KSU Proceedings on Cybersecurity Education, Research and Practice

2019 KSU Conference on Cybersecurity Education, Research and Practice

Oct 12th, 11:30 AM - 11:55 AM

Towards An Assessment of Audio and Visual Alerts and Warnings to Mitigate Risk of Phishing Emails Susceptibility

Molly Cooper
Nova Southeastern University, mollycooper@ferris.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Ling Wang
Nova Southeastern University

Laurie Dringus
Nova Southeastern University

Abstract
Phishing attacks target significant volume of Americans per year, and costs American organizations in the millions of dollars annually. Phishing is a cyber-attack using social engineering. Social engineering is the psychological manipulation of individuals in order to gain access to computer system(s) that the attacker is not authorized to use. Phishing can be presented in many ways: an email, link, website, text message, and other means. Phishing emails present a threat to both personal and organizational data loss. About 94% of cybersecurity incidents are due to phishing and/or social engineering. Significant volume of prior literature documented that end users are continuing to click on phishing links in emails, even after phishing awareness training, and it appears that there is a strong need for creative ways to warn and alert end users to signs of phishing in emails. Understanding a more aware state of mind, 'System 2 Thinking Mode' (S2), describes an individual in a more aware and alert state that s/he can utilize when making important decisions. End users have tendency to be more deliberate with their choices in S2, as opposed to 'System 1 Thinking Mode' (S1). S1 is more routine and not as deliberate. Some ways to trigger S2 include audio alerts, visual alerts, and vibrations. Assisting the end user in noticing signs of phishing in emails could possibly be studied through the delivery of audio and visual alerts and warnings. This study proposes to design and develop a method for a phishing alert and warning system that warns and alerts users to the signs of phishing in emails. The main goal of this work-in-progress research is to obtain Subject Matter Experts (SMEs) opinion to develop preliminary ranking of the top 10 signs of phishing in emails, and pair the signs of phishing with corresponding audio and visual warnings to be later used towards a phishing alert and warning system.

Keywords: Phishing, phishing alerting, phishing warning, social engineering, cybersecurity, audio warning in cybersecurity, visual warning in cybersecurity, cyber risk mitigation, phishing emails susceptibility.

Location
KSU Center Rm 400

Disciplines
Information Security

Comments
Submitted with reviewer revisions.

INTRODUCTION

Phishing and social engineering attacks target more than 37.3 million Americans per year, and costs American organizations an average of $3.7 million annually (Abass, 2018). Phishing and social engineering encompass approximately 93% of information security incidents (Anti-Phishing Working Group, 2018). Phishing emails continue to present a significant threat to both personal and corporate data loss (Almomani, Gupta, Atawneh, Meulenberg, & Almomani, 2013; Carlton, Levy, & Ramim, 2018).

End users are still falling for signs of phishing in emails (Wash & Cooper, 2018) and collectively costing themselves and their employers millions of dollars annually (Hernandez, Levy, & Ramim, 2016; Verizon, 2018). According to Clement (2018), email users have grown to more than 3.8 billion and is projected to reach 4.3 billion by the year 2022. Email remains the most pervasive form of communication, while other technologies such as social networking, instant messaging (IM), chat, mobile IM, and others are also taking hold, email is still the most ubiquitous form of business communication (Clement, 2018). In 2018, the total number of business and consumer emails sent and received per day exceeded 281 billion and is forecast to grow to over 333 billion by yearend 2022 (Radicati Group, 2018). Email nowadays is an essential part of personal and business communication (Clement, 2018). It is estimated that 72% of end users check their email via smartphone, and 19% of end users check email as soon as they arrive to work (Clement, 2018).

The overarching research problem this study will address is the significant volume of end users who continue to click on phishing links in emails, exposing them and/or their organizations to identity theft, monetary loss, and data loss (Aaron, 2010; Verizon, 2018). According to the Joint Task Force on Cybersecurity Education (2017):

> cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It draws from the foundational fields of information security and information assurance; and began with more narrowly focused field of computer security. (p. 16)

Dakpa and Augustine (2017) defined phishing as a way to obtain sensitive data, usernames, passwords, and other information from an end user in order to inflict future damage. Verizon (2018) indicated that signs of phishing in emails include poor grammar, sense of urgency in the message, incorrect sender address, and requests for personal information. Other signs of phishing in emails include incorrect Uniform Resource Locator (URL) in the email message, unfamiliar or inaccurate logo for a company, unfamiliar front, incorrect language translation, inconsistent greeting from common senders to the recipient, a request to update or verify information, an attachment, or an urgent request for a donation (Austin Technology, 2016).

Understanding a more aware state of mind, termed as 'System 2 Thinking Mode' (S2) by Kahneman (2011), describes an individual in a more aware and alert state that s/he can utilize when making important decisions. Users have a tendency to be more deliberate with their choices in S2, as opposed to 'System 1 Thinking Mode' (S1). S1 is more routine and not as deliberate or thoughtful. Alerts and warnings can be used to trigger S2 (Kahneman, 2011).

Alerts and warnings have been used for several common situations: fire alarms to alert of smoke, gas, or fire, weather alerts to signal imminent weather danger, and home intrusion alarms to signal unauthorized access. Alerts and warnings have been used with several manufacturers to warn drivers of danger in driving situations and have become universally adopted in most consumer vehicles. Warnings and alerts such as: loud beeps, blinking lights or icons, and seat or steering wheel vibrations (Zheng, Tang, Qing Li, & Fei-Yue Wang, 2004) have been used to obtain a driver's attention in order to alert the driver to a potentially dangerous situation.

Meaningful warning systems reflect specific urgency and prompt the user to pay attention based on the perception of the severity of the sound, visual prompt, and other system by the end user (Sousa et al., 2016). Specifically, audio alerting should be used when user safety is most important, and not used for insignificant issues. The balance between too many alerts, and what the user needs to pay attention to can be differentiated by users based on audio, visual and other techniques (Sousa et al., 2016).

It appears that developing ways to help users make decisions in S2 could be beneficial. Utilizing S2 could improve users' ability to recognize, alert, and react appropriately to phishing attempts. Assisting users to switch to S2 could potentially help decrease the amount of individual identity theft, business email compromise (BEC), and corporate data theft through risk of phishing in emails. Through the following literature synthesis, it appears little attention has been paid in research regarding audio, and visual warnings in the context of cybersecurity, or more specifically in the context of alerting and warning users to signs of phishing in emails through audio, and visual alert and warning combinations.

RESEARCH QUESTIONS AND METHODOLOGY

This study is a first in a sequence of several studies that will lead to the development of an audio and visual alert and warning system to mitigate risk of phishing emails susceptibility. The study will start by using Subject Matter Experts (SMEs) to ensure validity of the proposed system components. The main research question (RQ) that this study will address is: What audio and visual alert and warning system combination can be used to empirically assess end users' (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails?

1. What are the SMEs' top 10 signs of phishing in emails that they consider the most critical threats to end users?
2. What are the SMEs' identified audio and visual warning alerts to pair with the top 10 signs of phishing in emails?
3. What are the SMEs' validated maximum time and tasks for users': (a) *ability to notice,* and (b) *time to notice* signs of phishing in emails?
4. What are the SMEs' validated maximum time for users' *ability to notice* signs of phishing in emails?

This research study will utilize initial qualitative and quantitative data collection phrase using approximately 25 SMEs as an expert panel (Straub, 1989). The initial survey instrument will be conducted using Survey Monkey, using Delphi methodology for expert feedback on this subject (Ramim & Lichvar, 2014), each SME will receive an email invitation to participate in the initial survey. The survey will contain 15 examples of signs of phishing in emails including: sense of urgency, requiring action from the recipient, monetary gain for the recipient, misspelling of words, grammar errors, greeting errors, signature errors, incorrect URL, emails containing links, request for information, spoofed content, spoofed sender, unsolicited attachments, threatening language, addressing errors, and highly personalized emails. The survey will also contain a collection of audio and visual alerts. Audio alerts will include alarms, dings, vocal announcements, and tones. Visual alerts include variations of automotive dashboard icons, colors, and illustrations.

SMEs will be asked to rank their top 10 signs of phishing in emails from the survey list, and then pair each sign of phishing with what they feel would be an appropriate corresponding audio and visual alert. SMEs will also be asked what they feel an appropriate (a) *ability to notice* a phishing email (measured in tasks and seconds), and (b) *time to notice* a phishing email (measured in seconds) would be, along with any further qualitative feedback they have on the proposed study along with proposed project. Data collected in the SMEs survey will be used to construct an application to test (a) *ability to notice* and (b) *time to notice* phishing in emails using audio and visual warnings and alerts. Future research will also include a qualitative and quantitative data collection with participants through an application delivery system (Straub, 1989).

RATIONAL AND SIGNIFICANCE OF THE STUDY

This study is relevant as it presents a novel way of alerting end users to signs of phishing in emails using audio and visual warnings. Past studies have contributed to this issue; however, the problem still exists today. End-users are still susceptible to phishing attacks delivered through email (Anti-Phishing Working Group, 2018). Phishing continues to be a viable social engineering method, and collectively costs end users and businesses millions of dollars on an annual basis (Frauenstein, 2019). Phishing, spear phishing, and other social engineering techniques are being used against end users on a regular basis (Almomani et al., 2013; Carlton & Levy, 2017). This data includes loss of end user productivity, cost of containing malware exploited by the phishing attack, and cost to remediate loss of personal credentials. Phishing is also a corporate and personal data theft issue as noted by Nelson (2016). End users are clicking on phishing links and need improved ways to alert users to not fall for phishing in emails. Alerting end users to notice signs of phishing in emails by utilizing S2 triggers such as audio and visual alerting would directly add to the body of research aimed at assisting end users to be less susceptible to phishing attack.

This proposed study is significant, as it seeks to mitigate social engineering and phishing attempts on end users by increasing awareness (Abass, 2018; Mouton, Leenen, & Venter 2016). Zadelhoff (2016) indicated that end users are the biggest threat to an organization. Human behavior, while parsing emails, is also a factor in end user determination of whether an email is a phishing email containing a malicious link, or a safe email (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012).

Myounghoon et al. (2015) determined that auditory cues assist with dual task performance. Checking email and performing other work or personal tasks is considered dual task performance and causes individuals to be distracted (Kahneman, 2011; Mansi & Levy, 2013). This information, combined with the research by Kahneman (2011), indicate S2 could be triggered with auditory, and visual cues in order to alert a user of risk-taking behaviors. Some ways to trigger S2 include audio alerts, visual alerts, text and screen movement, text presented in a secondary language, and text presented in reverse. Assisting the end user in noticing signs of phishing in emails could possibly be studied through the delivery of audio and visual alerts, thus, triggering S2. Vance, Anderson, Kirwan, and Eargle (2014) studied security risk taking behaviors and effectiveness of security warnings. Their research determined that polymorphic warnings decrease habituation. Providing additional research towards audio and visual alerting for signs of phishing in emails could build upon previous research in order to combat the problem of end users clicking on phishing links. This could result in less data loss, significant costs associated with data recovery, and costs of information security efforts.

DISCUSSION AND CONCLUSIONS

Phishing attacks, a type of social engineering, is still a problem that needs to be solved or at least contribute to the body of research that aims at reducing phishing susceptibility among end users. This research proposes to reduce phishing susceptibility among end users by developing a prototype that alerts end users to the signs of phishing in emails with audio and visual alerting. SMEs opinions will be gathered to validate the most important signs of phishing end users should be warned about; this step will include asking SMEs opinions via survey to rank 15 simulated phishing examples down to the top 10 signs of phishing in emails. During this survey, all simulated phishing emails will be ranked and approved by SMEs. SMEs feedback will also use to pair audio and visual alerts with emails in order to rank by order of importance. SMEs feedback will be used to determine which set of audio and visual alerting should be paired with what sign of phishing in emails for presentation in an application prototype. SMEs feedback will also be used to determine a baseline time for (a) ability to notice and (b) time to notice signs of phishing in emails. Data collected from the SMEs will be used for a future application built to test the effects of audio and visual warning and alerting towards lessening the time it takes for an end user to notice signs of phishing in emails.

A limitation of this study includes unexpected events that limit the availability of SMEs. To mitigate it, efforts will be made to use professional cybersecurity circles to increase the SMEs pool. Another limitation of this study is that the survey is intended to best represent examples of phishing email messages to the participants of the study. If the examples of phishing emails are deemed incorrect, or irrelevant, the study will ensure adjustments are made to correct such issues based on the SMEs' recommendations. If the data input "is either incorrect, of low quality, or irrelevant, the resulted output is going to be ineffective regardless of the quality of the processing, colloquially, garbage-in/garbage-out" (Levy & Ellis, 2006, p. 185). Thus, testing will be done to ensure that data input from the survey and later from the system itself will be error free.

Future work includes constructing a prototype application that delivers the signs of phishing in emails with appropriate audio and visual warnings and alerts as determined by SMEs feedback. Participants will be tested on (a) *ability to notice* and (b) *time to notice* signs of phishing in emails with and without the assistance of audio and visual warning and alerting.

REFERENCES

Aaron, G. (2010). The state of phishing. *Computer Fraud and Security*, *2010*(6), 5–8.

Abass, I. (2018) Social engineering threat and defense: A literature survey. *Journal of Information Security*, 9, 257-264. https://doi.org/10.4236/jis.2018.94018

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys and Tutorials*, *15*(4), 2070–2090.

Anti-Phishing Working Group (2018). Phishing activity trends report. 1st quarter 2018. Retrieved from: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf

Austin Technology. (2016). How to spot phishing attacks and defend your business against them? Retrieved from: https://www.austintechnology.com.au/wp-content/uploads/2016/05/How-to-Spot-Phishing-Attacks-Austin-Technology-White-Paper.pdf

Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. *Online Journal of Applied Knowledge Management*, *6*(1), 107-118. Retrieved from: http://www.iiakm.org/ojakm/articles/2018/volume6_1/OJAKM_Volume6_1pp107-118.pdf

Clement, J. (2018). Email usage in the United States – statistics & facts. *Statista.com.* Retrieved from: https://www.statista.com/topics/4295/e-mail-usage-in-the-united-states

Dakpa, T., & Augustine, P. (2017). Study of phishing attacks and preventions, *International Journal of Computer Applications 163*(2), 5–8.

Frauenstein, E. D. (2019). An investigation into students responses to various phishing emails and other phishing-related behaviours. *Proceedings of the 17th Internaltional Information Security South Africa Conference*, 44–59. https://doi.org/10.1007/978-3-030-11407-7_4

Hernandez, W., Levy, Y., & Ramim, M. (2016). An empirical assessment of employee cyberslacking in the public sector: The social engineering threat. *Online Journal of Applied Knowledge Management*, *4*(2), 93-109. Retrieved from: http://www.iiakm.org/ojakm/articles/2016/volume4_2/OJAKM_Volume4_2pp93-109.pdf

Joint Task Force for Cybersecurity Education (2017). *Cybersecurity curricula 2017*. Retrieved from https://cybered.acm.org/

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, *9*, 181–211. http://doi.org/10.1049/cp.2009.0961

Mansi, G., & Levy, Y. (2013). Do instant messaging interruptions help or hinder knowledge workers' task performance? *International Journal of Information Management, 33*(3), 591-596. https://doi.org/10.1016/j.ijinfomgt.2013.01.011

Mouton, F., Leenen, L., & Venter, H.S. (2016) Social engineering attack examples, templates and scenarios. *Computers and Security*, *59*, 186-209. https://doi.org/10.1016/j.cose.2016.03.004

Myounghoon, J., Gable, T. M., Davison, B. K., Nees, M. A., Wilson, J. & Walker, B. N. (2015). Menu navigation with in-vehicle technologies: Auditory menu cues improve dual task performance, preference, and workload, *International Journal of Human–Computer Interaction*, *31*(1), 1-16. https://doi.org/10.1080/10447318.2014.925774

Nelson, J. (2016). Email phishing attacks estimated to cost $1.6M per incident. *Email Marketing Daily*.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing emails better than others? *Information Management & Computer Security*, *20*(1), 18–28.

Radicati Group. (2018). *Email statistics report.* Retrieved from: https://www.radicati.com/wp/wp-content/uploads/2017/12/Email-Statistics-Report-2018-2022-Executive-Summary.pdf

Ramim, M., & Lichvar, B. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, *2*(1), 122-126. Retrieved from: http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp122-136.pdf

Sousa, B., Donati, A., Özcan, E., van Egmond, R., Edworthy, J., Jansen, R., & Voumard, Y. (2016). Designing and deploying meaningful audio alarms for control systems. *Proceedings of the SpaceOps 2016 Conference*, 1–12. https://doi.org/10.2514/6.2016-2616

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13(2),* 147-169.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*, 679–722.

Verizon. (2018). *2018 data breach investigations report*, 30-68.

Wash, R., & Cooper, M. M. (2018). Who provides phishing training ? Facts, stories, and people like me. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Paper 492, 1-12. https://doi.org/10.1145/3173574.3174066

Zheng, N., Tang, S., Quing Li, H., & Fei-Yue Wang, G. (2004). Toward intelligent driver-assistance and Safety Warning Systems. *Intelligent Systems 19(2),* 8-11.

Zadelhoff, M. (2016). The biggest cybersecurity threats are inside your company. Boston, MA. *Harvard Business Review Publishing*.