Role of Digital Literacy in Preventing Hacking

Athmakuri Naveen Kumar
Hacking, Senior Software Engineer

Abstract: The foundations of cybersecurity awareness education are the fundamentals of information technology and digital literacy. Using Routine Activities Theory, investigate the role of digital literacy—a measure of guardianship—in phishing detection and response in this study. The American Association of Retired Persons (AARP) conducted a nationally representative survey that provided the study's data. Two conclusions are drawn from the analysis. First, respondents with greater digital literacy report receiving phishing emails more frequently but responding less to them. Second, a respondent's social standing is important, but primarily for phishing. According to these findings, phishing response and reception are significantly influenced by digital literacy.

Keywords: Digital Literacy, Hacking, Routine Activities Theory.

INTRODUCTION

Phishing is the act of sending bogus messages to a computer user with the intention of getting sensitive information from them (see Wall 2001; Yar 2013; Zhang and co. 2011,). Phishing is a type of cybercrime that is quite old and uses very little technology, but it is very effective. Even though there are a lot of "phish" scams out there, sending a well-crafted email to hundreds of people can still get results. "A campaign of just ten emails yields a greater than 90% chance that at least one person will become the criminal's prey," according to Verizon (2015:13). Despite the fact that phishing emails are initiated by individuals, the ultimate targets can be individuals or organizations. According to the Internet Crime Complaint Center (IC3), 6,495 individual complaints about phishing were filed between June 1, 2014 and December 31, 2014, resulting in a reported loss of $3.5 million (Internet Crime Complaint Center 2014). In the meantime, phishing schemes aimed at individuals initially assisted in facilitating several of the high-profile data breaches in organizations, such as those that occurred at Ebay in 2014 (Finkle and Seetheraman, 2014) and the Pentagon in 2015 (Brooke and Winter, 2015). The Data Breach Investigation Report is Verizon's annual report on cybersecurity incidents. The report from 2015 shows that all contributing associations revealed some sort of information break, with more than 2,000 separate breaks altogether. The individual figures and the number of large-scale security breaches are, without a doubt, conservative estimates. Businesses and institutions in particular have a strong incentive to conceal information about security breaches because not all crimes are reported. In this article, research that measures guardianship will be presented on the role that individuals' levels of digital literacy play in comprehending phishing e-mail reception and response. Phishing, in our view, is a two-stage process that is rooted in the everyday activities of digital environment users. Utilizing the insights of a situational theory of victimization known as Routine Activities Theory (RAT), we can investigate digital literacy as an aid to effective phishing guardianship.

Network protection related abilities frequently are considerably more applied, zeroing in on skills like great secret word the executives (utilizing different secure passwords, putting away passwords securely utilizing a secret key chief, two-factor verification), perceiving phishing endeavours, distinguishing vindictive messages, and utilizing open source knowledge (OSINT) devices. A powerful skill for identifying fake news, scams, and social manipulation in the world is the ability to combine intuition, curiosity, and the ability to search and analyse data gathered from the Internet and other open sources. (Bada, Sasse, and Attendant, 2019; (Carretero-Gomez, Vuorikari, & Punie, 2017) Digcomp, a digital competence framework for European citizens, presents competencies to protect devices and personal data from risks and threats in digital environments. It also applies cybersecurity skills to real-world employment scenarios, such as the use of social media in a corporate environment. Wells, Conflict, & Gibson, 2017. Despite the fact that the United States National Cyber Strategy (National-CyberStrategy.pdf, 2018) emphasizes the need to secure critical

infrastructure and protect networks, services, and information, organizations are realizing that humans are still the weakest link in cybersecurity (Boulton, 2017; 2019 Postimees; 2019 (Zimmermann & Renaud). One recent study, for instance, found that the majority of inexperienced users do not know how to encrypt their email messages. "Some say that the average computer user simply lacks knowledge and awareness of cybersecurity issues and the secure behaviours they ought to be carrying out... other researchers argue that users do not care about possible consequences, [and] are unmotivated to take responsibility," according to a 2016 study.

AWARENESS ON CYBERSECURITY AND DIGITAL LITERACY

People awareness of cybersecurity is based on their familiarity with fundamental methods for safeguarding their devices, data, and identities. The acquisition of fundamental technology and digital literacy skills can serve as the foundation for this awareness.

DIGITAL LITERACY SKILLS

The ability to use productivity tools, email, the World Wide Web, social media, collaboration tools, mobile devices, and the cloud have all contributed to the development of digital literacy skills (Dijk & Deursen, 2014; Frydenberg & Press, 2010) to online content creation, organization, sharing, and reuse, information access across devices and platforms, and online identity and privacy maintenance. When learning about cybersecurity, introductory IT courses frequently cover the importance of communicating safely online, using computers safely and responsibly, evaluating and repurposing digital content for a specific audience, and using online services responsibly; choosing, utilizing, and combining Internet services; understanding the capability of data innovation for cooperation when PCs are arranged; utilizing secure online services; recognizing that careful online identity protection is necessary in order to prevent data from persisting on the Internet; comprehending the ethical issues associated with the use of information technology.

CYBERSECURITY SKILLS

A classification model for cybersecurity-related skills is Stenmap (Mäses, Randmann, Maennel, & Lorenz, 2018). Along the horizontal axis, competencies range from non-cybersecurity-specific skills to cyber security-specific skills, and along the vertical axis, competencies range from nontechnical to technical skills. Leadership and communication abilities are examples of non-technical skills that are not specifically related to cybersecurity. These highly valued abilities are necessary for group and team activities. Quadrant 2 incorporates abilities that are network protection explicit, yet non-specialized, for example, distinguishing phishing messages or the significance of secure passwords. Coding and a fundamental understanding of browsers or the Internet are two examples of technical skills in Quadrant 3 that may not be related to cybersecurity. Implementing encryption or carrying out an SQL injection attack are two examples of the technical and cyber security-specific skills required in Quadrant 4. Mäses mentions that "positioning a skill in this Cyber sec-Tech window is not always easy." Reporting skills, for instance, could be broad and nontechnical or very specific and technical. Nonetheless, this Cyber Sec-Tech window can assist in facilitating a discussion regarding the skills that a cybersecurity exercise ought to focus on."

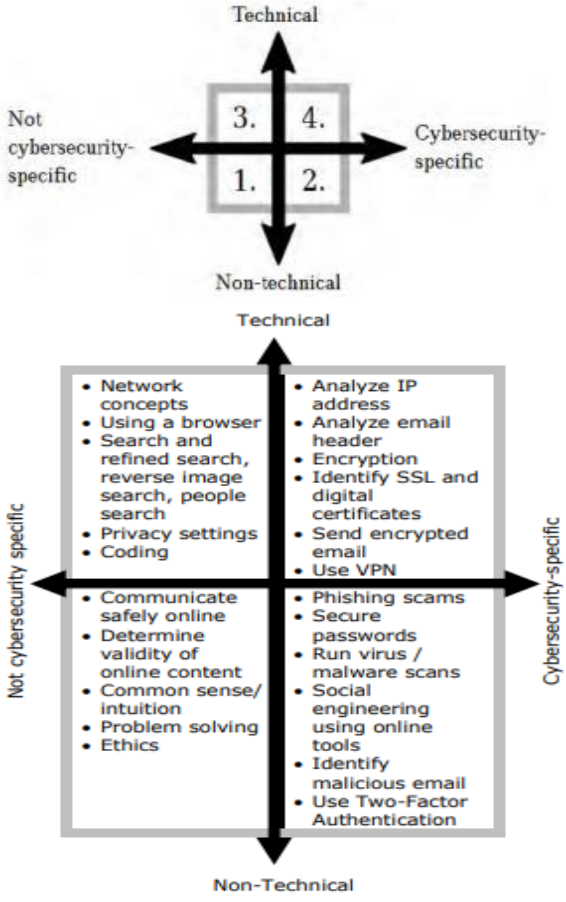

Figure. Applying Digital Literacy Competencies to Cybersecurity Skill Classifications

THE ROLE OF DIGITAL LITERACY IN GUARDIANSHIP AND PHISHING

The practice of phishing uses both "social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (Anti-Phishing Working Group 2015: 1). The manipulation of social relationships is the hallmark of social engineering phishing. A con artist might ask for private information by claiming to be the victim's friend or to be related to them professionally (a fellow researcher or an IT department employee, for instance). Fraudsters may likewise utilize mental components, for example, taking advantage of somebody's trust or submission to power (Muscanell, Guadagno, and Murphy 2014; (2008) Workman This individual may be attempting to steal identifying credentials in order to gain access to the larger computer network in large bureaucracies like universities and corporations. The manipulation of code is a characteristic of technical subterfuge phishing. For instance, a fraudster may make a site that seems to be like a real one (e.g., with a genuine organization's variety plan, logo, and sign in page plan). According to Geng, Lee, and Zhang (2014), a study, nearly 99 percent of phishing emails contain at least one type of brand entity. Phishing is also known as "brand spoofing" because of this. After that, the con artist sends an email asking for personal information. Although this tactic can also be used to gain access to a larger cache of data, its most well-known goal is to trick individual victims into providing financial institutions with login information for the purpose of theft.

INCORPORATING PHISHING IN TO EVERYDAY PRACTICES

Phishing can be broken down into two stages from the perspective of the target. First, it's possible to get an email or other communication that tries to get sensitive information from you. A "security incident" can be used to describe this initial stage. Using social engineering or technical subterfuge, the fraudster has identified one or more targets and is attempting to acquire sensitive information. This is widespread. Second, one can respond to a phishing email. For instance, the 70 contributing organizations to Verizon's 2015 Data Breach Investigations Report had a total of 79,780 security incidents.1 Information about a person's wider network, such as the login information used to access the network at their place of employment, or information specific to the individual target (such as bank account information) can be included in responses. In terms of network security, this second stage can be described as a "data breach." To proceed with the previous model, the 70 contributing associations to Verizon's 2015 Information Break Examinations Report had a sum of 2,122 affirmed information breaks. Grounding this two-stage process of targeting and victimization in the everyday activities of individuals as they navigate the digital environment is one way to think about it (Graham, 2014). This method builds on previous research in the fields of new media and communication that has identified numerous characteristics that distinguish the space created by computer networks that are interconnected (Baym 2015; 2007 Benkler; 2008 Shirky; Graham, 2014, pp. 35–50). These include the ability to connect with a wider range of social groups, a lower cost of communication, faster communication, and a high degree of pseudonymity in communications. The method focuses on how people, groups, and organizations have needed to adopt new ways of doing things to successfully navigate this new, distinct space. In terms of phishing, individual targets must learn to recognize suspicious communications as they move through the digital environment, just as pedestrians must learn to recognize context and exercise increased awareness when walking in particular neighbourhoods and at particular times. Similar to how they protect capital investments in the physical environment, organizations must adopt practices and technologies that protect their computer networks and the information they contain in the digital environment.

KNOWLEDGE OF PRIVACY AND SECURITY: SAFELY USING THE DIGITAL ENVIRONMENT

Understanding the rules governing the exchange of sensitive information is one way that targets may reduce their risk of being victimized. Herzberg (2009) records three normal pointers for secure data: the padlock symbol indicating a trusted connection, the communication protocol (http or https), and the

Uniform Resource Locator (URL). He argues that "the security of the security and identification indicators depends on users noticing, and correctly interpreting them" (65). There is also evidence to suggest that self-protection motivation may be based on knowledge of computer security. Following the collection of survey data, as Hsin-yi et al. 2016) say at the end, ". Not knowing about the dangers is enough. It matters how one responds to threats. In order to be motivated to adopt security protection behaviours, a person must be aware that he or she is responsible for their online security. In a similar vein, interviews conducted by Furnell, Tsaganidi, and Phippen (2008) demonstrate that people are aware of threats but lack the knowledge to defend themselves. Knowledge of privacy and security are both diffuse competencies that are utilized in a variety of contexts in addition to being specific competencies for the workplace. In this light we recommend that information on security and protection is a type of computerized education that enables clients to explore the computerized climate with certainty. The European Commission's report on five digital competencies, including "personal protection, data protection, digital identity protection, security measures, safe and sustainable use," aligns with this broader conception of security and privacy knowledge.

ACTIVITIES OF DAILY LIVING AND CYBERCRIME

Therefore, we see phishing as a two-stage process that is rooted in the routine activities of digital environment users. We can benefit from the insights from RAT, a situational theory of victimization that has produced a wealth of insights related to reducing the risk of victimization, by adopting this environmental approach. The central premise of RAT, first articulated by Cohen and Felson in 1979, is that "... the fundamentally human ecological nature of illegal acts as events that take place at specific points in space and time and involve particular people and/or things". In order for an offense to take place, according to RAT's predictions, a motivated offender, a suitable target, and a lack of a competent guardian are the three elements that must combine during an individual's activities. Since the theory is predicated on the existence of motivated criminals, its primary focus is on identifying suitable targets and competent guardians. Cohen and Felson (1979) recognized the impact that new technologies can have on crime rates for direct-contact predatory violations, and Felson (2006) acknowledges that the Internet provides opportunities for new crimes. Phishing research is relatively new. However, phishing has been applied to RAT in a few criminological studies. The discoveries, however, have been blended. Pratt, Holtfreter, and Reiseg (2010) examined the suitability of a target for Internet fraud, drawing on Newman and Clarke (2003). Finding out if the respondent had been an objective of Web extortion, they estimated reasonableness of focus as far as hours spent on the web and Web buys. They found that, after controlling for demographic factors, the effect of demographic factors was mediated by suitable target measures. However, Leukfeldt (2014) concluded that "there are few opportunities to aim prevention campaigns on a specific target audience, or a particularly dangerous online activity" and found no clear situational pattern in phishing. In a similar vein, Ngo and Paternoster (2011) utilized a LRAT—a combined version of RAT and lifestyles theory—and discovered no connection between phishing and situational variables. There are strong conceptual reasons to pursue phishing scholarship using a RAT approach, particularly the role of digital literacy as a means of capturing effective guardianship, despite the mixed findings in the research literature. Felson (1994, 2006) contends that the most significant guardian is not a professional crime fighter but rather an ordinary citizen with knowledge of the context. Reynald recently (2011; The concept of Guardianship in Action) deepens our comprehension of the procedures by which guardianship functions. In this context, Reynald emphasizes two aspects of guardianship that go beyond simple availability: the capacity to identify potential criminals and the willingness to intervene. She argues that monitoring the environment and being able to distinguish between those in the space who are potential offenders and those who are using the space for legitimate purposes is crucial for direct contact predatory crimes. She argues that understanding the context is necessary for this procedure because it helps identify suspicious behaviour. Reynald argues once more that knowledge is necessary for effective deterrent action in terms of willingness to intervene. In this instance, this knowledge serves as the foundation for comprehending the individual's role in preventing crime and its nature. The two-stage phishing process

that we have previously modelled roughly corresponds to this process. For both Felson (2006) and Reynald (2009, 2010, 2011), guardianship has a wider impact than merely being present or available. It depends on understanding the context. Most importantly, Vakhitova and Reynald (2014) argued recently that the concept of Guardianship in Action can be used in cyberspace. "Contextual awareness could be evident in the guardian's understanding of the rules of conduct, ability to recognize prohibited behaviours, ability to distinguish between offenders and complaint users, general technological competency, and ability to locate and use help to protect oneself and others from risks associated with cyberspace," they write (2014:158). Importantly, they argue that contextual awareness of cyberspace helps determine whether the guardian will intervene and identify potential offenders. The term "cyber guardianship" is defined as "a presence of a human third party capable of deterring the would-be offenders from committing a crime against an available target or acting to disrupt crime events in progress" (2014:159). They investigate the role of contextual awareness in witnessing and intervening in two forms of cyber abuse—cyberstalking and cyber harassment. They found that 19% of the sample had been a victim of cyber-abuse, 40% had witnessed cyber-abuse, and 41% had intervened. Contextual awareness was measured as awareness of anti-cyber-abuse policies, methods of reporting cyber-abuse, perceived level of computer competency, and prior victimization. Vakhitova and Reynald (2014) observed that witnesses were essentially more PC equipped, however not interveners. However, interveners were significantly more likely to be aware of policies against abuse. Witnessing and intervening in cyber abuse were significantly influenced by previous victimization.

RESEARCH QUESTIONS

Phishing, in our view, is a two-stage process that is rooted in the everyday activities of digital environment users. With this assumption as our starting point, we want to investigate how this process is influenced by digital literacy, or knowledge of privacy and security. We have chosen RAT as our theoretical framework in this setting. Our two exploratory inquiries are as follows: 1) How does digital literacy affect the likelihood of receiving a phishing email? We can look into this effect in terms of its magnitude—how strong it is—and its direction—a positive or negative association.

2) How does digital literacy affect how a person responds to a phishing email? In a similar vein, we can investigate this effect in terms of magnitude and direction (positive or negative association).

DATA AND METHODS

Data

The American Association of Retired Persons (AARP) commissioned a nationally representative survey in 2013 to provide the data for this study. 11,741 people made up the initial sample. From November 2013 to December 2013, the sample was taken. With a 3.1% error rate, the completion rate was 51.3%.

VARIABLES

Dependent variables

There are two dichotomous ward factors for this review — one estimating respondents' report of getting a phishing email and the other estimating respondents' reports of answering a phishing email. From this prompt about phishing scams, both can be derived:

Following this prompt, a number of questions were posed to respondents, two of which were: "Did you receive such an email?" and "Did you respond to such an email?" There was a total of 11,534 responses regarding receiving a phishing email. Out of this aggregate, 3,666 (32%) revealed they had gotten a phishing email, 7,735 (67%) detailed they had not gotten a phishing email, and 133 (1%) would not reply. Of the 3,666 people who said they had received a phishing email, 64 (2%) said they had responded, 3,578 (98%) said they didn't respond, and 24 people said they wouldn't answer.

Independent variables

Similar to studies done in the past (Holt and Bossler, 2009; Ngo and Paternoster 2011), we utilize various measures to catch the three components of routine exercises hypothesis. The appropriate target dimension is reached by two measures. The capable guardian dimension is tapped into by the third measure. The primary variable of interest is digital literacy, which is this capable guardian measure. The principal proportion of appropriate objective is the time one spends on the web, or Web Recurrence. For

time, respondents were asked, "Approximately how many hours do you spend on the Internet or email per day?" less than one hour, one to three hours, three to six hours, six to ten hours or more, ten hours or more? We measure this variable at the ostensible level, and five gatherings are made. The number of online activities, or Internet Variety, is the second metric. Internet variety is a count variable that measures a person's reported online activities. Eighteen activities served as the foundation for the test. With a mean of 10.09 and a standard deviation of 3.94, this scale had a range of 0 to 18. A reliability analysis was conducted to assess the scale's internal consistency and yielded a very acceptable alpha score of 0.83. Respondents were asked 11 true-false questions about Internet security and privacy for Digital Literacy, a guardianship measure. There could be "true," "false," or "not-sure" responses. Correct responses were coded 1 and incorrect responses were coded 1. There were two reasons why responses were coded in this way. We argue that, theoretically speaking, a victimized individual is more likely to be wrong about digital literacy than a sceptic. As a result, the code for the incorrect answer is "1" and the code for the unsure answer is "0." It was necessary for us to distinguish between these two distinct phenomena. We were able to increase the range of responses on our digital literacy scale without losing any data by including those who were unsure. Adding these reactions created a unique scale going from −9 to 11, to which 9 was added to all scores to make the base score 0. The digital literacy scale has a mean score of 13.16 and a standard deviation of 3.66, ranging from 0 to 20. A reliability analysis was conducted with an alpha score of 0.65 to assess the scale's internal consistency.

Control variables

Control variables include standard demographic variables. Age, race, education, gender, and income are all factors. There are 19 response categories for income, ranging from 1 (less than $5,000) to 19 (more than $175,000). Gender is a binary variable where 1 indicates males and 0 indicates females. From less than high school to post-baccalaureate education, education is a series of dichotomous variables. A set of dichotomous variables that include White, African American, Hispanic, and Asian people are used to define race. Lastly, the age range is 18 to 93. As a final control variable, a self-control scale is also included. According to Gottfredson and Hirschi (1990), individuals who lack self-control are more likely to engage in impulsive behaviours. The likelihood of receiving and responding to a phishing email can be increased by impulsivity. A person who lacks self-control is more likely to provide contact information without thinking about the consequences, which could eventually result in receiving a phishing email. In addition, a person who lacks self-control may not take the time to verify the authenticity of a phishing email, resulting in fraud. Phishing and self-control have been the subject of mixed research. While Ngo and Paternoster (2011) have not, Bossler and Holt (2010) and Higgins (2005) have discovered evidence of a relationship. In this study, however, we control for its effects due to the self-control's robustness in explaining various forms of crime. Respondents were asked, "I'm going to read some statements some people make about attitude and behaviour in general," in a series of five questions. Tell me how strongly you agree or disagree with each statement after considering your own attitudes and behaviour. I do things that are bad for me, even when they are fun, "I often do things without considering all the alternatives," "I don't mind taking risks with my money, as long as I think there's a chance it might pay off," "I enjoy making risky financial investments occasionally," and "There's no sense planning a lot—if something good is going to happen, it will." The idea of self-control is brought up in these statements. The responses included "strongly disagree," "somewhat disagree," "neither agree nor disagree," and "strongly agree."

ANALYSIS

Bivariate

For Internet Variety and Digital Literacy, T-tests are used (Table). For both the Internet variety and digital literacy scale, there were significant differences between those who had received a phishing email and those who had not. The average scores for Internet variety and digital literacy for those who received these emails were 11.18 and 14.32, respectively, compared to 9.57 and 12.61 for those who did not. There were no significant differences between groups in Internet variety when it came to responding to phishing emails. However, respondents' scores for digital literacy were significantly lower—12.32 compared to 14.36. Significant differences between groups with varying levels of Internet Frequency were

found using the chi-square test (Table). For both not responding to a phishing email and receiving one, the Internet Frequency groups were significantly different.

Table: Bivariate statistics

Phishing	Internet variety	Digital literacy
Receiving	11.18	14.32
Responding	11.17	12.32

THE SIGNIFICANCE OF SOCIAL STANDING

The likelihood of receiving a phishing email increases when a person has higher incomes, is male, Hispanic, has a higher level of education, or is older. Considering that these tremendous contrasts hold controlling for the power of Web movement (caught by the normal exercises measure), the best comprehension of these connections is that respondents with these segment profiles, aside from being Hispanic, are in settings that are practical objectives for fraudsters. Our interpretation of this finding is that respondents in these social positions are more likely to encounter motivated criminals and to navigate the digital environment more frequently than others. Males with more money and education are more likely to work in computer network-intensive white-collar jobs. These organizations either own valuable resources (like banks or military organizations) or gather wealthy individuals into a single network. It is suggested that when looking into phishing victims, social position and online time produce suitable targets.

CONCLUSION

Started this study assuming that networked computer technologies create a unique social environment. It was able to apply the insights from routine activities theory and claim that digital literacy is a form of personal guardianship that can keep users safe from phishing as they use the internet. This assertion is supported by our findings. These results look promising. Phishing and other forms of cybercrime may be combated through a potential mechanism that they point to. Simply put, it is simpler to alter a population's level of digital literacy through education. In routine activities theory, the motivated offender and the appropriate target are not as variable as the other factors. In the near future, there will not be a shortage of motivated criminals. According to Holt and Copes (2010), the prevalence of less technologically savvy fraudsters, like digital piracy, will increase as society's knowledge of computers grows. Suitable targets—the individuals who are the focus of phishing attacks will also continue to rise. Indeed, as more devices and workplaces become networked, as well as more personal information is uploaded to the internet, there will be more opportunities to breach these networks and obtain sensitive information by targeting individuals. However, it is possible to instruct individuals to recognize phishing emails and respond accordingly. We highlight some limitations of our research. The purpose of the data we used in this study was not to measure levels of digital literacy but rather patterns of cybercrime victimization. As a result, as a means of assessing digital literacy, we posed a series of inquiries regarding comprehension of privacy and security concepts. To better comprehend the impact of digital literacy on phishing, a more extensive test is required. Additionally, research is required to decipher the relationship between being able to report receiving a phishing email and having knowledge of phishing. This might require exploratory examinations that have some control over for this potential jumble. Based on our findings, we offer policy recommendations as a conclusion. Currently, the majority of online security measures are commercial. Security professionals can be hired by businesses, or they can buy technological defences like spam filters and computer algorithms that can find phishing emails. According to Yar (2013), this means that policing cybercrimes in the digital environment is much more privatized than policing crimes in the real world. Personal home networks, on the other hand, do not have the luxury of employing these experts, and they may not be able to spend their hard-earned money on the most recent technological enhancement. In high schools and colleges, digital literacy courses can be offered as general education or electives. These establishments already possess the resources necessary to provide such courses. Although this is a fairly insignificant measure, it has the potential to significantly contribute to the development of capable guardians and the reduction of phishing victims.

REFERENCE

[1] Anti-Phishing Working Group. 2015. "Phishing Activity Trends Report 4th Quarter 2014." Retrieved January 8, 2016.

[2] Baym, Nancy K. 2015. Personal Connections in the Digital Age. Malden, MA: Polity Press.
[3] Benkler, Yochai. 2007. The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven, CT: Yale University Press.
[4] Bossler, Adam and Thomas Holt. 2010. "The Effect of Self-Control on Victimization in the Cyberworld." Journal of Criminal Justice 38(3):227–236.
[5] Brooke, Tom Vanden and Michael Winter. 2015. "Hackers Penetrated Pentagon Email." USA Today. Retrieved January 18, 2016.
[6] Furnell, Steven, Valleria Tsaganidi, and Andy Phippen. 2008. "Security Beliefs and Barriers for Novice Internet Users." Computers and Security 27(7–8):235–240.
[7] Geng, Guang-Gang, Xiao-Dong Lee, and Yan-Ming Zhang. 2014. "Combating Phishing Attacks via Brand Identity and Authorization Features." Security and Communication Networks 8(6):888–898.
[8] Graham, Roderick. 2014. The Digital Practices of African Americans: An Approach to Studying Cultural Change in the Information Society. New York: Peter Lang Publishing.
[9] Herzberg, Amir. 2009. "Why Johnny Can't Surf (Safely)? Attacks and Defences for Web Users?" Computers and Security 28(1–2):63–71.
[10] Muscanell, Nicole L., Rosanna E. Guadagno, and Shannon Murphy. 2014. "Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams." Social and Personality Psychology Compass 8 (7):388–396.
[11] Ngo, F. T. and Raymond Paternoster. 2011. "Cybercrime Victimization: An Examination of Individual and Situational Level Factors." International Journal of Cyber Criminology 5: 773–793.
[12] Workman, Michael. 2008. "Wise crackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security." Journal of the American Society for Information Science and Technology 59(4):662–674.
[13] Yar, Majid. 2013. Cybercrime and Society. 2nd ed. Thousand Oaks, CA: Sage.
[14] Zhang, Yanping, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, and Hongmei Deng. 2011. "A Survey of Cyber Crimes." Security and Communication Networks 5(4):422–437.