boom Juridische Uitgevers.
8. Soudijn MRJ, Zegers BCHT. Cybercrime and virtual offender convergence settings. Trends in Organized Crime 2012; 15:111–129.
9. Bossler AM, Holt TJ. On-line activities, guardianship, and malware infection: an examination of routine activities theory. International Journal of Cyber Criminology 2009; 1:400–420.
10. Felson M, Clarke RV. (1998) Opportunity makes the thief: practical theory for crime prevention. In Webb B, ed. *Police research series*, paper 98. London: Home Office.
11. Anderson KB. Who are the victims of identity theft? The effect of demographics. Journal of Public Policy and Marketing 2006; 25:160–171.
12. Langton L, Planty M. (2010) *Victims of identity theft, 2008*. Washington: Bureau of Justice Statistics.
13. Van Wilsem JA. Slachtofferschap van identiteitsfraude. Een studie naar aard, omvang, risicofactoren en nasleep. [Victimship of identity theft. A study into nature, extent, risk factors and aftermath]. Justitiele Verkenningen 2012; 1:97–107.
14. Hinduja S, Patchin JW. Cyberbullying: an exploratory analysis of factors related to offending and victimization. Deviant Behavior 2008; 29:129–156.
15. Holt TJ, Bossler AM. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior 2009; 30:1–25.
16. Wilsem van JA. Digital and traditional threats compared. A study into risk factors of victimization. Tijdschrift voor Criminologie 2010; 1:73–87.
17. Choi KS. Computer crime victimization and integrated theory: an empirical assessment. International Journal of Cyber Criminology 2008; 1:308–333.
18. Marcum C. Identifying potential factors of adolescent online victimization for high school seniors. International Journal of Cyber Criminology 2008; 2:346–367.
19. Peretti KK. Data breaches: what the underground world of ''carding'' reveals. Santa Clara Computer & High Technology Law Journal 2008; 25:345–414.
20. Holt JT, Lampke E. Exploring stolen data markets online: products and market forces. Criminal Justice Studies 2009; 1:33–50.
21. Lu Y, Luo X, Polgar M, et al. Social network analysis of a criminal hacker community. Journal of Computer Information Systems 2010; 31–41.
22. Soudijn MRJ, Zegers BCHT. Cybercrime and virtual offender convergence settings. Trends in Organized Crime 2012; 15:111–129.
23. Décary-Hetú D, Dupont B. The social network of hackers. Global Crime 2012; 3:160–175.
24. Jagatic T, Johnson N, Jacobsson M, et al. (2005) *Social phishing*. Bloomington: School of Informatics, Indiana University.
25. Wright R, Marett K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. Journal of Management Information Systems 2010; 1:47–68.
26. Mitnick KD, Simon WL. (2002) *The art of deception. Controlling the human element of security.* Indianapolis*:* Wiley.
27. Domenie MML, Leukfeldt ER, van Wilsem JA, et al. (2013) *Victims of offenses with a digital component among Dutch citizens. Hacking, malware, personal and financial crimes mapped.* The Hague: Eleven International.
28. Arts CH, Hoogteijling EMJ. (2002) Het Sociaal Statistisch Bestand 1998 en 1999 [The Social Statistics Database 1008 and 1999]. CBS, Sociaal-economische maandstatistiek.
29. Dreßing H, Bailer J, Anders A, et al. Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims. Cyberpsychology, Behavior, & Social Networking 2014; 17:2.
30. Melander LA. College students' perceptions of intimate partner cyber harassment. Cyberpsychology, Behavior, & Social Networking 2010; 13:3.

Address correspondence to:
Rutger Leukfeldt
NHL University of Applied Sciences
P.O. Box 1080
8900 CB Leeuwarden
The Netherlands

E-mail: e.r.leukfeldt@nhl.nl