12-12-2020

Improving Cybersecurity Behaviors: A Proposal for Analyzing Four Types of Phishing Training

Alanah Mitchell

Improving Cybersecurity Behaviors: A Proposal for Analyzing Four Types of Phishing Training

Alanah Mitchell[1]
Department of Information Management and Business Analytics
Drake University
Des Moines, IA, USA

ABSTRACT

Phishing is an attack on organizational data that involves employees. In order to prepare for these attacks some safeguards can be put into place, but ultimately employees need to be trained in how to identify and respond to phishing attacks. There are a number of different methods that can be used for employee phishing training, but are these methods effective? This proposal presents a plan to analyze the effectiveness of four different types of organizational phishing training in order to determine which types of phishing training methods are effective.

Keywords: information security, cybersecurity behaviors, training, phishing, deception, email communication.

INTRODUCTION

Information security is an organizational priority that requires the support of organizational leaders (Bansal 2018; Burns 2019). A key challenge to information security is the concept of phishing, which continues to be a persistent challenge for today's organizations causing impact through financial loss or data breaches (Bose and Leung 2007; Firstbrook and Wynne 2018; Hong 2012). In general, *phishing* takes place when an adversary sends emails enticing users to click on links to false websites in order to capture usernames and passwords (Bose and Leung 2007) thus taking advantage of people, the weakest link in the security chain

[1] Corresponding author. alanah.mitchell@drake.edu +1 515 271 3724

(Goel, Dennis, et al. 2017). Previous research has noted cybersecurity attacks, including phishing, are increasing and has highlighted the importance of understanding why people fall victim to phishing and how these types of attacks can be prevented (Anderson et al. 2013; Jensen et al. 2017; Sen 2018).

In order to protect an organization from phishing attacks there are some safeguards that organizations can put into place. For example, organizations can use anti-spam filters (Bose and Leung 2007), sender identification verification on secure email gateways (Firstbrook and Wynne 2018), or other types of anti-phishing solutions. However, technological controls (such as firewalls, encryption, certificates, two-factor authentication, and others) will not help an organization stay safe if their employee falls for a phish (Hong 2012). Ultimately, employees need to be trained in how to identify and respond to phishing attacks (Ohaya 2006). In fact, Gartner recommends anti-phishing education as a critical part of an organization's email security (Firstbrook and Wynne 2018). Furthermore, some research has suggested that understanding and protecting against phishing is a necessary part of individual and corporate social responsibility (Bose and Leung 2007).

According to the 2020 Verizon Report, phishing is the top action for organizational data breaches with 22% of breaches credited to phishing ("DBIR" 2020). With phishing identified as the leading cause of data breaches, it is critical to understand the most effective methods for employee training related to phishing. Understanding the most effective type of phishing training program for improving employee responses to phishing is critical to both research and practice. Therefore, this proposal presents a plan to analyze the effectiveness of four different types of organizational phishing training in order to determine which types of phishing training methods are effective.

The following sections present background on the concept of phishing and related research, followed by the methodology plans for this study. This proposal concludes with a discussion of the possible implications from this work.

BACKGROUND

The term phishing first appeared in the late 1990s and is based on the concept of using bait to allure individuals (Bose and Leung 2007). The most common use of phishing is related to email communications (Bose and Leung 2007), however phishing has extended to deceptive websites (Abbasi et al. 2015) and even gaming (Hong 2012). Phishing attacks can be targeted or directed at specific individuals or groups in the form of *spear phishing* or even directed towards an organization's senior executives in the form of *whaling* (Butavicius et al. 2015).

Phishing messages are primarily sent from cybercriminals knows as *phishers* (Jensen et al. 2017) and generally involve three key steps: 1) an act of deception in which a user receives a phishing email enticing them to respond, 2) the user is motivated to click on a link and evaluate what is shown, and 3) a user is ultimately convinced to share personal information with an adversary (Goel, Williams, et al. 2017). Previous research on phishing has suggested the method is able to work as phishing exploits basic human emotions including fear, greed, curiosity, and even patriotism (Goel, Williams, et al. 2017). However, other reasons employees fall for phishing include lack of systems knowledge, lack of security and/or security indicators, lack of attention to security and/or security indicators, and the sophistication of phishing attacks (Ohaya 2006).

Research has suggested that there have not been many studies focused on anti-phishing training (Kumaraguru et al. 2009) and training has been cited as the least popular approach for protecting organizational data from phishing due to the challenges of motivating users to be

secure (Hong 2012). However, prior research has found that appropriate training can improve an individual's ability to detect deception through the use of e-training methodologies (George et al. 2008). In fact, e-training was found to be more successful than conventional classroom learning (George et al. 2008). Other types of phishing training might include embedded training or even microgames (Hong 2012).

METHODOLOGY

Research Setting

For this study, a case study methodology was used in order to examine phishing training within a single organization and to learn from their implementation of a phishing training program (Van Horn 1973). The case study approach is well suited to understanding the use of phishing training as theory can be developed based on the practice of phishing training in an actual setting (Benbasat et al. 1987). For this study, data was gathered from four types of phishing training offered at a mid-size, non-profit organization in the Midwest. This organization sent out multiple simulated (fake) phishing emails to their employees. All employees received the same messages and, as seen in Figure 1, the phishing emails in this study were all regular phishing emails and not targeted or spear phishing messages. Following an employee's reaction to the phishing messages, employees were directed to four different training options depending on their susceptibility to phishing deception. Specifically, organizational employees were presented with four types of phishing training including: 1) general training, 2) just-in-time training, 3) follow-up training, and 4) in person training. Details for each training type follow.

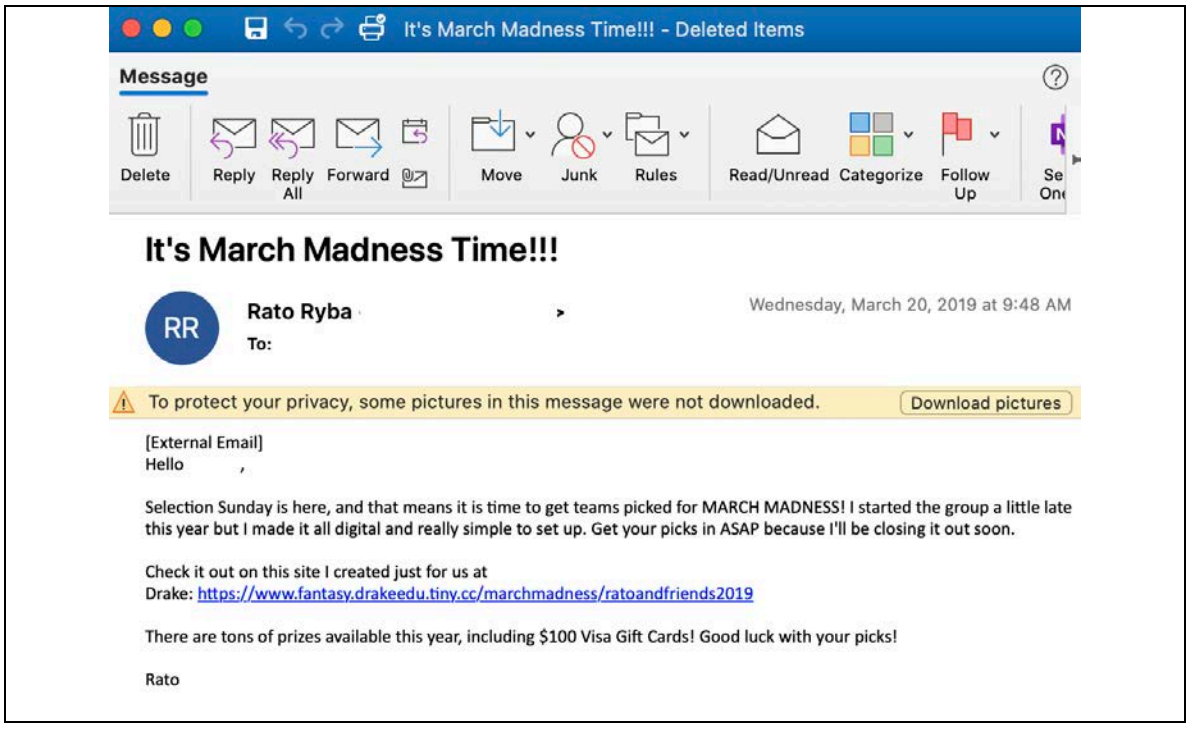

Figure 1. An example simulated phishing email sent to organizational employees

General phishing training was required for all employees by the organization's senior leadership. The general training process required the completion of an online module which was included in the organization's learning management system. Figure 2 shows a couple of screenshots from this required training. It is worth noting, previous research of online, required training has found success with this type of approach (Kumaraguru et al. 2009).

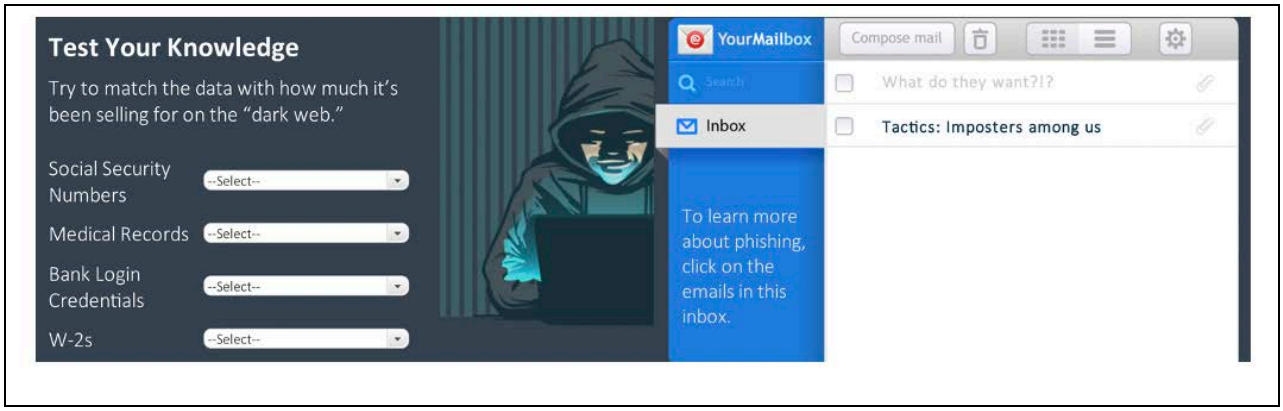

Figure 2. Example screenshots from the general training lessons

Just-in-time training was shared with an employee immediately following their first phishing failure. When an employee was deceived by a fake phishing email, they were immediately presented with a guide of what they missed. Similar to the general training, previous research has found success with this type of training for phishing detection (Karumbaiah et al. 2016).

Follow-up training was offered to employees who failed a second phishing test. Employees in this category would have already completed the just-in-time training and were required to complete an online training module to follow up on the just-in-time training. Similar to general training, this training required the completion of an online module which was included in the organization's learning management system.

Finally, *in-person training* was offered to employees who failed multiple phishing tests. These employees were provided with an in-person training tutorial.

Data Analysis

At this point, the data from this case has been collected and is ready for analysis. In the next stage of research, the research data will be analyzed using SPSS. For each type of training, the analysis will consider if more employees were "phished" after concluding the various types of phishing training.

For general training, the analysis will simply compare how many employees failed a phishing test after completing the required training and compare it with those who did not complete the training.

For just-in-time training, the data analysis will review how many employees, failed an initial test, viewed just-in-time training, and then failed a follow up test.

For follow-up training, data analysis will review how many employees failed an initial test, completed just-in-time training, failed a follow up test, completed the online follow-up training, and failed a third test. We will compare this finding with employees who did not fail the third phishing test.

For in-person training, analysis will review how many employees failed a phishing test following the in-person training.

Finally, additional variables including demographics (e.g., age, gender, employee role) and other details (e.g., time of day of phishing response) will be reviewed as a part of the data analysis.

CONCLUDING REMARKS

The aim of this study is to analyze the effectiveness of four different types of organizational phishing training approaches in order to determine which types of phishing training methods are most effective. This exploration of phishing training effectiveness will allow for benefits in relation to both research and practice. In terms of research implications, researchers can use the findings from this work to gain a better understanding of cybersecurity training techniques and how these techniques can be used in the development of both short- and long-term security plans. Furthermore, this work provides a foundation for future research studies in this area. In terms of practical implications, this work can provide a guide to organizations looking to implement employee phishing training practices within their organizations, which will ultimately benefit the organization and the IT security team. While all four types of phishing training were used by the organization in this study, their goal would be to focus their efforts on the training type with the highest success rate. Any lessons learned from this study, could be useful for others looking to implement phishing training programs.

REFERENCES

"2020 Data Breach Investigations Report." 2020. Verizon. (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf).

Abbasi, A., Zahedi, F., Zeng, D., Chen, Y., Chen, H., and Nunamaker, J. 2015. "Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information," *Journal of Management Information Systems* (31:4), pp. 109–157.

Anderson, B., Vance, A., and Eargle, D. 2013. "Is Your Susceptibility to Phishing Dependent on Your Memory?," in *Workshop on Information Security and Privacy (WISP)*, Milano, Italy, pp. 1–8.

Bansal, G. 2018. "Got Phished! Role of Top Management Support in Creating Phishing Safe Organizations," in *Proceedings of the Midwest Association for Information Systems*, St. Louis, MO, pp. 1–6.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3), pp. 369–386.

Bose, I., and Leung, A. 2007. "Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities," *Communications of the Association for Information Systems* (19:24), pp. 544–566.

Burns, A. J. 2019. "Security Organizing: A Framework for Organizational Information Security Mindfulness," *Data Base for Advances in Information Systems* (50:4), pp. 14–27.

Butavicius, M., Parsons, K., Pattinson, M., and McCormac, A. 2015. "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails," in *Australasian Conference on Information Systems*, Adelaide, pp. 1–10.

Firstbrook, P., and Wynne, N. 2018. "Fighting Phishing — 2020 Foresight," Gartner, July 19. (https://www.gartner.com/doc/3883275/fighting-phishing---foresight).

George, J., Biros, D., Burgoon, J., Nunamaker, J., Crews, J., Cao, J., Lin, K., Adkins, M., Kruse, J., and Lin, M. 2008. "The Role of E-Training in Protecting Information Assets against Deception Attacks," *MIS Quarterly Executive* (7:2), pp. 85–97.

Goel, S., Dennis, A., Williams, K., and Babb, J. 2017. "A Proposal to Recondition Learned Security Behaviors to Improve Response to Phishing Emails," in *Proceedings of IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*.

Goel, S., Williams, K., and Dincelli, E. 2017. "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems* (18:1), pp. 22–44.

Hong, J. 2012. "The State of Phishing Attacks," *Communications of the ACM* (55:1), pp. 74–81.

Jensen, M., Dinger, M., Wright, R., and Thatcher, J. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597–626.

Karumbaiah, S., Wright, R., Durickova, A., and Jensen, M. 2016. "Phishing Training: A Preliminary Look at the Effects of Different Types of Training," in *Workshop on Information Security and Privacy (WISP)*, Dublin, Ireland, pp. 1–10.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M., and Pham, T. 2009. "School of Phish: A Real-World Evaluation of Anti-Phishing Training," in *Symposium on Usable Privacy and Security (SOUPS)*, Mountain View, CA.

Ohaya, C. 2006. "Managing Phishing Threats in an Organization," in *InfoSec Conference*, Kennesaw, GA, pp. 159–161.

Sen, R. 2018. "Challenges to Cybersecurity: Current State of Affairs," *Communications of the Association for Information Systems* (43:2), pp. 22–44.

Van Horn, R. 1973. "Empirical Studies of Management Information Systems," *Data Base for Advances in Information Systems*, pp. 172–180.