Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 8, Issue 2, 2020

Subject matter experts' feedback on a prototype development of an audio, visual, and haptic phishing email alert system

Molly Cooper, Ferris State University, USA, mollycooper1305@gmail.com

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Ling Wang, Nova Southeastern University, USA, lingwang@nova.edu

Laurie Dringus, Nova Southeastern University, USA, laurie@nova.edu

Abstract

Phishing emails, also defined as email spam messages, present a threat to both personal and organizational data loss. About 93% of cybersecurity incidents are due to phishing and/or social engineering. Users are continuing to click on phishing links in emails even after phishing awareness training. Thus, it appears that there is a strong need for creative ways to alert and warn users to signs of phishing in emails. 'System 2 Thinking Mode' (S2) describes an individual in a more aware state of mind when making important decisions. Ways to trigger S2 include audio alerts, visual alerts, and haptic/vibrations. Assisting the user in noticing signs of phishing in emails could possibly be studied through the delivery of audio, visual, and haptic (vibration) alerts and warnings. This study outlines the empirical results from 32 Subject Matter Experts (SMEs) on an initial prototype design and development of an email phishing alert and warning system. The prototype will be developed to alert and warn users to the signs of phishing in emails in an attempt to switch them to an S2 state of mind. The preliminary results of the SMEs indicated that several features for a phishing alert and warning system could be assembled, resulting in a mobile phishing alert and warning prototype. Visual icons were chosen for each sign of phishing used in the prototype, as well as voice over warnings and haptic vibrations. The preliminary results also determined task measurements, 'ability to notice', and 'time to notice' signs of phishing in emails.

Keywords: Phishing, cybersecurity, social engineering, cyber threat mitigation, cyber alerts, cyber warnings, human factor in cybersecurity.

Introduction

Phishing emails continue to present a significant threat to both personal and corporate data loss (Almomani et al., 2013; Carlton et al., 2018). 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 et al., 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 is an essential part of personal and business communication, and most users read their emails on mobile devices (Clement, 2018). It is estimated that 72% of users check their email via smartphone, and 19% of users check email as soon as they begin work for the day (Clement, 2018).

The overarching research problem this study will address is: the significant volume of 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, 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).

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 also been used with several manufacturers to warn drivers of danger in driving situations and have become universally adopted in most consumer vehicles. Alerts and warnings such as: loud beeps, blinking lights or icons, and seat or steering wheel vibrations (Zheng et al., 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).

User training towards noticing the signs of phishing in email is considered a first line of defense against social engineering and phishing attacks (NIST, 2018). Some methods of user training include web-based videos, flyers and handouts, embedded training, and realistic phishing tests (Miranda, 2018). Miranda (2018) indicated that training users on phishing detection and incident response are important in setting up a successful corporate phishing training system. Foundational research by Dhamija et al. (2006) suggested alternative approaches are needed to assist users in noticing signs of phishing attack. Thus, 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.

This paper outlines the empirical results assessed from Subject Matter Experts (SMEs) to ensure validity of the prototype components. The following are the Research Questions (RQs) that this study will address:

RQ1. What are the SMEs' top signs of phishing in emails that they consider the most critical threats to users?

RQ2. What are the SMEs' identified audio, visual, and haptic warning alerts to pair with the top signs of phishing in emails?

RQ3. What are the SMEs' validated time and tasks for users': (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails?

Literature Review

Phishing

Email phishing is the most common social engineering method (Hong, 2012). An attacker can send an email with several ways to "bait" the user into giving personal information to the attacker. Phishing with email can also be used to direct a user to a fake website and then have the user enter personal information into the fake website. Phishing usually involves three phases (Hong, 2012). During the first phase, the victim usually receives an email with one or more signs of phishing in the email. The next phase usually includes the victim either taking action by entering information as prompted by the attacker or other action suggested in the message usually resulting in the victim giving the attacker the desired information. The final phase is monetizing the stolen information in the form of selling the account information or logging in as the user and stealing money from an account or stealing the desired intellectual property or secrets (Hong, 2012).

Signs of phishing in emails researched through a literature synthesis include but are not limited to: sense of urgency, requiring action, monetary gain, misspelling and grammar issues, greeting errors, signature errors, incorrect URL, request to click on links, request for information, spoofed sender or content, unsolicited or unexpected attachments, address mismatch, threatening language, and highly personalized emails (Chandrasekaran et al., 2006; Sheng et al., 2010; Wash & Cooper, 2018).

Alerts and Warnings

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). In the context of cybersecurity and more specifically phishing emails, mobile users appear to read their emails while on-the-go and in many instances also click links in phishing emails too quickly (while in S1) especially when in distracting environments (Goel & Jain, 2018), causing them the 'Oh-Shoot' syndrome. This well-known 'Oh-Shoot' syndrome causes people to perform activity such as click "OK" to authorize features on their mobile device or even provide their credentials, while not reading what the message stated, given they are on S1 state of mind. Then, their S2 kicks in and they appear to realize something was wrong, hence the ‘Oh-Shoot’, and backtrack to check what they did, while in most cases in the context of cybersecurity, this is too late and permissions or credentials were provided to the cyber criminals or adversaries (McAlaney & Benson, 2019).

There are several email filtering solutions available today as a way to warn users of signs of phishing in emails. Most warnings are visual messages, popup windows, and/or buttons to click in order to report phishing emails to administration. There are also several appliance-based products that filter email on the corporate email server, and “learn” signs of phishing in email either warn the user, or block the phishing URL (Dublin, 2018).

Audio beeps, visual alerts, icons, and vibrations (haptic warnings) are used in several consumer areas today to alert and warn users of potential issues or emergency. Seatbelt warning systems are arguably the most recognizable automobile warning system. According to Lohr (1974), many individuals were reluctant to use seatbelts in automobiles. Adding an audible sound to remind the driver and passengers to buckle up was used as an alert or warning. Collision warning systems for vehicles using audio, visual, and haptic factors are also incorporated into modern vehicles (Kane, 2012). Systems can be configured to minimize nuisance factors of the alarms (Ernst & Wilson, 2002). According to Ernst and Wilson (2002), collision warning systems reduce car accidents by warning and alerting the driver of potential hazards.

Other areas consumers benefit from audio, visual, and haptic alerting are medical alarm systems for patients. Audio beeps, visual flashing icons, and alarm sounds alert to get the attention of medical personnel if a patient is having difficulty or in danger (Chen et al., 2014). Urgency is represented by color of visual information and specific urgent frequencies. Weather warnings also convey urgency by specific colors used and specific alarm warnings (Event Alert System, 2019).

Email and Mobile Devices

Poushter and Stewart (2016) indicated that the volume of smartphone ownership and use has increased in Europe, the United States, and emerging economies around the world. Their research concluded that at least 89% of Americans own a smartphone (Poushter & Stewart, 2016). Van Rijn (2019) studied smartphone use as it pertains to reading email and determined an average of 67% of consumers use a smartphone to check their email. Most email is checked with a mobile device and then with a laptop/desktop (Van Rijn, 2019). Van Rijn (2019) stated that emails opened and viewed on a mobile device have doubled over the last five years. McLeod (2018) indicated that consumers now spend more than five hours a day on their smartphones.

Methodology

This research study utilized qualitative and quantitative data collection phase using 32 SMEs as an expert panel (Straub, 1989). Criteria for SMEs participation included the SME serving as an analyst job level and above in information security, and at least one year of information security experience. The initial survey instrument was conducted (April 2020) using Survey Monkey and using Delphi methodology for expert feedback on this subject (Ramim & Lichvar, 2014), each SME received an email invitation to participate in the initial survey. The survey contained 16 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 contained a collection of audio and visual alerts including alarms, dings, vocal announcements, and tones. Visual alerts included variations of automotive dashboard icons, colors, and illustrations. The most statistically significant results will be used towards the development of a Phishing Alert and Warning System (PAWS).

SMEs were asked to rank their top signs of phishing in emails from the survey list as specified in RQ1. This is important toward the development of PAWS as narrowing down the signs of phishing in email to a smaller number (5-10) can help with user fatigue (Kesselheim et al., 2011). The SMEs were then asked to pair each sign of phishing with what they feel would be an appropriate corresponding audio and visual alert. This is important towards RQ2 to determine if specific visual, audio, and haptic warnings are better suited for the top signs of phishing in emails. SMEs were also 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 towards mobile app design. Data collected in the SMEs survey will be used to construct a mobile app prototype to test (a) *ability to notice* and (b) *time to notice* phishing in emails using audio and visual warnings and alerts.

A limitation of this study was that PAWS was designed 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 to the user, the study was not effective. 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). Other potential limitation considerations include email content not being relevant to the participant, audio sounds and visual icons not being relevant or understandable by the participant, graphics and/or visual representations not consistent to the viewer, and urgency level of the audio not matching the urgency understanding of the participant.

Data Analysis and Results

Invitation emails to participate in the Subject Matter Expert (SME) survey were sent to 45 cybersecurity experts with a goal of 25 respondents. An SME panel of 32 cybersecurity experts were surveyed in one Delphi cycle (71.1% response rate) and a consensus was met on the survey questions. Table 1 provides the descriptive statistics of the 32 respondents during April 2020. Cybersecurity experts ranged from cybersecurity and information security professors, cybersecurity and information security C-level managers, cybersecurity and information security senior managers, cybersecurity and information security analysts, and cybersecurity investigators. Over 56% of the respondents had over 10 years of experience in cybersecurity and/or information security followed by 28% at five to 10 years of cybersecurity and/or information security experience. SMEs could enter one current profession for the survey.

Table 1. Descriptive Statistics of SMEs (N=32)

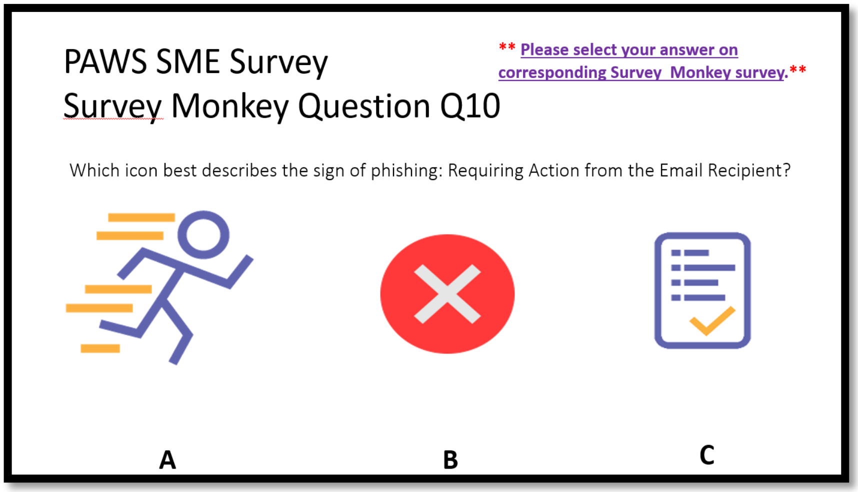
Survey Question	Frequency	Percentage
Current Cybersecurity Position:		
Professor	13	40.63%
Senior Management	6	18.75%
Middle Management	3	9.38%
IT Security Analyst	3	9.38%
Owner/Executive/C-Level	3	9.38%
Private Practice	1	3.12%
IT Senior Auditor	1	3.12%
IT Security Staff	1	3.12%
Cybersecurity Investigator	1	3.12%
Experience in Cybersecurity and/or Information Security:		
10 Years or More	18	56.25%
5-10 Years	9	28.13%
1 Year or Less	2	6.25%
1-3 Years	2	6.25%
3-5 Years	1	3.13%

The SMEs' top signs of phishing in emails that they consider and rank the most critical threats to users are shown in Table 2. Sense of urgency, requiring action, request for information, misspelling and grammar issues, and request to click on links were considered the top five signs of phishing in emails.

Table 2. SME Top Five Signs of Phishing in Emails – Ranked (N=32)

Survey Question	Rank	Percentage
Rank Signs of Phishing		
Sense of Urgency	1	11.32%
Requiring Action	2	11.22%
Request for Information	3	8.87%
Misspelling and Grammar	4	8.53%
Request to Click on Links	5	8.34%

The SMEs' identified audio, visual, and haptic warning alerts to pair with the top signs of phishing in emails were determined through SME survey answers. Each question was represented in a companion PowerPoint™ presentation. An example PowerPoint™ slide for the sign of phishing – requiring action from the email recipient, is shown in Figure 1. Each sign of phishing had a corresponding figure for SMEs' voting in the survey.



PAWS SME Survey
Survey Monkey Question Q10

** Please select your answer on corresponding Survey Monkey survey.**

Which icon best describes the sign of phishing: Requiring Action from the Email Recipient?

Figure 1. Visual Representation of SME Survey Question – Requiring Action

SMEs rank of icon matching to the top signs of phishing in emails is shown below in Table 3. SMEs feedback indicates the most effective visual icon for sense of urgency is a red alarm graphic,

Table 3. SME Rank of Icon Matching to Top Signs of Phishing in Emails (N=32)

Survey Question	**Frequency**	**Percentage**
Which Icon Best Represents the Sign Of Phishing: Sense of Urgency?		
Red Alarm	16	50.00%
Purple Alarm with Yellow Lines	15	46.88%
Purple Stopwatch	1	3.13%
Which Icon Best Represents the Sign of Phishing: Requiring Action?		
Running Person	14	43.75%
Red and White X	11	34.38%
Paper List	7	21.88%
Which Icon Best Represents the Sign of Phishing: Request for Information?		
Red Button with “i”	17	53.13%
Purple Icon and “i”	12	37.50%
Purple Arrow Over Text Box	3	9.38%
Which Icon Best Represents the Sign of Phishing: Misspelling and Grammar Issues?		
Red and Black Circle “Aa”	11	34.38%
Purple and Yellow “Aa”	6	18.75%
Purple Pencil with “X”	5	46.88%
Which Icon Best Represents the Sign of Phishing: Request to click on Links?		
White Link on Red Background	21	65.63%
Purple Link	7	21.88%
Purple Down Arrow	4	12.50%

and the most effective visual icon for the sign of phishing requiring action is a running person graphic (as shown for choice A in Figure 1). For the sign of phishing – request for information, the SMEs indicated a red button with a white letter "i" was the best representation of the sign. The sign of phishing – misspelling and grammar issues, as a red and black circle with the letters "Aa", and the sign of phishing - request to click on links, is most effectively portrayed as a white chain link on a red background. SMEs ranking of the audio and haptic pairings (as shown in Table 4) resulted in the consensus that the audio alerts would be most effective as a female voice-over alert. Other audio choices were stock mobile device sounds (iPhone, Android alerts), household alerts sounds (fire alarms, microwave sounds), and automobile alert sounds (seatbelt alerts, tire pressure warnings, check engine alerts). The SMEs panel also determined that shaking/vibration alerts should happen immediately upon the recipient seeing the email on the mobile screen.

Table 4. SME Rank of Audio and Haptic Matching to Top Signs of Phishing in Emails (N=32)

Survey Question	Frequency	Percentage
Which Audio Alert Group Would Be the Most Effective in Alerting Participants to Signs of Phishing in Email?		
Voice-Over Description of The Sign of Phishing (Female Voice Narration)	11	34.38%
Stock Mobile Device Notification Sounds (iPhone, Android)	9	28.13%
Household Alert Sounds (Fire alarm, Microwave sounds)	6	18.75%
Automobile Alert Sounds (Seatbelt ding)	6	18.75%
Haptic/Shaking Alerts Will Be Presented to The Participants. When Should the Mobile Device Shake Upon an Email Appearing on The Screen?		
Immediately as The Email Appears	12	38.71%
One Second After the Email Appears	9	29.03%
Two Seconds After the Email Appears	5	16.13%
Three Seconds After the Email Appears	5	16.13%

Table 5. SME Rank of Determining Factors for The Ability to Notice Top Signs of Phishing in Emails (N=32)

Survey Question	Frequency	Percentage
What Determines a Recipient's Ability to Notice Signs of Phishing in Emails?		
The Email Recipient's Experience with Phishing Training	29	90.63%
The Email Recipient's Past Experience with Being Phished	27	84.38%
The Email Recipient's Experience with Reading Emails	24	75.00%
The Email Recipient's Attention Span	19	59.38%
The Email Recipient's Native and Secondary Languages	15	46.88%
The Email Recipient's Gender	1	3.13%

The SMEs' validated tasks for users' demographic indicators of *ability to notice* signs of phishing in emails are illustrated in Table 5. The highest rank of ability to notice include the email recipient's experience with phishing training, followed by the email recipient's experience with being phished, experience reading emails, age, languages spoken, buttons clicked and gender. SMEs were instructed to choose all that applied. Table 6 illustrates the SME tasks that further determine a user's *ability to notice* signs of phishing in emails. The SMEs indicated the recipient of the email needs the *ability to notice* what signs of phishing they saw in the email, followed (in importance) by the time it takes to click legitimate or phishing buttons. The SMEs were instructed to choose all that applied.

Table 6. SME Rank of Tasks for The Ability to Notice Top Signs of Phishing in Emails (N=32)

Survey Question	Frequency	Percentage
What Are Some Tasks That Determine a Recipient's Ability to Notice Signs of Phishing in Emails?		
The Ability to Identify What Signs of Phishing They Saw In The Email	28	90.32%
Time it Takes to Click "Legitimate "or "Phishing" Buttons	13	41.94%

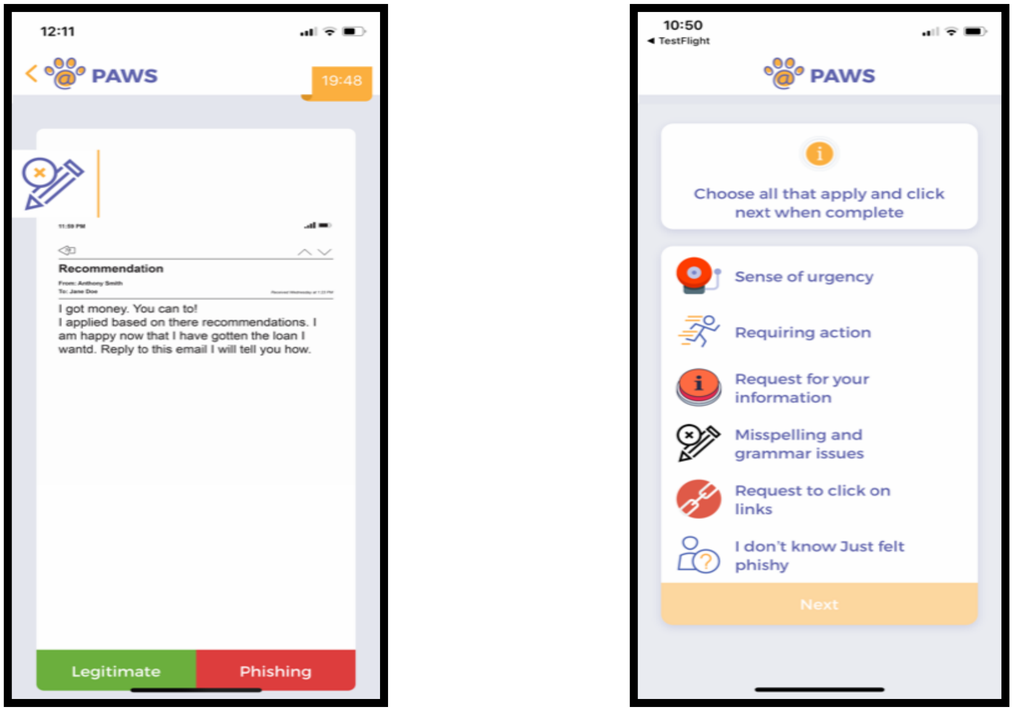
Table 7 further identifies SMEs feedback towards an audio, visual, and haptic alert and warning system combination can be used to empirically assess users' (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails. SMEs feedback indicated the email alert and warning groups: audio and visual alerts and warnings (AV), haptic alerts and warnings (H), and audio, visual, and haptic alerts and warnings (AVH), should be presented in a specific manner in order to alleviate participant habituation, and fatigue. It was determined the top five signs of phishing should be shown for each alert and warning group. This will result in 20 simulated email screens for the alert and warning system (including the no audio, visual, or haptic alerts and warnings (NAVH) group). Combined with feedback regarding the top signs of phishing, audio, visual, and haptic alerts and warnings, constructs for an audio, visual, and haptic phishing alert and warning system can be created.

Table 7. SME Rank of Presentation Order of Alerts and Warnings to The Top Signs of Phishing in Emails (N=32)

Survey Question	Frequency	Percentage
How Should Emails with Haptic Alerts and Warnings Be Presented?		
Show the Top 5 Signs of Phishing Emails in 1-5 Order	17	53.13%
Show the Top 5 Signs of Phishing Emails in Randomized Order	6	18.75%
Show the Top 10 Signs of Phishing Emails in 1-10 Order	5	15.63%
Show the Top 10 Signs of Phishing in Randomized Order	4	12.50%
How Should Emails with Audio and Visual Alerts and Warnings Be Presented?		
Show the Top 5 Signs of Phishing Emails in 1-5 Order	12	37.50%
Show the Top 10 Signs of Phishing Emails in 1-10 Order	9	28.13%
Show the Top 5 Signs of Phishing Emails in Randomized Order	6	18.75%
Show the Top 10 Signs of Phishing in Randomized Order	5	15.63%
How Should Emails with Audio, Visual, and Haptic Alerts and Warnings Be Presented?		
Show the Top 5 Signs of Phishing Emails in 1-5 Order	13	40.63%
Show the Top 10 Signs of Phishing in Randomized Order	9	28.13%
Show the Top 10 Signs of Phishing Emails in 1-10 Order	6	18.75%
Show the Top 5 Signs of Phishing Emails in Randomized Order	4	12.50%

Conclusion and Discussion

This study presents the results of SMEs validation process of a novel prototype system of alerting users to signs of phishing in emails using audio, visual, and haptics. Past studies have contributed to this issue; however, the problem still exists today. 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 users and businesses millions of dollars on an annual basis (Frauenstein, 2019). Phishing, spear phishing, and other social engineering techniques are being used against users on a regular basis (Almomani et al., 2013; Carlton & Levy, 2017). Alerting users to notice signs of phishing in emails by utilizing S2 triggers such as audio, visual, and haptic alerting would directly add to the body of knowledge aimed at assisting users to be less susceptible to phishing attacks through email. This research proposes to reduce phishing susceptibility among users by developing a prototype that alerts users to the signs of phishing in emails with audio, visual, and haptics on a mobile device. The main goal of this study was to determine what audio and visual alert and warnings combination can be used to empirically assess users' (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails. An alert and warning system prototype to assist users with phishing email detection will be developed that combines the SMEs ranking based on the SMEs survey results. The SMEs' identified audio, visual, and haptic warning alerts will also be paired with the top five signs of phishing in emails. The SMEs' validated time and tasks for users': (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails will be utilized as a baseline and variables towards PAWS mobile app analysis.



Recommendation
From: Anthony Smith
To: Jane Doe
Received Wednesday at 1:23 PM

I got money. You can to!
I applied based on there recommendations. I am happy now that I have gotten the loan I wantd. Reply to this email I will tell you how.

Choose all that apply and click next when complete

- Sense of urgency
- Requiring action
- Request for your information
- Misspelling and grammar issues
- Request to click on links
- I don't know Just felt phishy

(a) (b)

Figure 2. PAWS Prototype Screenshot: (a) Simulated Email Screen with Visual Icon – Sense of Urgency; (b) Ability to Notice the Top 5 Signs of Phishing

Future Research

Future research is planned for finalizing the validated mobile app prototype into the proposed PAWS and to test it with about 100 participants. As specified by the SMEs, *ability to notice signs of phishing* will be measured by the participant clicking legitimate or phishing buttons upon seeing a simulated email. Figure 2a illustrates a simulated email screen with a visual icon. Additionally, *ability to identify the signs of phishing* will be measured by the participant correctly identifying the sign of phishing they saw in the simulated email from the list provided as shown in Figure 2b. *Time to notice signs of phishing* will be measured in the amount of time it takes for a participant to click legitimate or phishing buttons upon seeing a simulated email. The SMEs survey results also indicate 25 seconds is the maximum amount of time to lapse before it is determined a participant did not notice signs of phishing in the simulated email. This baseline will also be used during future research of the PAWS mobile app study. Additionally, future research should include SMEs feedback on additional audio, visual, and haptic alerting methods. The timing of the alerts and warnings could also be studied further. Additional research could also include mobile app design questions for SMEs feedback regarding app page layout, volume of audio warnings, animation of visual cues, and simulated phishing email content or other innovative approaches to trigger end user S2 state of mind in effort to curb the 'Oh-Shoot' syndrome.

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*(4), 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. 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? 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. https://doi.org/10.36965/OJAKM.2018.6(1)107-118

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection based on structural properties. *Proceedings of the NYS Cyber Security Conference, 3*, 2-8.

Chen, L. Y., Tee, B. C.-K., Chortos, A. L., Schwartz, G., Tse, V., Lipomi, D. J., et al. (2014). Continuous wireless pressure monitoring and mapping with ultra-small passive sensors for health monitoring and critical care. *Nature Communications, 5*, 5028. https://doi.org/10.1038/ncomms6028

Clement, J. (2018). Email usage in the United States – statistics & facts. *Statista.com.* 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.

Dublin, J. (2019). Email filtering tools and techniques. https://searchsecurity.techtarget.com/tip/Email-filtering-tools-and-techniques

Dhamija R., Tygar J., & Hearst M. (2006) Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 581-590. https://doi.org/10.1145/1124772.1124861

Ernst, R., Wilson, T. (2002) Vehicular collision avoidance system (US 7124027B1). Yazaki North America, Inc.

Event Alert System. (2019). https://www.rrca.org/resources/event-directors/guidelines-for-safe-events/eas

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

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers and Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

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. https://doi.org/10.36965/OJAKM.2016.4(2)93-109

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Joint Task Force on Cybersecurity Education. (2017). Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity. https://cybered.hosting.acm.org/wpcontent/uploads/2018/02/newcover_csec2017.pdf

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kane, S. (2012). Pay attention to that buzz below: Cadillac’s new Safety Alert Seat. https://www.thecarconnection.com/news/1074766_pay-attention-to-that-buzz-below-cadillacs-new-safety-alert-seat

Kesselheim, A. S., Cresswell, K., Phansalkar, S., Bates, D. W., & Sheikh, A. (2011). Clinical decision support systems could be modified to reduce ‘alert fatigue’ while still minimizing the risk of litigation. *Health Affairs*, *30*(12), 2310-2317.

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

Lohr, T. (1974). *United States Patent No. 3,840,849.* https://patentimages.storage.googleapis.com/

b8/67/29/0bd5bb4784e4c4/US3840849.pdf

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

McAlaney, J., & Benson, V. (2019). Cybersecurity as a social phenomenon. *Cyber Influence and Cognitive Threats*, 1. https://doi.org/10.1016/B978-0-12-819204-7.00001-4

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

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

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity version 1.1, 31, PR-AT-1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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.

Phishing Emails – What's the risk, how to identify them and deal with them. (2019). https://pixelprivacy.com/resources/phishing-emails/

Poushter, J., & Stewart, R. (2016). MobilePhone, *22*. https://www.pewresearch.org/

Radicati Group. (2018). *Email statistics report.* 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. http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp122-136.pdf

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems, ACM*, 373–382. http://doi.org/10.1145/1753326.1753383

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.

Van Rijn. (2019). The ultimate mobile email stats overview. https://www.emailmonday.com/mobile-email-usage-statistics/

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.* Harvard Business Review. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Authors Biographies

Molly Cooper, Ph.D. is an Assistant Professor of Information Security and Intelligence at Ferris State University (FSU), and former Governance, Risk, and Compliance Lead for Michigan State University. Dr. Cooper has created several compliance programs ensuring the security of payment card data, security control compliance, and healthcare data. She has assisted with phishing research grants funded by the National Science Foundation, and has submitted several publications and has formed several culture building committees including Club25, and Empower IT - representing women of information technology (IT) and underrepresented members of the IT community. She is currently the faculty advisor for Women in Cybersecurity at FSU. Her primary technical and research interests are information security controls, gamification of cybersecurity concepts, cybersecurity risk, information security compliance, and phishing prevention. She holds both undergraduate and graduate degrees in information security and intelligence and received her Ph.D. in information assurance from Nova Southeastern University.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (http://infosec.nova.edu/), and chair of the Cybersecurity curriculum committee at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity and Information Assurance. He heads the Levy CyLab (http://CyLab.nova.edu/), which conducts innovative research from the human-centric lens of three key research areas cybersecurity, social engineering, and user-authentication. Levy authored numerous peer reviewed journal, conference proceedings, book chapters, and other publications. His scholarly research has been cited over 3,400 times. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and

FDLE South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a board member on the South Florida FBI/InfraGard. He consults federal agencies, state and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: https://sites.nova.edu/levyy/

Ling Wang, Ph.D. joined Nova Southeastern University in 2003, after receiving her Ph.D. in educational technology and a statistical consulting certificate from Purdue University. She teaches graduate courses in Information Systems, Information Assurance, and Cybersecurity Management. Dr. Wang is an active member of several professional associations, including AERA, AIS, and IEEE, and presents at the conferences associated with and sponsored by these associations. She has authored various journal articles and conference presentations in the areas of learning systems – integration and evaluation, information privacy paradox, and security and ethical issues in online computing communities. She also serves on the editorial board and as a reviewer for many national and international journals. Since 2008, Dr. Wang has served as the IRB representative for the college.

Laurie Dringus, Ph.D. is a Professor in the College of Computing and Engineering at Nova Southeastern University. Her research interests include human-computer interaction, user experience (UX) and information design, and usability. She has published widely in journals and conferences on many aspects of the user experience in various technology contexts, including the complex nature of human interaction and discourse in online settings. In addition to HCI, Laurie has been dedicated to the advancement of the field of online learning since 1983, having joined the pioneer group that developed online programs at NSU. From 1998-2014, she served as Editor-in-Chief of *The Internet and Higher Education*, a top ranked, internationally recognized research journal published by Elsevier. She served as Conference Co-Chair for the Online Learning Consortium (OLC) Accelerate 2017 Conference and Program Co-Chair for Accelerate 2016. She has received several distinctions and awards including being named as an OLC Fellow in 2017, CCE Distinguished Professor of the Year, 2015-2016, and the co-recipient of a research grant awarded by the NSU 2017-2018 President's Faculty Research and Development Grants Award competition. One of her former Ph.D. students, Dr. Harold Henke, established a student scholarship fund in her name.