https://doi.org/10.48009/2_iis_2020_1-8
Issues in Information Systems
Volume 21, Issue 2, pp. 1-8, 2020

PREVENTION OF PHISHING ATTACKS: A THREE-PILLARED APPROACH

Bryon Miller, Northeast Alabama Community College, millerb@nacc.edu
Katelin Miller, University of North Alabama, kmiller14@una.edu
Xihui Zhang, University of North Alabama, xzhang6@una.edu
Mark G. Terwilliger, University of North Alabama, mterwilliger@una.edu

ABSTRACT

This paper presents a three-pillared strategy for the prevention of phishing attacks. Phishing is a deceptive method of creating and distributing emails and/or websites that attempt to fool users into sharing sensitive financial or identification information. Current literature agrees that these scams can be highly damaging to companies, their employees, and their stakeholders. Unlike traditional scams, though, the Internet adds a layer of anonymity and even invisibility, making it far more difficult to identify the source of the scam, or, in some cases, masking the fact that a scam has been perpetrated. In this paper, we first review information about tactics that can effectively reduce the success rate of phishing attempts. We then formulate a three-pillared prevention strategy based on: (1) one-time passwords, (2) multi-level desktop barrier applications, and (3) behavior modification. By utilizing this approach, individuals and organizations should be better able to protect their information and decrease the damage caused by phishing attacks.

Keywords: Phishing, Data Privacy, Cybersecurity, One-Time Passwords, Barrier Applications, Behavior Modification

INTRODUCTION

"Phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity" (Jagatic et al., 2007, p. 94). Typically, an email is sent with a link to a fake website that replicates the real one. Sometimes successful attempts have simple remedies and other times they create newsworthy disasters for a business and its stakeholders.

Phishing is economically motivated (Berghel 2006). According to the US Federal Bureau of Investigation (Jensen et al., 2017), thousands of people are victims of phishing attempts each month with billions of dollars in losses. Young and old, entry-level and top management, male and female, all are susceptible and have fallen prey to these attempts. While it is true that the Internet has created great opportunities for businesses to thrive and improve their processes, it has also put millions of users' identifiable financial and personal information at risk (Wright & Marett, 2010). "Bait-and-hook" phishing attempts successfully display the vulnerabilities of users every day. These vulnerabilities make researching defenses against phishing attempts worthwhile.

According to Bose and Leung (2009), the phases of a phishing attack include: (1) preparation: identify target companies for phishing and explore potential system vulnerabilities; (2) mass broadcast: spread phishing message to the public; (3) mature: wait for victims to respond to phishing messages; and (4) account hijack: conduct identity theft to cause financial loss to victims. Berghel (2006) maintains that the essential requirements of effective phishing are as follows: (1) look real; (2) present itself to an appropriate target-of-opportunity; (3) satisfy the reasonableness condition; (4) cause the unwary to suspend any disbelief; and (5) clean up after the catch.

Despite our best efforts, current automated prevention techniques fall short and quickly become outdated (Jensen et al., 2017). Therefore, new strategies should be implemented to address this need. There is much to be learned from current research on phishing prevention and this information can be consolidated into a three-step plan of action for managers and end-users to protect themselves and their businesses.

LITERATURE REVIEW

Aside from discussing the prevalence of phishing attempts and the consequences of these attacks, current literature also explores techniques that may protect against them. Friedman and Hoffman (2008) provide a taxonomy that divides threats to mobile devices into seven categories, with phishing and social engineering being one of them. They describe phishing and social engineering attacks as attempts to dupe computer users into either sending confidential information to third parties or downloading malware. They suggest that educating computer users and filtering for malicious content or spam are the two major defense mechanisms against phishing and social engineering.

According to LaRose et al. (2008), online safety is everyone's responsibility. Their experimental findings suggest that "improving user responsibility for overall online safety is a desirable and achievable goal" (LaRose et al., 2008, p. 76). Wang et al. (2016) examined user overconfidence, which can lead to failure to detect e-mail based phishing attempts. Results from a survey experiment with 600 subjects show that cognitive effort decreases overconfidence, while variability in attention allocation, dispositional optimism, and familiarity with the business entities in the emails all increase overconfidence.

Wright and Marett (2010) studied how three experiential characteristics (i.e., self-efficacy, web experience, and knowledge of appropriate security policies) and three dispositional characteristics (i.e., disposition of trust, perceived risk, and suspicion of humanity) of online users affect their susceptibility to potentially malicious phishing emails. Their research results indicate that experience and training are the most effective tools for guarding against phishing.

Ference (2017) suggests that we approach any email from an unknown source with suspicion. Red flags may include: (1) a mismatch between the displayed URL and the actual hyperlinked web address, which we can detect by hovering over the link without actually clicking on it; (2) use of poor spelling or grammar; (3) use of urgent or threatening language; (4) suspicious domain names in email headers; (5) requests for personal information; or (6) offers that seem too good to be true.

Musuva et al. (2019) showed how an organization can stage naturalistic field experiments to identify susceptibility to social engineering through phishing attacks. O'Leary (2019) used text analysis to determine if a neural network was able to distinguish between phishing emails and a database of Enron emails.

Workman (2008) presented a theory-grounded investigation of phishing and pretext social engineering threats to information security. He concluded that training should be seen as an important component in dealing with social engineering. It was also suggested that "training should mitigate by first making employees aware, and second in developing new coping behaviors" (Workman, 2008, p. 671). Perhaps our greatest mistake is excessive reliance on technology solutions; when it comes to email, common sense still goes a long way (Berghel, 2006).

As with many other complex issues, a quick and simple solution is not always enough. In the case of phishing attempts, this is true. Each of the methods discussed above offers a single approach to minimizing the impact of phishing attempts. A wise company will note, however, that if one method is successful, two or three will be more successful. Therefore, we would like to suggest an integrated and redundant approach to counter phishing attacks. Taking this approach will allow organizations and individuals to better protect their information and decrease the damage caused by these attacks.

A THREE-PILLARED PREVENTION APPROACH

Three of the more popular approaches to combat phishing attacks include: (1) one-time passwords to be a successful tool for phishing protection, (2) multi-level desktop barriers, and (3) behavior modification. These three pillars are illustrated in Figure 1 and are described next in more detail.

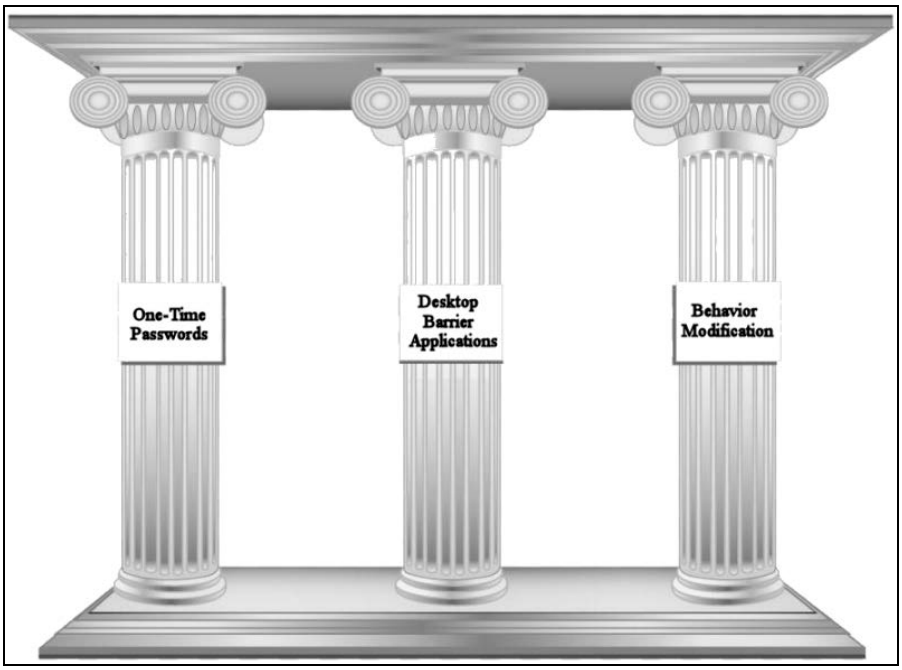

Figure 1. Three-Pillared Approach for Phishing Prevention

One-Time Passwords

A one-time password (OTP) is a commonly used method for securing online systems (Nasiri et al., 2017). An OTP is essentially a short-term password that is generated as needed and is no longer effective after the first use. It is typically a random-looking assortment of numbers and/or letters, and will automatically expire if not used within a relatively short period of time. An OTP forces a user to take another step in addition to entering a user name and password. Even if a scammer is able to obtain a user's password, they are usually unable to pass the second authentication step. According to Hickey (2018), scammers can so easily prey on emails, user names, and passwords. Therefore, having a secondary authentication is one of the best practices to keep user information safe.

Hwang et al. (2015) propose an OTP system that utilizes Short Message Service, or SMS. In their model, an SMS message is sent to the customer at the time he or she is ready to complete a transaction. If the customer fails to enter the OTP within a specified time interval, the transaction is rejected. It is common today for customer transactions with banking, stocks, taxes, etc. for an institution to send an OTP for verification using an SMS message or email.

The main concerns with this strategy are user-based, rather than security-based. For example, a customer could misread the OTP and be forced to repeat the confirmation process. Similarly, if the customer is too slow in entering the OTP, the system could time out, forcing the process to be repeated. Sometimes, companies elect against OTP usage because of the inconvenience it causes customers. The OPT, however, offers extreme system security with a minimal likelihood of hacking able to take place (Hwang et al., 2015). Customers may be inconvenienced, but they can have peace of mind that their information is secure.

Multi-Level Desktop Barrier Applications

Kaur and Kalra (2016) propose a five-level desktop barrier application designed to prevent users from opening suspicious webpages. Phishers are motivated by recognition, monetary gain, or identity improvements (Kaur & Kalra, 2016). Multi-level desktop barrier applications can detect these motivations as weaknesses. This aids in preventing the phishing attempts from being successful.

The five barriers proposed by Kaur and Kalra (2016) include:

1) Verification barrier: Essentially a whitelist in which suspicious webpages are checked against to find potentially dangerous sites.
2) Text field barrier: Raises suspicion and alerts anytime an insert text field is found within the webpage. This leaves an open door for secure information to pass through to a potential scammer.
3) The anchor tag endorsement barrier: Detects the existence of hyperlinks against the existence of text fields. There is cause for alarm if a website has a text field such as a login form (as found in the text barrier phase), but with no hyperlink such as 'login', 'sign up', or 'forgot password' leading a user elsewhere.
4) The null (#) link barrier: Tracks links directing to its own webpage, which raises red flags because the phisher typically wants to try to keep the user on the susceptible page for as long as they can in order to contract large amounts of information from them.
5) Webpage identity barrier: Analyzes the structure of the hyperlink and how frequent a hyperlink points to the webpage's own domain. Many phishers use hyperlinks with different domains to conduct their scam (Kaur & Kalra, 2016).

These barriers do not rely on human behavior, but rather attempt to predict the possible mistakes that humans can make and put a stop to the phishing before it happens.

Behavior Modification

In addition to relying on the software-based strategies described above, users must be educated to recognize potential phishing attacks. The most common and widely accepted method for reducing the success rate of phishing attempts is behavior modification. This can be challenging, because behaviors can be very difficult to change. Lim et al. (2016) suggest that users be educated on the psychology of phishing attempts, as well as the techniques that are used.

Behavior modification may begin to prioritize training for all employees, but efforts should also be made to identify employees who are most susceptible to clicking on a phishing email. People belonging to various demographics may be more susceptible to phishing scams. For example, Metzger et al. (2003) found that students rely more on information from the Internet and that they do not verify the information as often as non-students. Age also appears to be an important factor. Another study finds that "women and people between 18 and 25 years old were less suspicious of phishing than people of other ages" (Gavett et al., 2017, p. 2). Organizations can use a number of techniques to help identify those demographics that are most susceptible, including the use of fake phishing scams, using questionnaires to test employees' security knowledge, and reviewing the number of actual phishing attempts made on certain individuals or departments.

It will also improve training if managers and information technology (IT) staff recognize the thought processes that lead to risky behaviors. For example, research has shown that people are more susceptible to phishing when they process information by paying closer attention to elements in the email such as company logos, phone numbers, or signatures (Harrison et al., 2016).

Managers and IT staff also need to teach their employees to identify phishing scams by looking for typical signs, including misspellings, a high sense of urgency, threats, generic salutations or signatures, and requests for personal or work-related information (Lungu & Tăbuşcă, 2010). When employees are trained to recognize these signs, they are less likely to open the emails or to click on phishing links.

Wright et al. (2010) tested Grazioli's Theory of Deception as an explanation for the process utilized to detect phishing attempts. The results from both the statistical testing and the interview data analysis confirmed and added to the Model of Deception Detection. Their study showed that both a user's disposition to trust and their web experience can directly impact phishing detection. They emphasize that training and education are critical to combat online deception.

The identification of common features shared by most e-mail based phishing attempts is the focus of Bergholz et al. (2010). They use statistical analyses to identify low dimensional descriptions of topics, as well as sequential analysis of e-mail text and external links. They also look at embedded logos as possible evidence of "hidden salting." This is

defined to be the addition or distortion of content that is not visible to the reader. In experiments, their methods outperform other published approaches to identify phishing e-mails.

Using an approach based on design science, Abbasi et al. (2015) proposed a novel strategy to detect phishing websites. They call their approach the genre tree kernel. It uses fraud cues that are associated with differences in purpose between legitimate and phishing websites. The results from a series of experiments indicated that the proposed method provided significantly better detection capabilities than state-of-the-art anti-phishing methods.

Heartfield and Loukas (2016) present a taxonomy of semantic attacks and a survey of applicable defenses. They divide the mitigation techniques into two major categories. The first is organizational, which includes policy and process control and awareness training. The second is technical, and includes sandboxing mechanism; authorization, authentication, and accounting (AAA); monitoring; integrity checking; and machine learning. Florêncio et al. (2016) conclude that "harder-to-guess passwords do not always reduce the likelihood of successful guessing attacks," and they suggest that "enterprises should focus on users with the most easily guessed passwords" (p. 66).

Jensen et al. (2017) maintain that regular repetition of rule-based training may not yield increasing resistance to phishing attacks. They developed a novel training approach that can be performed after individuals are familiar with rule-based training, using the mindfulness theory. "The mindfulness approach teaches individuals to dynamically allocate attention during message evaluation, increase awareness of context, and forestall judgment of suspicious messages - techniques that are critical to detecting phishing attacks in organizational settings, but are unaddressed in rule-based instruction" (Jensen et al., 2017, p. 598). At one American university, a field study was conducted that involved 355 students, faculty, and staff who were familiar with phishing attacks and received regular rule-based guidance. They found that participants who received mindfulness training were better able to avoid phishing attacks.

The research results of Goel et al. (2017) reveal that contextualizing messages to appeal to recipients' psychological weaknesses increased their susceptibility to phishing. Specifically, "the fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing" (Goel et al., 2017, p. 22). Their findings suggest "the need to identify the precise vulnerabilities based on demographic groups and provide targeted education designed for each group" (Goel et al., 2017, p. 37).

Sarika and Paul (2017) present the design and evaluation of an agent-based anti-phishing method to identify phishing websites. The results show that their proposed method outperforms the state-of-the-art phishing detection methods and achieves an accuracy of 97.3%. Sebescen and Vitak (2017) evaluated how three sets of employee characteristics (demographic, company-specific, and skills-based) can be used to predict an employee's likelihood of becoming a security breach victim. They analyzed four risk categories concurrently: phishing, passwords, bring your own device (BYOD), and company-supplied laptops. Their findings suggest that "organizations must consider all security threats and their interconnected nature when developing strategies to increase employee knowledge and compliance and decrease security threats" (Sebescen & Vitak, 2017, p. 2246).

A malicious website is a foundation mechanism for cybercrimes such as phishing, spamming, identify theft, financial fraud, and malware. Vinayakumar et al. (2018) evaluated various deep learning architectures used in detecting malicious URLs and found that deep learning mechanisms outperformed the hand-crafted feature mechanism. Specifically, the deep learning architectures such as long short-term memory (LSTM) and a hybrid network of convolution neural network (CNN) and LSTM achieved the highest accuracy at 99.96% and 99.95%, respectively.

Canfield and Fischhoff (2020) propose an application based on a Monte Carlo simulation. Their system has three steps: (1) identify poor detectors, (2) assess system vulnerability due to poor detectors, and (3) perform a benefit-cost analysis. Silic and Lowry (2020) created a gamified security training system to address two organizational issues: (1) unsuccessful employee phishing prevention and (2) poorly received internal security training. Miranda (2018) developed a structured and comprehensive phishing exercise training program and showed that this program (along with email security technology) can be used to reduce cybersecurity risks originating from fraudulent emails.

Since interactive training is often more effective than reading material or sitting through a seminar, trainers are encouraged to simulate phishing scams and educate employees on how to identify them. When discussing the results

of their simulated phishing exercise, Jansson and von Solms (2013) state that "a simulated phishing attack together with embedded training can contribute towards cultivating users' phishing resistance as this approach reduces the user's risk of becoming a victim to any future phishing attack" (p. 591). This evidence seems to support the notion that simulation and interactive training is one tool for effectively altering behaviors associated with phishing attacks and responses to them.

IMPLEMENTING THE THREE-PILLARED APPROACH

In our three-pillared integrated approach (see Figure 1), there are options and flexibility as to how each pillar is implemented. For example, a firm could implement an OTP-based system by having all employees utilize two-step authentication for their work accounts. This could be accomplished by using a USB-key or authentication via a second device such as a smartphone. This step will ensure that, even if login information is stolen, it will be much more difficult to log in to the accounts without the second form of authentication.

In the second step, users can implement Kaur and Kalra's (2016) multi-tiered desktop barrier algorithm via a Google Public DNS. As explained in their article, this will protect the user by thoroughly evaluating URLs of links they click on regardless of where they originated and will alert them when the URLs are illegitimate (Kaur & Kalra, 2016). The algorithm is thorough enough that many scams will be prevented by this step alone. It will also protect the user from falling prey to seemingly legitimate sites that actually contain traps set to steal their information.

Finally, an organization should educate and prepare employees for potential dangers. Understanding what to look for, how to report phishing attempts, and how to use the first two steps appropriately will be essential pieces to our integrated approach. While behavior modification can be one of the most powerful tools for prevention, it can also be one of the hardest to implement successfully. We suggest that the organization offer mandatory training for employees to learn about each of these aspects as well as interactive anti-phishing training sessions. Training could be implemented on a monthly, quarterly, or yearly basis. While more research needs to be conducted to determine the most effective amount and frequency of training, it is certain that new employees should receive it as soon as possible and other employees should receive training refreshers at least once per year.

CONCLUSION

Research suggests there are many different methods for the prevention of phishing attacks. We conclude that with a combination of automated techniques such as one-time passwords and multi-level barrier applications, along with human behavior modification, we can successfully reduce the likelihood of being preyed upon by phishers. "While many users are vulnerable to the phishing attacks, playing catch-up to the phishers' evolving strategies is not an option" (Qabajeh et al., 2018, p. 10). With phishing attempts having such a short, deadly lifespan, it is almost impossible to catch up to them. With a combination of different defense techniques, though, we can contest these attacks effectively. Organizations should be compelled to use one-time passwords, include a type of barrier application in their systems, and to do their due diligence in educating and training their employees to recognize and avoid phishing scams.

REFERENCES

Abbasi, A., Zahedi, F., Zeng, D., Chen, Y., Chen, H., & Nunamaker, J. F., Jr. (2015). Enhancing predictive analytics for anti-phishing by exploiting website genre information. *Journal of Management Information Systems, 31*(4), 109-157.

Berghel, H. (2006). Phishing mongers and posers. *Communications of the ACM, 49*(4), 21-25.

Bergholz, A., Beer, J. D., Glahn, S., Moens, M.-F., Paaβ, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of Computer Security, 18*(1), 7-35.

Bose, I., & Leung, A. C. M. (2009). What drives the adoption of anti-phishing measures by Hong Kong Banks? *Communications of the ACM, 52*(8), 141-143.

Canfield, C. I., & Fischhoff, B. (2020). Setting priorities in behavioral interventions: An application to reducing phishing risk. *Risk Analysis*, *38*(4), 826-838.

Ference, S. B. (2017). The armor of awareness. *Journal of Accountancy*, *223*(3), 1-3.

Florêncio, D., Herley, C., & van Oorschot, P. C. (2016). Pushing on string: The 'don't care' region of password strength. *Communications of the ACM, 59*(11), 66-74.

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7*(1/2), 159-180.

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE, 12*(2), 1-16.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of Association for Information Systems*, *18*(1), 22-44.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, *40*(2), 265-281.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 37.1-37.39.

Hickey, M. C. (2018). Protect yourself from these 7 scams. *Consumer Reports*, *83*(6), 26.

Hwang, J., Hsu, Y., & Liao, G. (2015). An SMS-based one-time-password scheme with client-side validation. *Journal of Digital Information Management*, *13*(2), 69-75.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

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

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Kaur, D., & Kalra, S. (2016). Five-tier barrier anti-phishing scheme using hybrid approach. *Information Security Journal: A Global Perspective*, *25*(4-6), 247-260.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM*, *51*(30), 71-76.

Lim, I., Park, Y., & Lee, J. (2016). Design of security training system for individual users. *Wireless Personal Communications*, *90*(3), 1105-1120.

Lungu, I., & Tăbușcă, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. *Informatica Economica*, *14*(2), 27–36.

Metzger, M. J., Flanagin, A. J., & Zwarun, L. (2003). College student Web use, perceptions of information credibility, and verification behavior. *Computers & Education*, *41*(3), 271–290.

Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10.

Musuva, P. M. W., Chepken, C. K., & Getao, K. W. (2019). A naturalistic methodology for assessing susceptibility to social engineering through phishing. *African Journal of Information Systems*, *11*(3), 157-182.

Nasiri, S., Sharabian, M. T., & Aajami, M. (2017). Using combined one-time password for prevention of phishing attacks. *Engineering, Technology & Applied Research*, *7*(6), 2328-2333.

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44-55.

O'Leary, D. E. (2019). What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis. *Journal of Information Systems*, *33*(3), 285-307.

Sarika, S., & Paul, V. (2017). Parallel phishing attack recognition using software agents. *Journal of Intelligent & Fuzzy Systems*, *32*(5), 3273-3284.

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, *68*(9), 2237-2247.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129-161.

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Evaluating deep learning approaches to characterize and classify malicious URL's. *Journal of Intelligent & Fuzzy Systems*, *34*(3), 1333-1343.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 759-783.

Workman, M. (2008). Wisecrackers: 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.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision & Negotiation*, *19*(4), 391-416.