2020

An Empirical Assessment of Audio/Visual/Haptic Alerts and Warnings to Mitigate Risk of Phishing Susceptibility in Emails on Mobile Devices

Molly Marie Cooper

An Empirical Assessment of Audio/Visual/Haptic Alerts and Warnings to Mitigate Risk of Phishing Susceptibility in Emails on Mobile Devices

by

Molly M. Cooper

A Dissertation in Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy
in
Information Assurance

College of Computing and Engineering
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Molly Cooper conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Yair Levy, Ph.D.
Chairperson of Dissertation Committee

August, 11, 2020
Date

Laurie P. Dringus

Laurie P. Dringus, Ph.D.
Dissertation Committee Member

August 11, 2020
Date

Ling Wang, Ph.D.
Dissertation Committee Member

August 11, 2020
Date

Approved:

Meline Kevorkian

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

August 11, 2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements of the Degree of Doctor of Philosophy

An Empirical Assessment of Audio/Visual/Haptic Alerts and Warnings to Mitigate Risk of Phishing Susceptibility in Emails on Mobile Devices

By
Molly M. Cooper

August 2020

Phishing emails present a threat to both personal and organizational data. Phishing is a cyber-attack using social engineering. About 94% of cybersecurity incidents are due to phishing and/or social engineering. A significant volume of prior literature documented that users are continuing to click on phishing links in emails, even after phishing awareness training. It appears there is a strong need for creative ways to alert and warn users to signs of phishing in emails.

The main goal of the experiments in this study was to measure participants' time for recognizing signs of phishing in emails, thus, reducing susceptibility to phishing in emails on mobile devices. This study included three phases. The first phase included 32 Subject Matter Experts (SMEs) that provided feedback on the top signs of phishing in emails, audio/visual/haptic pairings with the signs of phishing, and developmental constructs toward a phishing alert and warning system. The second phase included a pilot study with five participants to validate a phishing alert and warning system prototype. The third phase included delivery of the Phishing Alert and Warning System, (PAWS Mobile App ™) with 205 participants.

The results of the first phase aligned the constructs for the alert and warning system. A female voice-over warning was chosen by the SMEs as well as visual icon alerts for the top signs of phishing in emails. This study designed, developed, as well as empirically tested the PAWS Mobile App, that alerted and warned participants to the signs of phishing in emails on mobile devices. PAWS displayed a randomized series of 20 simulated emails to participants with varying displays of either no alerts and warnings, or a combination of alerts and warnings. The results indicated audio alerts and visual warnings potentially lower phishing susceptibility in emails. Audio and visual warnings appeared to have assisted the study participants in noticing phishing emails more easily, and in less time than without audio and visual warnings. The results of this study also indicated alerts and warnings assisted participants in noticing distinct signs of phishing in the simulated phishing emails viewed. This study implicates phishing email alerts and warnings applied and configured to email applications may play a significant role in the reduction of phishing susceptibility.

Acknowledgements

I am extremely blessed and grateful to receive such support throughout this special journey. There are several I would like to thank, especially my Mom and Dad who are always a constant inspiration. To my husband Larry, Major, and the members of CCoTY for supporting me every step of the way. To Mandy, the wind beneath my wings. To John, Rex, Bandit, Mallu, and Bubba. To Aaron, Jarred, Drake, Kristi, Kevin, and Mason, and to my grandparents who always encouraged me to constantly improve.

To my friends and family - Mickey and Roger Beebe, Peter and Brittany Dillman, Dr. Marcia Ward, Elisabeth Anderson, Dr. Jess Knott, Christine Collette, and Sherri Archer. Thank you for your help.

To Liam Topping, Dr. Sean Aviv, Dr. Rick Wash, and Alexey - thank you for your talents and creative energy.

To Dr. Greg Gogolin - thank you for always believing in me and being such an inspiration. Thank you to Dr. Jim Jones and Dr. Doug Blakemore. To my colleagues, especially Amy Ruba -thank you for your expertise and hours towards this goal. Thank you to Dr. Jim Furstenberg, Dr. Jason Otting, Dr. Steve Schuiling, and Professor Jerry Emerick.

Thank you to everyone at NSU working through this process together. Especially: Bob Jones, Tommy Pollock, John McConnell, Mel Tomeo, Javier Coto, Kimberly Smith, Tyler Pieron, Vazzi, David Zeichick, Andrea Di Fabio, Amy Antonucci, Dr. Emily Brown, Dr. Darrell Eilts, Dr. Melissa Carlton, Dr. Michelle Ramim, and Dr. Karla Clark. To Rob McCurdy, and everyone at MSUIT, I thank you.

Thank you to all of the SME Survey and PAWS Mobile App participants. I greatly appreciate it!

To Dr. Dringus and Dr. Wang – I was so incredibly fortunate to have such amazing and talented women on my committee. Thank you for your time, expertise, and guidance through the process.

To Dr. Levy – you have been an inspiration to me from the very beginning. Thank you for pushing me to be the best I can be. Thank you for taking me on and investing so much of yourself into this dream. I appreciate your vision and guidance more than words can say. It has been such an honor to work with you.

Table of Contents

Chapters

Appendices

List of Tables

List of Figures

Chapter 1

Introduction

Background

According to Clement (2018), the volume of email users has 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 addition, email is integral to the overall Internet experience as an email account (i.e. email address) is required to sign up to most online activities, including social networking sites, IM, and any other kind of account or presence on the Internet. In 2018, the total number of professional emails sent and received per day exceed 281 billion and is forecast to grow to over 333 billion by yearend 2022 (Radicati Group, 2018). Over the past two decades, email became an essential part of personal and business communication (Clement, 2018). It is estimated that 72% of users check their email via mobile smartphone, and 19% of users check email as soon as they arrive to work (Clement, 2018). However, users are still falling for signs of phishing in emails (Wash & Cooper, 2018) and collectively costing themselves and their employers millions of dollars annually.

Phishing and social engineering attacks target more than 37.3 million people per year, and costs 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). Also defined as an email spam message, phishing emails continue to present a significant threat to both personal and corporate data loss, even after phishing awareness training (Almomani et al., 2013; Carlton et al., 2018). Thus, it appears that there is a strong need for creative ways to warn and alert users to signs of phishing in emails.

Problem Statement

The overarching research problem this study addressed 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). Dakpa and Augustine (2017) defined phishing as one way to obtain sensitive data, usernames, passwords, and other information from a user to inflict future damage. The Anti-Phishing Working Group (2018) also described signs of phishing in emails including 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).

Phishing is a type of social engineering that is part of cybersecurity (Canfield, 2018; Hernandez et al., 2016). 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)

Termed as ‘System 2 Thinking Mode’ (S2) Kahneman (2011), describes an individual in a more aware state that s/he can utilize when making important decisions. 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 or thoughtful (Kahneman, 2011). Warning is defined as “something that makes you understand there is a possible danger or problem, especially one in the future”, and the definition of alert as, “an alarm or other signal of danger” (Merriam-Webster Dictionary, 2018, p. 30). 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 all vehicles. Examples of some automotive related warnings and alerts include 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 prompt 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 user (Sousa et al., 2016). Specifically, audio alerting should be used when user safety if most important, and not used for insignificant issues (Sousa et al., 2016).

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, visual, and haptic (vibration) 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/visual/haptic alert and warning combinations.

Dissertation Goal

The main goal of this research study was to design, develop, and empirically test the effectiveness (via the measures of (a) *ability to notice*, & (b) *time to notice*) of an audio, visual, and haptic warning system that alerts users to the signs of phishing in emails on mobile devices. The need for this work was demonstrated by Almomani et al. (2013), Acquisti (2016), and The Anti-Phishing Working Group (2018). An initial list of signs of phishing in emails, that are considered the most critical threats, was developed from published research, and preliminarily identified in the corresponding literature synthesis. Additionally, libraries of both audio/visual/haptic alerts and warnings to correspond with each of the signs of phishing in emails were developed to use towards the Phishing Alert Warning System (PAWS) mobile application.

The first specific goal of this study was to develop and validate, using Subject Matter Experts (SMEs), the list of the top signs of phishing in emails that are considered the most critical threats. Frauenstein (2019) indicated that there are certain signs of phishing in emails that should be more commonly seen by users currently, as well as certain signs of phishing in emails that are considered more dangerous than others (based on a high percentage of automated security controls in place to ward off commonly seen risks). Outcome from the first goal was used to determine the SMEs' identified and validated list of the top signs of phishing in emails that are the most critical threats, in rank order, paired with an audio/visual/haptic alert and warning for the second goal.

Anderson et al. (2013) indicated that polymorphic warnings (beeps, sounds, & vibrations) can reduce habituation. Axon et al. (2017) indicated that audio warnings are more effective when appropriately designed for the human ear, pertaining to cybersecurity warnings. Appropriately matched audio/visual/haptic alerts and warnings for the related signs of phishing in emails is important to examine.

The third and fourth specific goals of this study was to determine the tasks for measures of (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails using SMEs. The SMEs validated measures helped to determine if improvement was made with or without the assistance of PAWS for the user. The measure of *ability to notice* is referred to an individual user's ability (or lack thereof) to notice if an email has signs of phishing. The measure of *time to notice* is referred to the time (in seconds) of an individual user's ability to determine if an email has signs of phishing.

The fifth goal of this research was to determine validation and testing procedures that should be considered to deliver a mobile app phishing alert and warning system prototype. The development of valid components of the phishing alert and warning system utilized SME validated feedback for (a) top signs of phishing in emails in rank order, (b) SME validated feedback for audio/visual/haptic alerts and warnings to pair with the signs of phishing, (c) characteristics to assess users' *ability to notice* and/or *time to notice* signs of phishing in emails, (d) based on SMEs' response, the measure of *time to notice* will determine how long (in seconds) users 'notice signs of phishing in emails. This research goal included the actual programing and building of the PAWS mobile app prototype. Testing procedures included capturing the qualitative feedback of prototype testers, and correcting any significant issues with the mobile app.

The sixth goal of this study was to determine if there are any significant mean differences among the users' *ability to notice*, *time to notice*, and *time to notice signs* of phishing in emails with or without PAWS. The seventh goal of this research study was to determine if there are any significant mean differences among the users' *ability to notice*, *time to notice*, and *time to notice signs* of phishing in emails based on (a) age, (b) gender, (c) experience with phishing training, and (d) attention span.

Ability to notice that an email has signs of phishing, or poses a significant risk, is critical to user's cybersecurity situational awareness (Wash & Cooper, 2018). As practiced in other fields, such as automotive, audio/visual/haptic warnings are used for alerting such as fasten seatbelt, lane departure, loss of air pressure, and engine trouble (Sternlund et al., 2017). The hypothesis is that a user's *time to notice* the signs of phishing in emails may improve if measured first without the use of audio/visual/haptic warnings, then again with the use of audio/visual/haptic warnings to determine if the user notices the signs of phishing to start with or faster with the assistance of audio/visual/haptic warnings, while also attempting to see if any significant differences exist base on key demographics indictors as well as audio/visual/haptic alert and warning combinations.

Sheng et al. (2010) indicated the importance of demographic research in the context of studying and training specific user groups against risk behavior and phishing susceptibility. The PAWS Mobile App was configured to determine if there are any mean differences in the users' *ability to notice*, *time to notice*, and *time to notice signs* of phishing in emails using PAWS based on (a) age, (b) gender, (c) experience with phishing training, as well as (d) attention span. In summary, PAWS was developed using SME feedback and used to determine if audio/visual/haptic alerts and warnings improve a user's ability to notice the top signs of phishing in emails more quickly, thus, reducing phishing susceptibility.

Research Questions

The main Research Question (RQ) that this study addressed was: What audio/visual/haptic alert and warning system combination can be used to empirically assess users' (a) *ability to notice*, and (b) *time to notice* phishing in emails on mobile devices?

RQ1: What are the SMEs' validated top signs of phishing in emails that are considered the most critical threats to users?

RQ2: What SMEs' identified audio/visual/haptic alerts and warnings are most valid to pair with the top signs of phishing in emails?

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

RQ4: What is the SMEs' validated maximum *time for users' ability to notice* signs of phishing in emails?

RQ5: What validation and testing procedures should be considered to deliver a mobile app phishing alert and warning prototype?

RQ6a: Do statistically significant mean differences exist among users' *ability to notice* signs of phishing in emails with or without PAWS?

RQ6b: Do statistically significant mean differences exist among users' *time to notice* signs of phishing in emails with or without PAWS?

RQ6c: Do statistically significant mean differences exist among users' *ability to notice signs* of phishing in emails with or without PAWS?

RQ7a: Do statistically significant mean differences exist among users' *ability to notice* signs of phishing in emails using PAWS based on: (a) age, (b) gender, (c) experience with phishing training, and (d) attention span?

RQ7b: Do statistically significant mean differences exist among users' *time to notice* of phishing in emails using PAWS based on: (a) age, (b) gender, (c) experience with phishing training, as well as (d) attention span?

RQ7b: Do statistically significant mean differences exist among users' *ability to notice signs* of phishing in emails using PAWS based on: (a) age, (b) gender, (c) experience with phishing training, as well as (d) attention span?

Relevance and Significance

Relevance

The relevance of this research study is that it presented a novel way of alerting users to signs of phishing in emails on mobile devices using audio/visual/haptic warnings. Past studies have contributed to this issue; however, the problem persists.

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). Phishing attacks target more than 37.3 million people per year (Real, 2013), and costs organizations an average of $3.7 million annually (Wombat Security, 2015). This figure includes loss of 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). According to Acquisti et al. (2010), users are clicking on phishing links and need improved ways to alert users to not fall for phishing in emails. Alerting users to notice signs of phishing in emails by utilizing S2 triggers such as audio/visual/haptic alerting would directly add to the body of research aimed at assisting users to be less susceptible to phishing attack.

Significance

This study contributes to the significant area of phishing prevention social engineering mitigation by increasing user phishing awareness through alerts and warnings (Abass, 2018; Hong, 2016; Mouton et al., 2016). Zadelhoff (2016) indicated that users are the biggest threat to an organization. Human behavior, while parsing emails, is also a factor in user determination of whether an email is a phishing email containing a malicious link, or a safe email (Pattinson et al., 2012).

Myounghoon et al. (2015) determined 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, visual, and haptic cues 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 user in noticing signs of phishing in emails could possibly be studied through the delivery of audio/visual/haptic alerts, thus, triggering S2. Vance et al. (2014) studied security risk taking behaviors and effectiveness of security warnings. Their research determined polymorphic warnings decrease habituation. Providing additional research towards audio/visual/haptic alerting for signs of phishing in emails could build upon previous research to help combat the problem of users clicking on phishing links. This could result in less data loss, significant costs associated with data recovery, and costs of information security efforts.

Barriers and Issues

This research study had several potential barriers and issues that were addressed. One challenge was developing a SME survey containing as many elements of the PAWS prototype as possible. A separate companion document was added to the survey to play audio samples and visual icons for the SMEs to choose from. One barrier was collecting SME responses and feedback in a two-week time period. This time factor had potential to disrupt the research study timeline SME participants were rewarded with gift cards to help mitigate this risk. Participants for the PAWS mobile application were recruited through LinkedIn contacts of the primary investigator, a potential barrier was participants becoming unwilling to download an app to their mobile device. Contact information of the researcher was added to the recruitment email to be available for questions and comments about the mobile app. Another potential barrier was participants not understanding the mobile app email screens or functionality of the mobile alert and warning application. Contact information of the researcher was utilized in the few cases users had issues with the mobile app itself.

Assumptions, Limitations, and Delimitations

Assumptions

It was assumed that SMEs understood the survey and answered appropriately. It was also assumed that PAWS participants will be readily available and willing to participate in the study. Another assumption of this study was that participants were able to operate their mobile device, that they regularly utilize sound and vibration on their mobile phone, and that the simulated emails represented in the PAWS mobile application were understandable and relatable for the study participants.

Limitations

A limitation of this study included unexpected events that limited the availability of participants. 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, and urgency level of the audio not matching the urgency understanding of the participant. Financial limitations included inability to program a hover over links in email originating from the participants email. This feature was limited to a picture, or screen of an email with limited functionality.

Delimitations

A potential delimitation of this proposed study was choosing vague simulated phishing messages. As a validation of emails chosen, extensive literature review, and re-creation of emails were performed. Another delamination included audio/visual/haptic warnings potentially not representing the urgency needed to spark the user's attention. As a validation of audio/visual/haptic warnings used in the prototype, SMEs were asked to pair warnings with their perceived urgency of the simulated emails.

Definition of Terms

The following represent terms and definitions.

Alert –An alarm or other signal of danger (p. 30). (Merriam-Webster Dictionary, 2018).

Cybersecurity – "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" (Joint Task Force on Cybersecurity Education, 2017, p. 16).

Haptics – "The science of touch. Use of technology promoted by interacting with physical objects" (Chang, 2002, p. 84)

Phishing – “Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party” (Jagatic, 2007, p. 1).

System 2 Thinking – “Understanding a more aware state of mind in human behavior and response” (Kahneman, 2011, p. 13).

Tactile cues – “Perceptible by touch: textures, vibrations, and bumps” (Chang, 2002, p. 84).

Vulnerability – “Human, organizational, and technical weaknesses that can be exploited by an adversary” (Canfield, 2018, p. 827).

Warning – “Something that makes one understand there is a possible danger or problem, especially one in the future” (Merriam-Webster Dictionary, 2018, p. 390).

Summary

Social engineering and phishing are still problems that needs to be properly mitigated and further included in the body of research that aims at reducing phishing susceptibility among users. This research contributes toward phishing susceptibility improvements among users by developing a prototype that alerted users to the signs of phishing in emails with audio/visual/haptic alerting. SMEs opinion was gathered towards validation of the most important signs of phishing users should be warned about. This step included collecting SME opinion via survey to rank simulated phishing examples. SMEs feedback was also used to pair alerts and warnings with emails. SMEs feedback was also used to determine which set of audio/visual/haptic alerting should be paired with matching signs of phishing in emails for presentation in the PAWS mobile application prototype.

Chapter 2

Review of Literature

Social Engineering

According to Krumholtz et al. (2015), social engineering can be defined as manipulating users into providing sensitive information to an untrustworthy source. Social engineering is also defined as one way to gain sensitive information about an email recipient by taking advantage of human behavior (Abass, 2018). The sensitive information obtained can consist of passwords, date of birth, mother's maiden name, social security number, and other identifiers that could be used to open or gain access to a variety of financial, network, and social accounts (Krumbolz et al., 2015). According to Hong (2012), phishing attacks are also used to steal personal information, credit card information, intellectual property, corporate information, and national security secrets.

People are easily hacked by luring them to click on harmful links that lead to fake websites with malware, downloading software, and running malicious applications (Krumbolz et al., 2015). Deceiving the user into giving personal information can lead to compromise of accounts (Abass, 2018). Social engineering preys on the innate human tendency to trust and/or help others (Mouton et al., 2016). Depending on the level of access the user has, this can lead to business compromise, as well as personal account compromise. This research will focus on the social engineering channel of phishing, and the signs of phishing in emails.

Motivators for attackers include money and information. According to Hong (2012), money can be stolen directly out of a bank account from access granted directly or indirectly by the victim. In some cases, account credentials can be stolen through a few different social engineering channels. For example, an attacker could lure people to a website created to appear as a legitimate site and ask for the victims to enter their username and password (Hong, 2012). Through this method, the attackers can harvest several username and password combinations in attempt access to bank accounts or other private accounts. Sometimes the account information is sold online in underground networks where the access information is sold to others (Hong, 2012).

Social engineering attacks include and combine physical, social, and technical aspects to achieve the goal of deceiving the user (Krumbolz et al., 2015). According to Phishing.org (2019), social media can be exploited in many ways, including Facebook Messenger. In this attack, Facebook users receive messages from someone already familiar with them. This spoofed or impersonated person sends a message to the Facebook user redirecting them to a spoofed page asking for log in credentials (Phishing Examples, 2019). Many channels and attack vectors can be used in combination to gain access to user accounts, and user networks through social engineering. Social engineering channels include instant messaging, telephone, social network applications, cloud services for corporations, multiplayer games, and websites (Hong, 2012; Kromboltz et al., 2015). Fraudulent or phishing websites are also a common way to trick a user into entering personal data. Some clues to fraudulent websites include spoofed content (the web site was crafted to appear as a legitimate website) incorrect address bar URL, status bar errors and overall security indicators (Dhamija et al., 2006).

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 many 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 by actually logging in as the user and stealing money from an account or stealing the desired intellectual property or secrets (Hong, 2012).

Hong (2012) concluded that the phishing is a problem that most likely will never be solved. Hong (2012) suggested to address the worst aspects of phishing and work on improving ways to prevent, attack, and respond to phishing attacks. Abass (2108) determined the most effective defense to social engineering is to educate and assist users in noticing signs of social engineering. This proposed research study aims at preventing or at least mitigating the threat of phishing attacks by alerting users to the signs of phishing in emails.

Table 1

Summary of Social Engineering Description Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Abass, 2018	Literature review and synthesis	18 papers	Social engineering analysis	Determined people are the weakest link, but also the best tool to defend against social engineering.
Contech & Schmick, 2015	Literature review and synthesis	15 papers	Social engineering analysis	Determined the most effective defense against social engineering is an educated user.
Hong, 2012	Literature review and synthesis		State of social engineering/analysis	Suggested to work towards better ways to prevent, detect, and respond.
Krumbholtz et al., 2015	Literature review and synthesis		Social engineering taxonomy	Provided a taxonomy of social engineering attacks, illustrated real-world incidents of successful attacks
Mouton et al., 2016	Literature review and synthesis	Two models	Social engineering template	Proposed 10 social engineering templates

Signs of Phishing in Emails

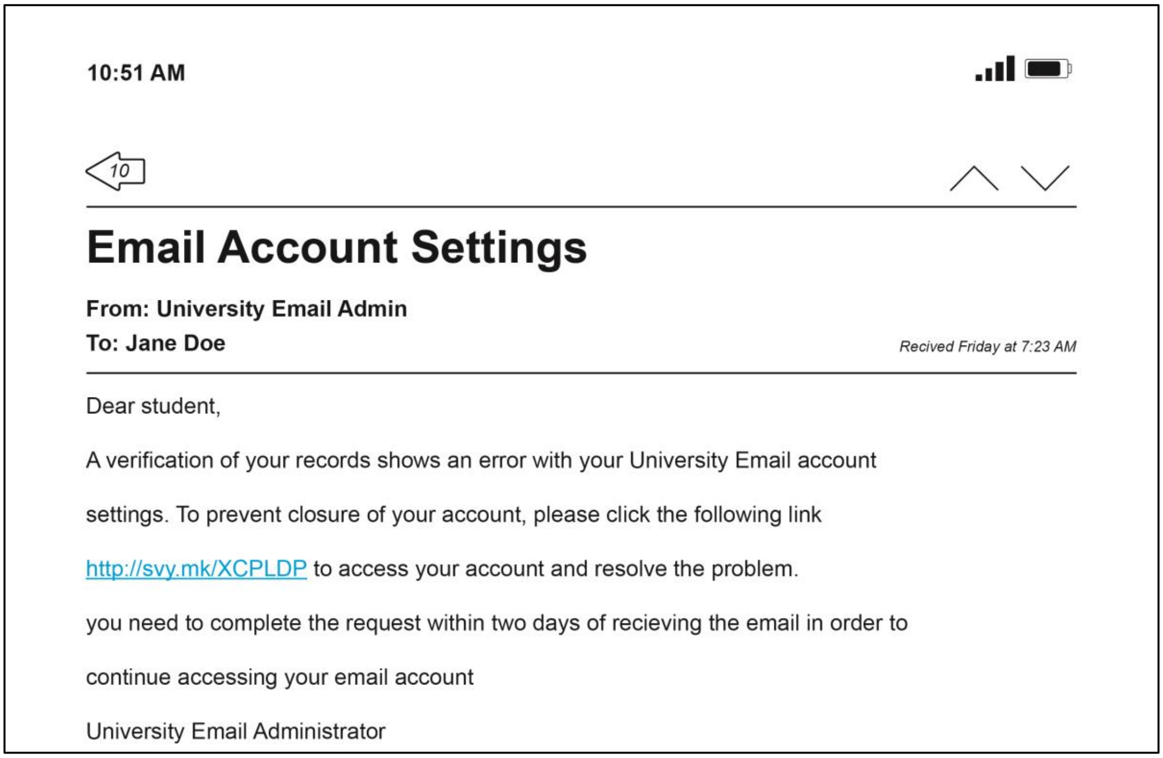
There are several signs of phishing in emails (Wash & Cooper, 2018). Most frequently, phishing emails will include more than one sign of phishing. Signs of phishing in emails researched through a literature synthesis include but are not limited to: sense of urgency, requiring action, monetary gain, misspelling 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; “Phishing Examples,” 2018; “Phishing Examples- What’s the risk, and how to identify and deal with them”, 2019; Sheng et al., 2010; “The anatomy of a phishing email,” 2019; Wash & Cooper, 2018; Yates & Harris, 2015).

Urgency

Urgency is a main sign of phishing in emails. Hong (2012) indicated that urgency is a method for criminals to misdirect attention. They also described an urgency email as sending an email to an email recipient warning people of an attack and instilling a sense of urgency that a patch must be installed immediately. Urgency can also be used to attempt to invoke an impulse emergency response from the recipient (Chandrasekaran et al., 2006). Unusual log-in activity is another example of a tech-based urgency email that requires an action from the user for an account to not be closed. Another example of urgency would be notifying users of several failed logins to their account, instilling urgency by insisting the user verifies their account immediately to avoid account deletion (Sheng et al., 2010). Urgency can be presented in several ways. One example as illustrated in Figure 1 illustrates the need for an urgent request from the recipient, so their account is not closed (Wash & Cooper, 2018). For the purpose of this research, urgency will be portrayed as both technical (including loss of corporate email account, loss of personal account connectivity, and corporate account access) and personal (including immediate need to verify shipping address to a personal resistance and personal bank account issues).

Figure 1

Sign of Phishing in Email: Sense of Urgency



Email Account Settings

From: University Email Admin
To: Jane Doe

Recived Friday at 7:23 AM

Dear student,

A verification of your records shows an error with your University Email account settings. To prevent closure of your account, please click the following link http://svy.mk/XCPLDP to access your account and resolve the problem.

you need to complete the request within two days of recieving the email in order to continue accessing your email account

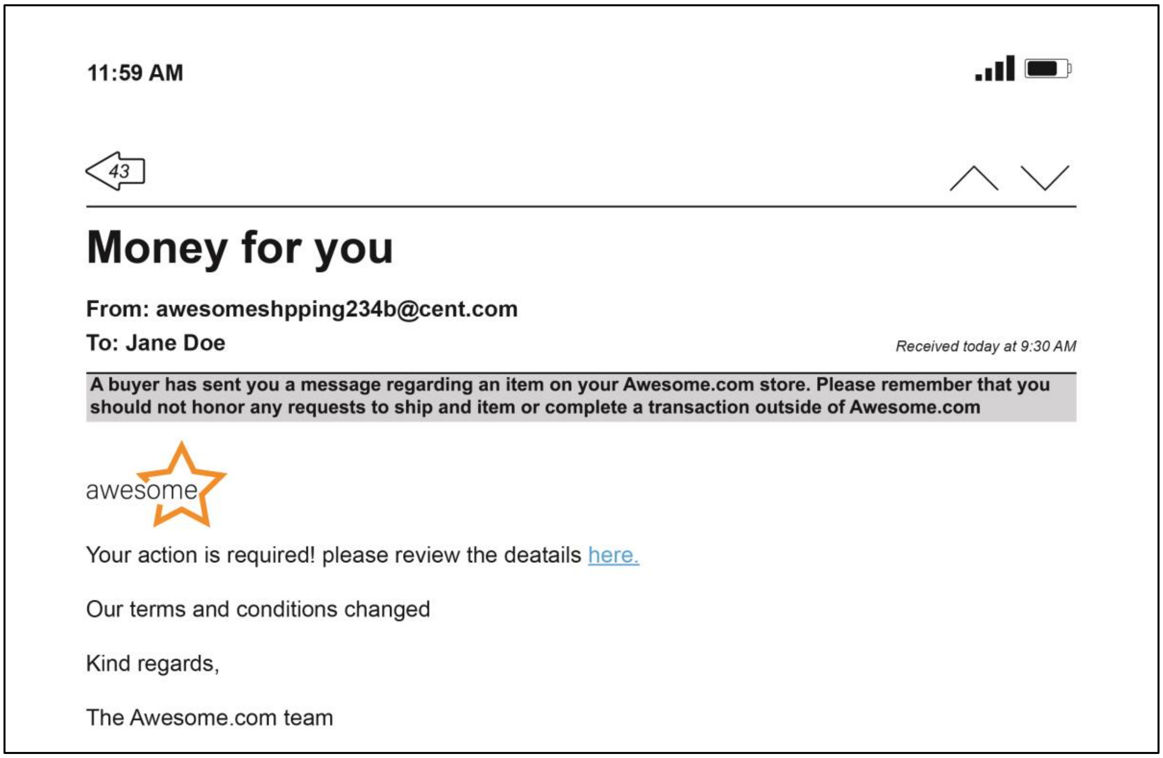
University Email Administrator

Requiring Action from the Recipient

Requiring action from the email recipient is a sign of phishing in emails that plays upon urgency and the user’s accounts or activities (“Phishing Examples - What’s the risk, how to identify them and deal with them”, 2019). Figure 2 illustrates the need for action from the recipient. The email appears to be from a shipper sending something to the email recipient. Other phishing emails that utilize action on the part of the recipient include asking the recipient to review personal details for a specified account. Other examples are phishing emails that ask the recipient to upgrade their account or to reset their password. Phishing emails requiring action can also include unsolicited emails about accounts the user does not have. Most businesses have policies that specify personal information will not be requested through email, which should be an indication the email is a phishing attempt.

Figure 2

Sign of Phishing in Email: Requiring Action



Money for you

From: awesomeshpping234b@cent.com

To: Jane Doe

Received today at 9:30 AM

A buyer has sent you a message regarding an item on your Awesome.com store. Please remember that you should not honor any requests to ship and item or complete a transaction outside of Awesome.com

Your action is required! please review the deatails here.

Our terms and conditions changed

Kind regards,

The Awesome.com team

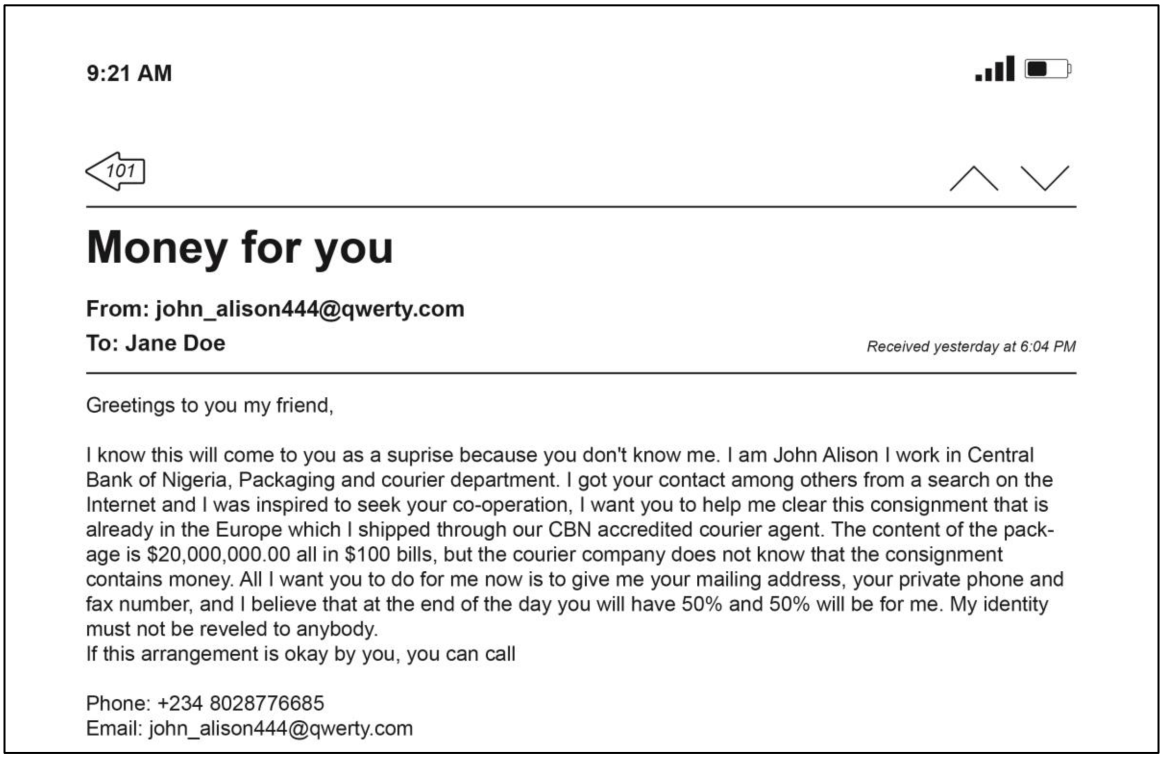
Monetary Gain for The Recipient

Monetary gain is also a sign of phishing in emails. Hong (2012) described filling out a survey in exchange for a cash award. Cash reward is promised as a result from action from the participant. This sign of phishing is usually accompanied by a request for the victim’s bank account number to have a deposit directly sent to the victim’s account.

The famous Nigerian Prince scam, or the Nigerian 419 scams are an example of monetary gain as a sign of phishing in emails. The scam offers free money in exchange for helping the attacker send large amounts of money. This style of attack has migrated to social media platforms as spoofed accounts appearing to be accounts of the victim's friends asking for money or donations, as illustrated in Figure 3. The Nigerian prince scam is still alive and well today through the social engineering channel of email ("What motivates people to click: Phishing examples and techniques used", 2018).

Figure 3

Sign of Phishing in Email: Monetary Gain



Money for you

From: john_alison444@qwerty.com
To: Jane Doe

Received yesterday at 6:04 PM

Greetings to you my friend,

I know this will come to you as a suprise because you don't know me. I am John Alison I work in Central Bank of Nigeria, Packaging and courier department. I got your contact among others from a search on the Internet and I was inspired to seek your co-operation, I want you to help me clear this consignment that is already in the Europe which I shipped through our CBN accredited courier agent. The content of the package is $20,000,000.00 all in $100 bills, but the courier company does not know that the consignment contains money. All I want you to do for me now is to give me your mailing address, your private phone and fax number, and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must not be reveled to anybody.
If this arrangement is okay by you, you can call

Phone: +234 8028776685
Email: john_alison444@qwerty.com

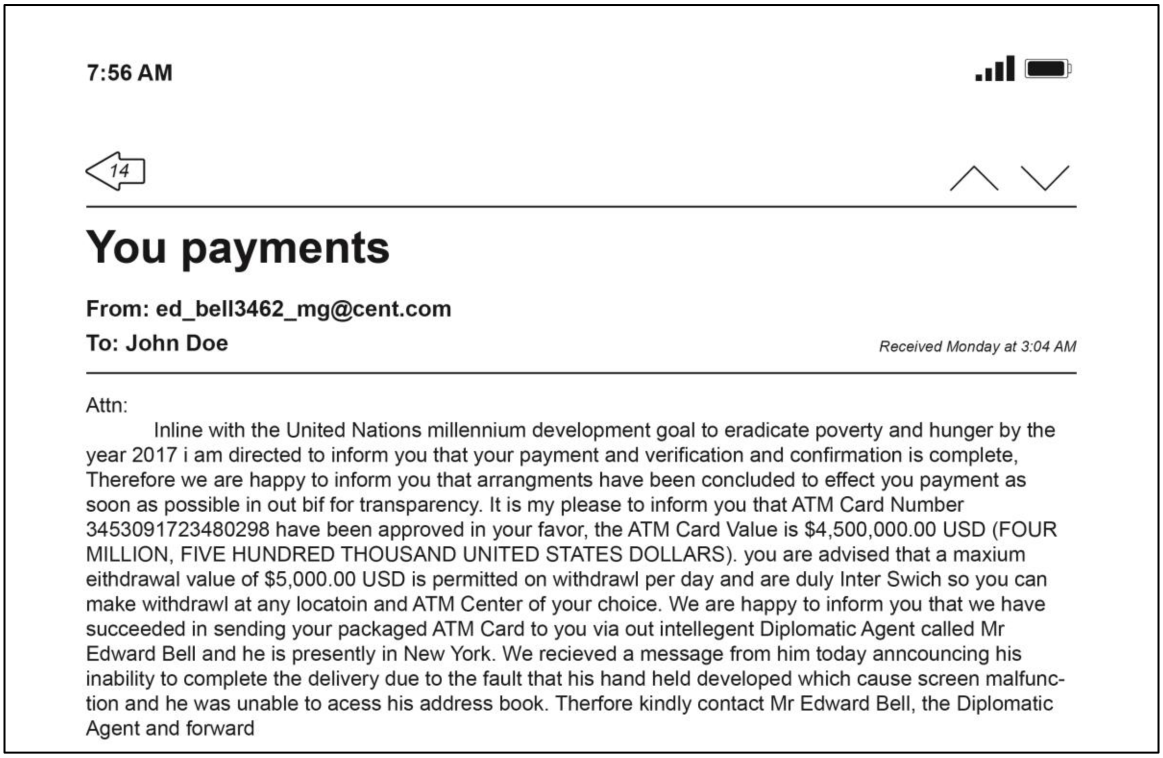
Misspelling and Grammar Issues

Misspelling and grammar errors in emails can be another sign of phishing in emails as shown in Figure 4. Incorrect use of words, fragmented sentences, improper word choice and misspelled words are cues to this sign of phishing (Caputo et al., 2014).

Grammar errors are common in phishing emails crafted for recipients that are not in the senders' primary language spoken or are usually due to rushing to send out the emails. With spellcheck and other grammar assistants with word processors, this sign of phishing should be easily spotted ("Phishing Emails", 2018). Misspelling of a spoofed account can also be common for example of phishing (Hong, 2012). Punctuation errors as well as odd or incorrect spacing may also fall under this category. Homographs may also be present in grammatical errors. Homographs are words with the same spelling but different meaning. These are usually used to persuade the recipient to click on a link ("Phishing Emails" 2018).

Figure 4

Sign of Phishing in Email: Misspelling and Grammar Issues



You payments

From: ed_bell3462_mg@cent.com
To: John Doe

Received Monday at 3:04 AM

Attn:

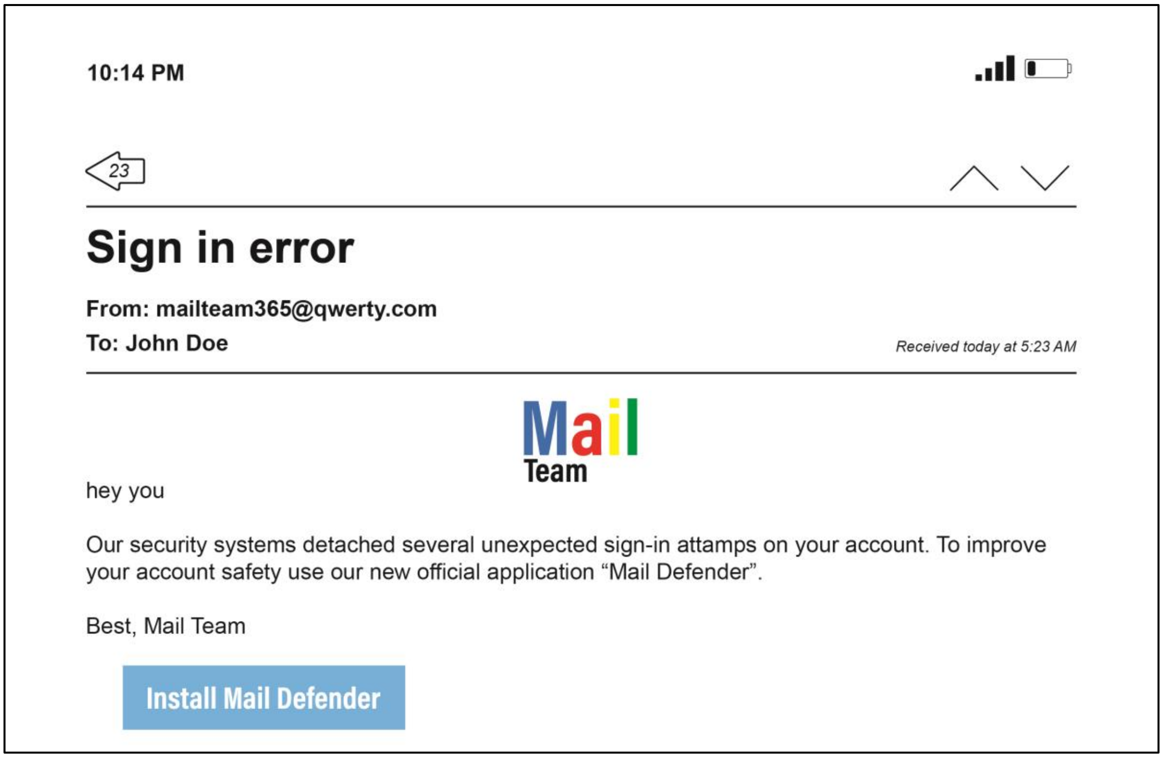
Inline with the United Nations millennium development goal to eradicate poverty and hunger by the year 2017 i am directed to inform you that your payment and verification and confirmation is complete, Therefore we are happy to inform you that arrangments have been concluded to effect you payment as soon as possible in out bif for transparency. It is my please to inform you that ATM Card Number 3453091723480298 have been approved in your favor, the ATM Card Value is $4,500,000.00 USD (FOUR MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS). you are advised that a maxium eithdrawal value of $5,000.00 USD is permitted on withdrawl per day and are duly Inter Swich so you can make withdrawl at any locatoin and ATM Center of your choice. We are happy to inform you that we have succeeded in sending your packaged ATM Card to you via out intellegent Diplomatic Agent called Mr Edward Bell and he is presently in New York. We recieved a message from him today anncouncing his inability to complete the delivery due to the fault that his hand held developed which cause screen malfunction and he was unable to acess his address book. Therfore kindly contact Mr Edward Bell, the Diplomatic Agent and forward

Greeting Errors

Greeting errors such as impersonal greeting, formal greeting, or unexpected greeting, are another sign of phishing in emails as shown in Figure 5. If the recipient is normally addressed from the sender with “Hi”, the recipient does not expect to see “Hey” from the sender. Sirull (2019) described other examples of this sign of phishing in emails as addressing the recipient in a formal way with “Dear Sir or Madam”. Another example is addressing the recipient as “Dear User” or “Valued Customer”, (Hacquebord, 2017). Figure 5 illustrates an incorrect greeting error of “hey you” from a sender that would not address the customer in that way.

Figure 5

Sign of Phishing in Email: Greeting Errors



Sign in error

From: mailteam365@qwerty.com

To: John Doe

Received today at 5:23 AM

hey you

Our security systems detached several unexpected sign-in attamps on your account. To improve your account safety use our new official application “Mail Defender”.

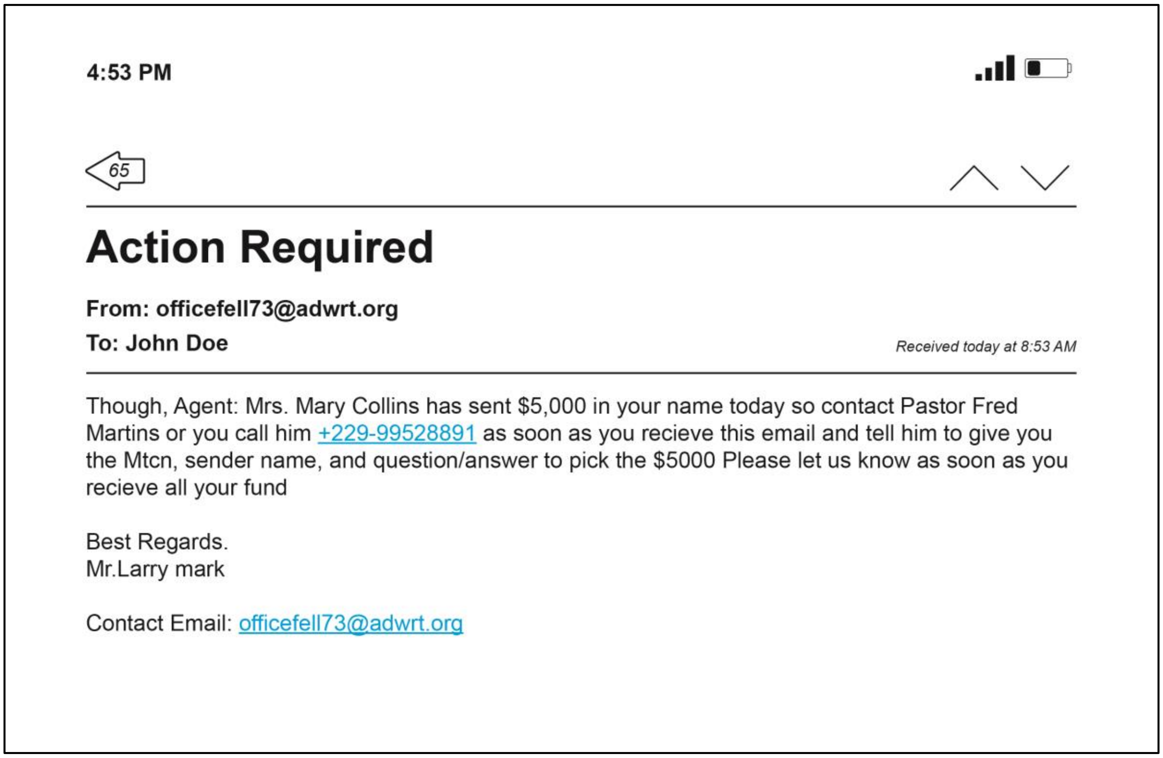
Best, Mail Team

Signature Errors

Signature errors such as Incorrect/Unexpected Signature include missing information that should be contained in the signature such as phone number, address, title and additional contact information (Hegde, 2019; Sirull, 2019). Missing this type of contact information, especially for emails requesting or promising financial implications can be a red flag for suspicion when identifying signs of phishing in emails, as illustrated in Figure 6. Additionally, a sender including their email address in the signature block could also be a signature error.

Figure 6

Sign of Phishing in Email: Signature Errors



Action Required

From: officefell73@adwrt.org
To: John Doe
Received today at 8:53 AM

Though, Agent: Mrs. Mary Collins has sent $5,000 in your name today so contact Pastor Fred Martins or you call him +229-99528891 as soon as you recieve this email and tell him to give you the Mtcn, sender name, and question/answer to pick the $5000 Please let us know as soon as you recieve all your fund

Best Regards.
Mr.Larry mark

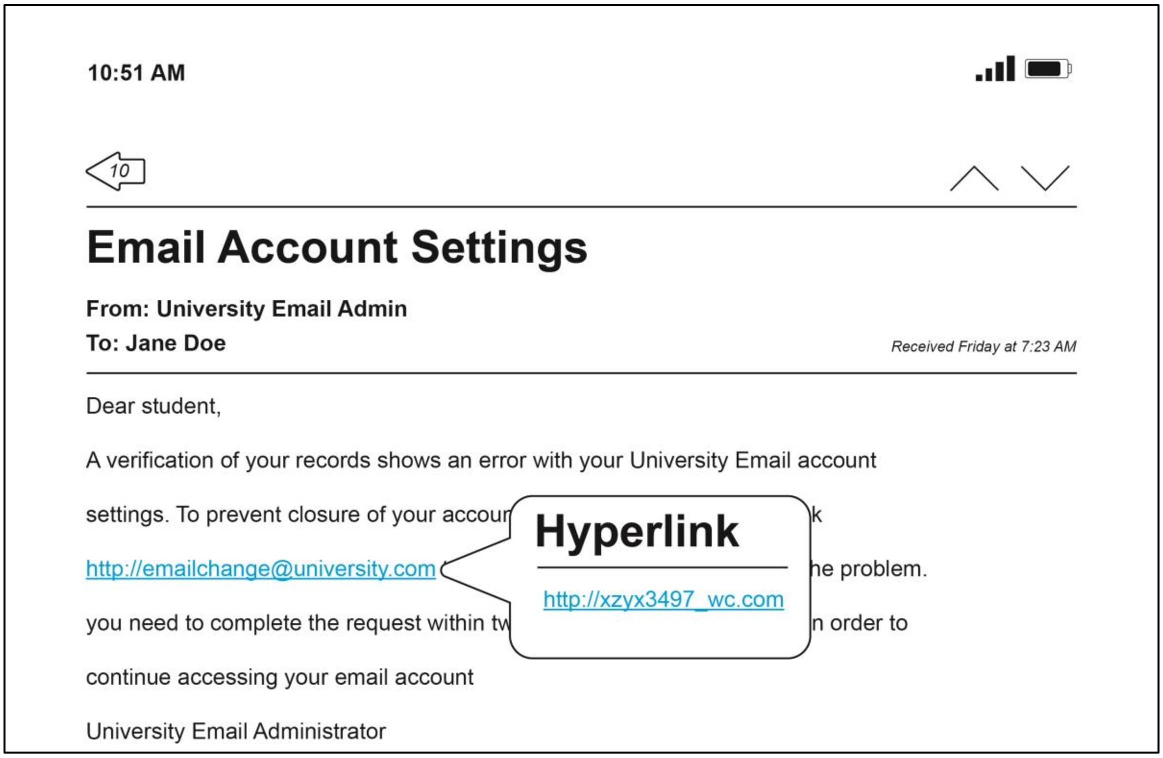
Contact Email: officefell73@adwrt.org

Incorrect URL

Incorrect URL encompass issues with the URL continued in the email. In some cases the target link does not match the link text (Berls, 2016). Misspelled URL's are also common and a sign of phishing in an email (Hale et al., 2015). Hovering over URL’s will allow the recipient to examine the text of the URL. Some signs of phishing include link masks, shortened URL’s, incorrect email address from the sender, and hyperlinks leading to a different URL than what is expected, as shown in Figure 7.

Figure 7

Sign of Phishing in Email: Incorrect URL



Email Account Settings

From: University Email Admin
To: Jane Doe
Received Friday at 7:23 AM

Dear student,

A verification of your records shows an error with your University Email account settings. To prevent closure of your accour k http://emailchange@university.com he problem. you need to complete the request within tw n order to continue accessing your email account

University Email Administrator

Hyperlink

http://xzyx3497_wc.com

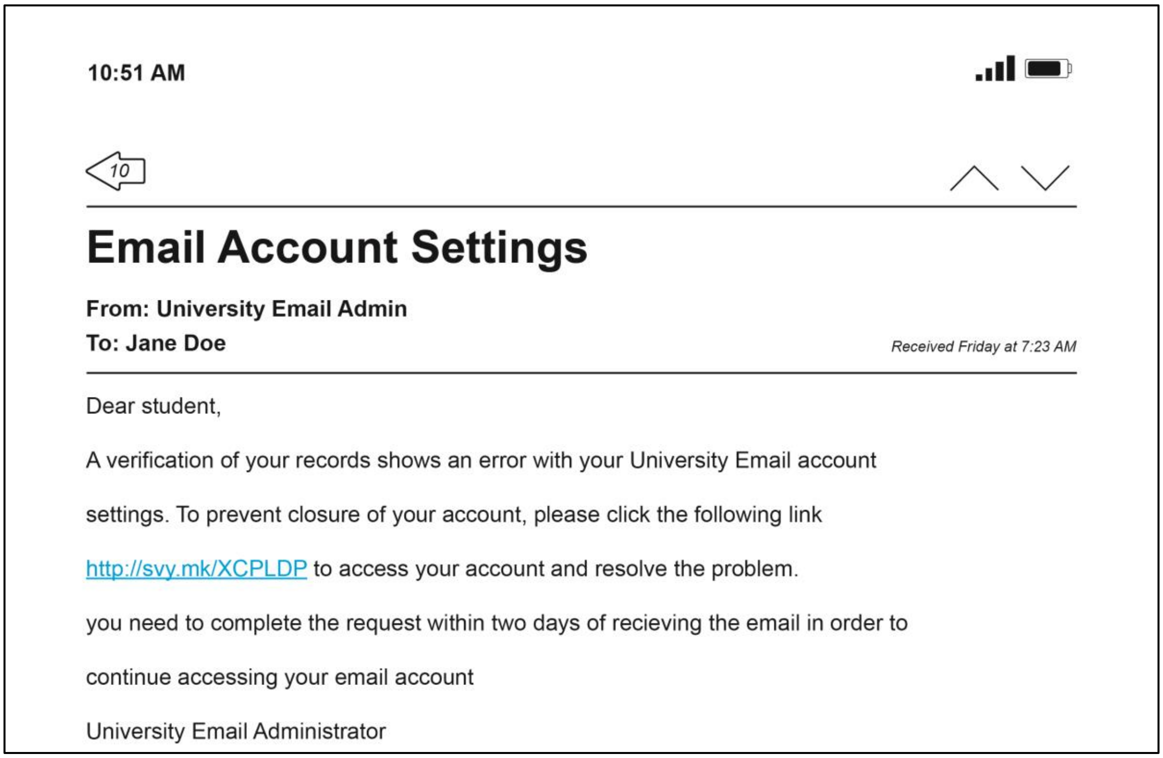
Requesting the Recipient to Click on Links

Request to click on links are a sign of phishing in emails that is sometimes characterized by asking the user to “Please click on the following link”. Misleading links can be masked as a legitimate site (Vishwanath et al., 2018). Yates and Harris (2015) indicated links should be typed, not copied, to the browser when requested from an email. An example of requesting the recipient to click on a link is shown in

Figure 8. In this example, the recipient is asked to click on a link to accept new terms and conditions (“Phishing Scam”, 2017).

Figure 8

Sign of Phishing in Email: Request to Click on Links



Email Account Settings

From: University Email Admin
To: Jane Doe

Received Friday at 7:23 AM

Dear student,

A verification of your records shows an error with your University Email account settings. To prevent closure of your account, please click the following link http://svy.mk/XCPLDP to access your account and resolve the problem.

you need to complete the request within two days of recieving the email in order to continue accessing your email account

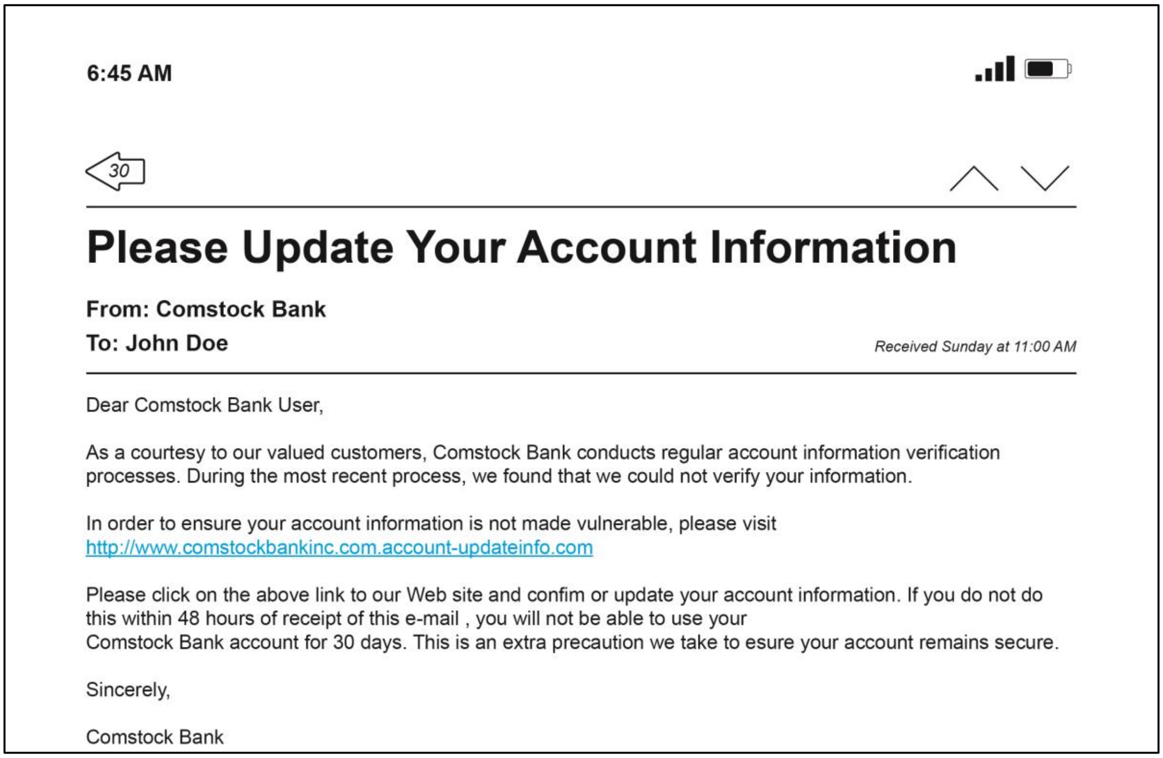
University Email Administrator

Request for Information from the Recipient

Requests for information from the recipient is also a sign of phishing in email (Hale et al., 2015). Phishing attempts will ask the recipient for password information, username used on websites, personal information, health information, and payment card data. Sirull (2019) indicated the sender should already have the information being requested from the recipient. An example of this sign of phishing is shown in Figure 9. In this example the recipient is directed to click on a link and then enter personal information (“What Is Phishing?”, 2018).

Figure 9

Sign of Phishing in Email: Request for Information



Please Update Your Account Information

From: Comstock Bank
To: John Doe

Received Sunday at 11:00 AM

Dear Comstock Bank User,

As a courtesy to our valued customers, Comstock Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit
http://www.comstockbankinc.com.account-updateinfo.com

Please click on the above link to our Web site and confim or update your account information. If you do not do this within 48 hours of receipt of this e-mail , you will not be able to use your
Comstock Bank account for 30 days. This is an extra precaution we take to esure your account remains secure.

Sincerely,

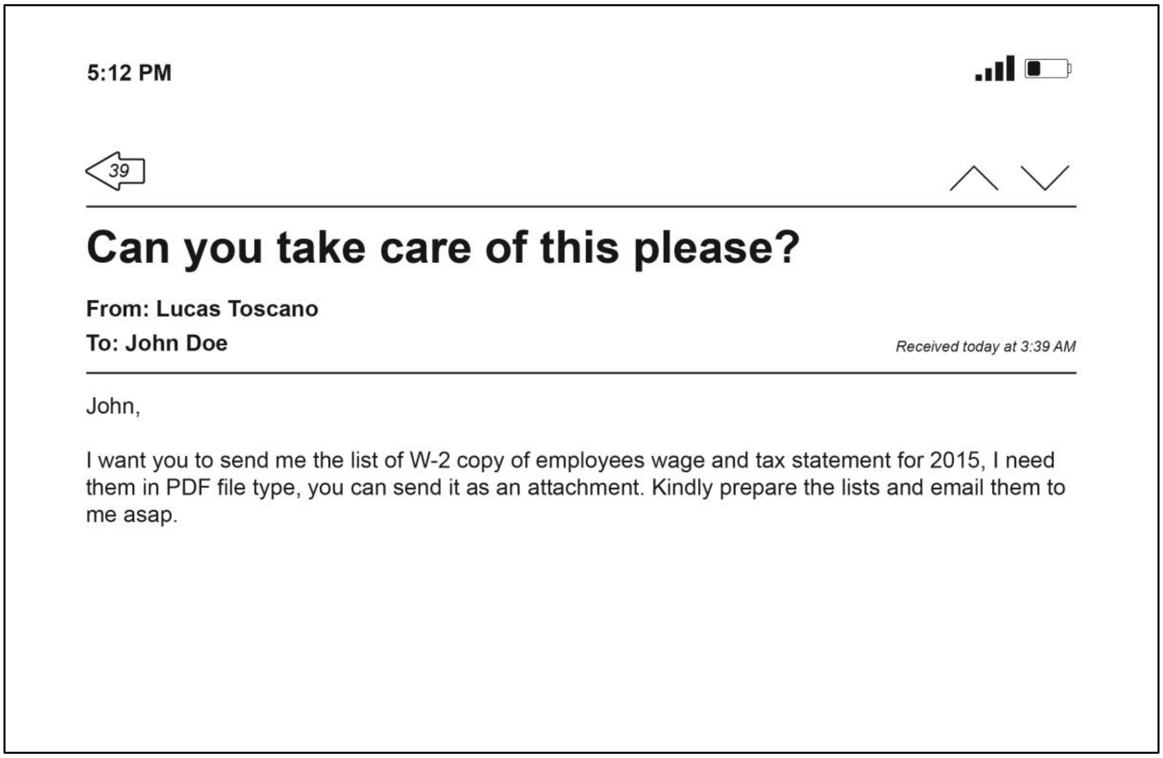
Comstock Bank

Spoofed Content or Spoofed Sender

Spoofed content and Spoofed sender are a common sign of phishing in emails. Emails such as the one shown in Figure 10, appear to be from coworkers, family, or even businesses the recipient has accounts with such as Paypal, Bank of America, or other accounts (Caputo et al., 2014). The emails may also appear to come from the recipient’s manager or boss. Another spoofed sender would be the CEO or other executive from the participant’s place of employment (Dakpa & Augustine, 2017).

Figure 10

Sign of Phishing in Email: Spoofed Sender or Content



Can you take care of this please?

From: Lucas Toscano

To: John Doe

Received today at 3:39 AM

John,

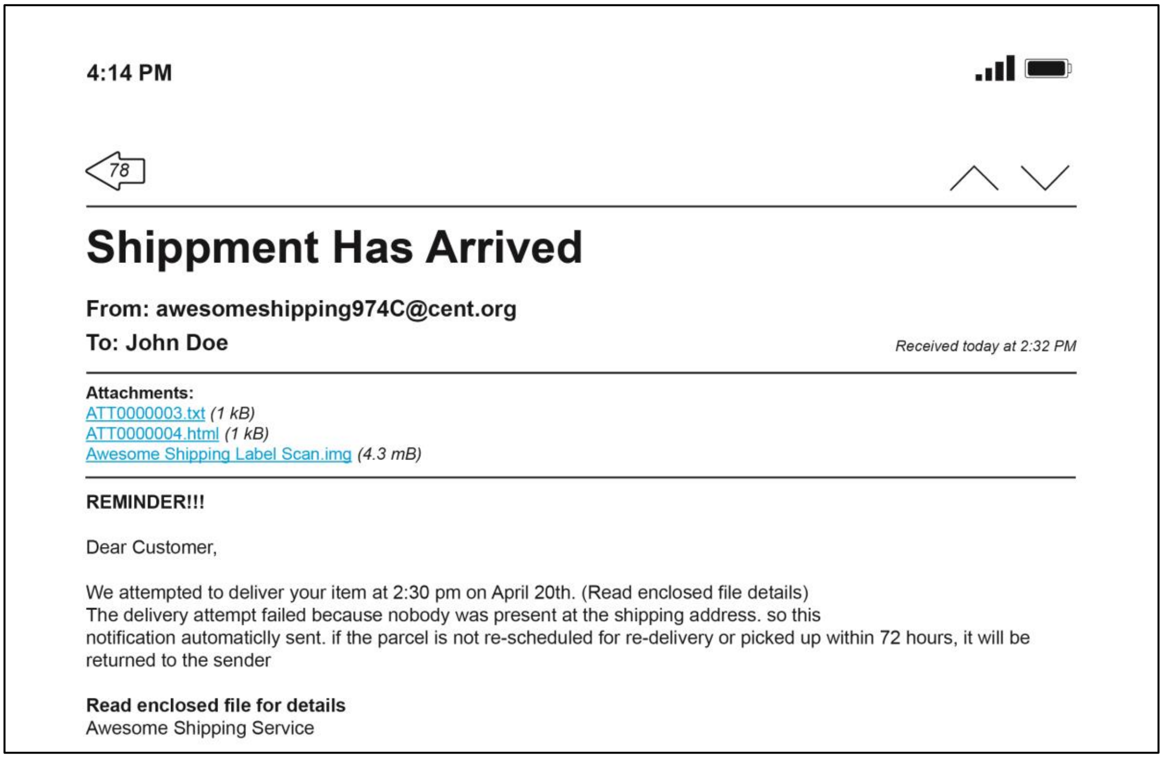
I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

Unsolicited or Unexpected Attachments

Unsolicited or Unexpected Attachments can also be a sign of phishing in emails. Opening an attachment can sometimes infect the recipient’s device with virus or spyware (Wyro, 2019). This sign of phishing in emails asks the recipient to open attachments that the recipient did not ask for, or expect (Sirull, 2019). Email containing this sign of phishing can appear to look like Figure 11.

Figure 11

Sign of Phishing in Email: Unsolicited Attachment



Shippment Has Arrived

From: awesomeshipping974C@cent.org
To: John Doe

Received today at 2:32 PM

Attachments:
ATT0000003.txt *(1 kB)*
ATT0000004.html *(1 kB)*
Awesome Shipping Label Scan.img *(4.3 mB)*

REMINDER!!!

Dear Customer,

We attempted to deliver your item at 2:30 pm on April 20th. (Read enclosed file details)
The delivery attempt failed because nobody was present at the shipping address. so this
notification automaticlly sent. if the parcel is not re-scheduled for re-delivery or picked up within 72 hours, it will be
returned to the sender

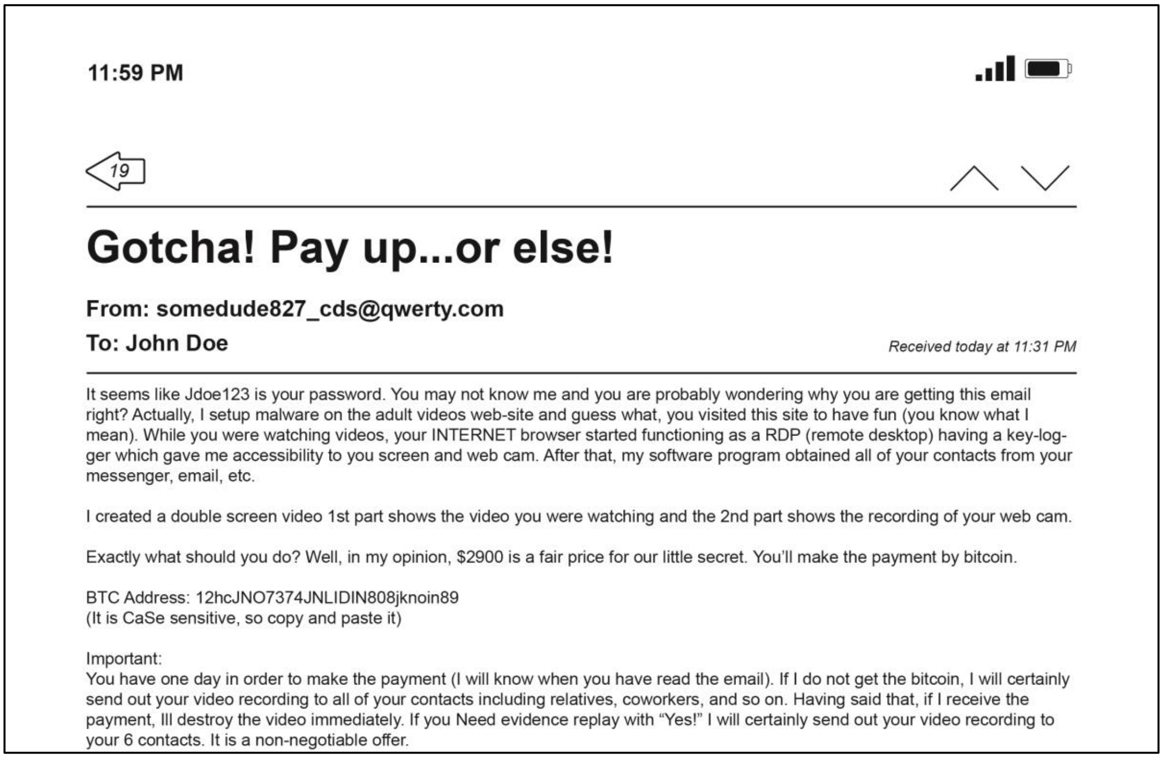
Read enclosed file for details
Awesome Shipping Service

Threatening Language

Threatening language can be a sign of phishing in emails presented in several forms. Some emails such as this can be a result of a previous phishing attempt resulting in a ransomware attempt towards the recipient (Abrams, 2018). Some threatening language emails contain a “do this now, or you will pay” tone to the message. A threatening language sign of phishing email with ransomware language is illustrated in Figure 12.

Figure 12

Sign of Phishing in Email: Threatening Language



Gotcha! Pay up...or else!

From: somedude827_cds@qwerty.com

To: John Doe

Received today at 11:31 PM

It seems like Jdoe123 is your password. You may not know me and you are probably wondering why you are getting this email right? Actually, I setup malware on the adult videos web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your INTERNET browser started functioning as a RDP (remote desktop) having a key-logger which gave me accessibility to you screen and web cam. After that, my software program obtained all of your contacts from your messenger, email, etc.

I created a double screen video 1st part shows the video you were watching and the 2nd part shows the recording of your web cam.

Exactly what should you do? Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by bitcoin.

BTC Address: 12hcJNO7374JNLIDIN808jknoin89
(It is CaSe sensitive, so copy and paste it)

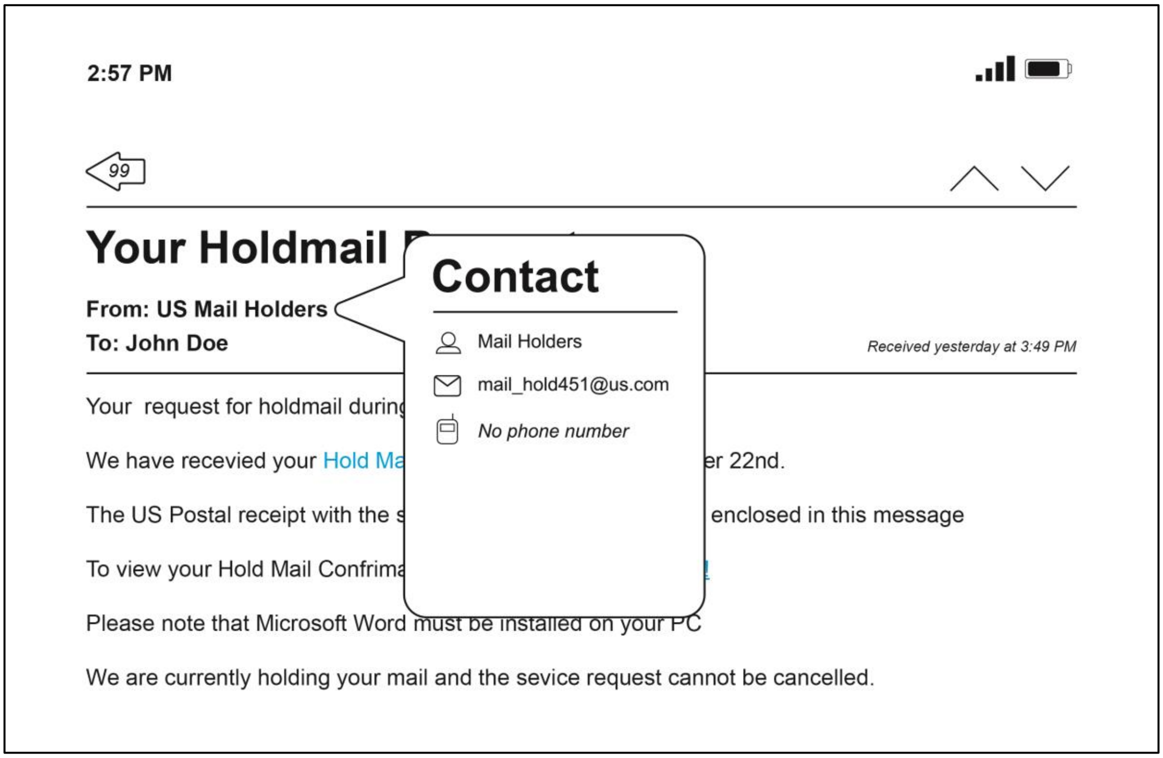
Important:
You have one day in order to make the payment (I will know when you have read the email). If I do not get the bitcoin, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, Ill destroy the video immediately. If you Need evidence replay with "Yes!" I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer.

Email Address Mismatch

Molinaro and Bolton (2017) indicated address mismatch is a common sign of phishing in emails where the from address does not match the reply address as illustrated in Figure 13.

Figure 13

Sign of Phishing in Email: Sender Address Mismatch



Your Holdmail

From: US Mail Holders

To: John Doe

Received yesterday at 3:49 PM

Contact

Mail Holders

mail_hold451@us.com

No phone number

Your request for holdmail durin

We have recevied your Hold Ma er 22nd.

The US Postal receipt with the s enclosed in this message

To view your Hold Mail Confrima

Please note that Microsoft Word must be installed on your PC

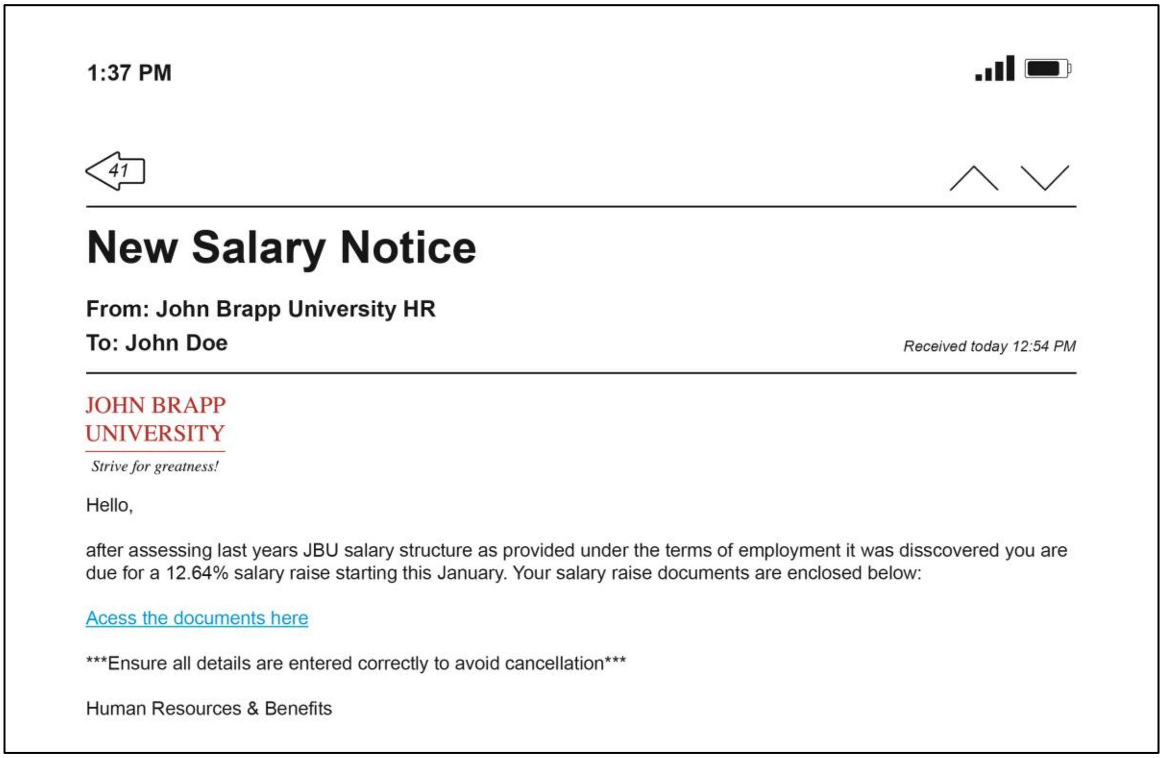
We are currently holding your mail and the sevice request cannot be cancelled.

Highly Personalized Emails

Highly personalized emails can indicate the sender has studied the recipient through social media or search techniques (“Phishing Emails – What’s the risk, how to identify them and deal with them”, 2019), which can be difficult to determine if an attacker has studied the victim extremely well. Some examples of this sign of phishing in emails include specific information social engineers can obtain from social medial sites to craft an email that will grab the recipient’s attention (Corsica Technologies, 2018). Figure 14 describes this type of sign of phishing as a salary increase from the recipient’s place of employment.

Figure 14

Sign of Phishing in Email: Highly Personalized



New Salary Notice

From: John Brapp University HR

To: John Doe

Received today 12:54 PM

JOHN BRAPP UNIVERSITY

Strive for greatness!

Hello,

after assessing last years JBU salary structure as provided under the terms of employment it was disscovered you are due for a 12.64% salary raise starting this January. Your salary raise documents are enclosed below:

Acess the documents here

Ensure all details are entered correctly to avoid cancellation

Human Resources & Benefits

Many examples of recent phishing attempts exist online or in literature. As previously discussed, several signs of phishing in emails can be combined into one email to increase the chances of tricking the recipient. For purposes of this study, one “main” sign of phishing in email will be used for each example to obtain SMEs ranking preferences for the top signs of phishing in emails. As illustrated through Figures 2-15, many signs of phishing exist today and are still tricking recipients into clicking links, and/or divulging personal information, despite user training methods.

Table 2

Summary of Signs of Phishing in Emails from Literature

Sign Number	Signs of Phishing in Email Characteristics	Literature Sources	Description from Literature	Figure Example Source
1	Urgency	Chandrasekaran et al., 2006; Sheng et al., 2010, Hong, 2012	Attempting to invoke an impulse emergency response from the recipient. A needed response from the user as soon as possible.	Wash & Cooper, 2018
2	Requiring action from the participant	Dakpa & Augustine, 2017; Sirull, 2019	Plays upon urgency, and requests action from the recipient in order to correct a situation.	"Phishing Emails – What's the risk, how to identify them and deal with them", 2019
3	Monetary gain for the participant	Hale et al., 2015	A cash reward is promised as a result from action from the recipient.	What motivates people to click: Phishing examples and techniques used", 2018

Table 2

Summary of Signs of Phishing in Emails from Literature - (continued)

Sign Number	**Signs of Phishing in Email Characteristics**	**Literature Sources**	**Description from Literature**	**Figure Example Source**
4	Misspelling and/or grammar errors	Caputo et al., 2014; Dakpa & Augustine, 2017; Hale et al., 2015; Sirull, 2019; Yates & Harris, 2015	Incorrect use of words, fragmented sentences, improper word choice, and words misspelled in an email. Usually due to senders rushing to write the email	"Phishing Emails", 2018
5	Greeting errors	Dakpa & Augustine, 2017; Hale et al., 2015; Sheng et al., 2010; Sirull, 2019	Not addressing the recipient as expected. Too personal, or formal of a greeting. "Dear account holder" instead of name (Sirull, 2019)	Hacquebord, 2017
6	Signature errors	Hegde, 2019; Sirull, 2019;	Sender not signing an email as expected. Missing or too much information	"Phishing Emails", 2018

Table 2

Summary of Signs of Phishing in Emails from Literature - (continued)

Sign Number	Signs of Phishing in Email Characteristics	Literature Sources	Description from Literature	Figure Example Source
7	Incorrect URL	Hale et al., 2015; Sheng et al., 2010; Sirull, 2019	URL does not match the description of what the recipient expected. (When hovering over the url it does not match the indicated text)	Berls, 2016
8	Requresting the participant to click on links	Vishwanath et al., 2018; Yates & Harris, 2015	Plays upon urgency, asking the recipient to "click here."	Vishwanath, Harrison, & Ng, 2018
9	Request for information	Hale et al., 2015; Sirull, 2019	Asking the recipient for personal information, files or unexpected items. Asking the recipient to send or input personal data that the sender should already have.	"What is phishing", 2018

Table 2

Summary of Signs of Phishing in Emails from Literature - (continued)

Sign Number	Signs of Phishing in Email Characteristics	Literature Sources	Description from Literature	Figure Example Source
10	Spoofed content and/or spoofed sender	Caputo et al., 2014; Dakpa & Augustine, 2017; Sirull, 2019; Yates & Harris, 2015	Content appears to be from a familiar or reputable source. Sender appears to be from a familiar source. Clone fishing. (An email appearing to be from your bank, but the logo is odd looking)	Corsica Technologies, 2017
11	Unsolicited and/or unexpected attachments	Hale et al., 2015; Sirull, 2019; Vishwanath et al., 2018	Attachments the recipient did not ask for or expect in the email.	Wyro, 2019
12	Threatening language	Molinaro & Bolton, 2018; Sirull, 2019	Addressing the recipient in an aggressive manner. “Do this now or your will pay.”	Abrams, 2018

Table 2

Summary of Signs of Phishing in Emails from Literature - (continued)

Sign Number	Signs of Phishing in Email Characteristics	Literature Sources	Description from Literature	Figure Example Source
13	Address mismatch	Molinaro & Bolton, 2018; Sirull, 2019	The email address of the sender does not match the expected sender.	“Watch your inbox for fake postal service emails”, 2017
14	Highly personalized emails	“Phishing Emails – What’s the risk, how to identify them and deal with them.”2019	Emails containing too many or too good to be true details for the recipient. “You have received a raise from your place of employment.”	Corsica Technologies, 2017

User Phishing Training

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 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.

Several approaches to end-user phishing training have been used to better train end-users to the dangers of social engineering and phishing. Foundational research in this area include Kumaraguru et al. (2009) who tested an embedded anti-phishing training system, PhishGuru with 515 participants. PhishGuru trained participants to recognize signs of phishing in email by delivering training messages after the user clicked URL links in the phishing email (Kumaraguru, 2009). The training was delivered several times over a 35-day period. Their results concluded that users with anti-phishing training appear to be less vulnerable to phishing attempts against them as compared to participants that did not receive anti-phishing training. On the other hand, Caputo et al. (2014) determined embedded training did not reduce click rates on phishing emails. They also suggested repetitive phishing training might yield better results over short-term training.

Several styles of phishing training have been researched. Wash and Cooper (2018) studied a phishing training method utilizing immediate feedback training from simulated peers or experts. Facts-and-advice training was similar to common phishing training today from experts, or rule-based training. “Stores” was a training style crafted to appear to tell a story about a phishing experience. Simulated phishing messages were presented to the user, and training was delivered if the user clicked on a simulated phishing link. Facts-and-advice style training led to lower click rates when appearing to come from an expert, while stories-based training appeared to have a lower click rate when appearing to come from a peer (Wash & Cooper, 2018). Jensen et al. (2017), also utilized simulated phishing messages and introduced a combination of rule-based and mindfulness training over a multi-day time period. Their study concluded that mindfulness techniques show promise as a phishing training method.

Gamification strategies, such as Anti-Phishing Phil (Sheng et al., 2007) uses an interactive approach to training users to notice signs of phishing websites. Their research concluded that gamification interaction can be an effective way to train users to notice phishing signs (Sheng et al., 2007). Hale et al. (2014) began developing an anti-phishing game that encompasses email simulation, email inbox simulation, web browser simulation, and social medial simulation. Several end-user training strategies exist in literature. Contributions to the area of research include recognizing when a user cannot distinguish between a legitimate website and a spoofed website or email, and that anti-phishing training participants are less likely to click on real phishing messages than those that do not.

Table 3

Summary of Phishing End-User Training Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Caputo et al., 2014	Empirical study via experiment	813	Embedded phishing training through email	Creating and implementing embedded training effective in a corporate setting is difficult.
Dhamija et al., 2006	Empirical study via experiment	22	Website	Many users cannot distinguish between a legitimate website and a spoofed/phishing website

Table 3

Summary of Phishing End-User Training Literature –(continued)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Jensen et al., 2017	Empirical study via experiment	355	Rule based and Mindfulness Phishing training interventions	Evidence supporting a mindfulness-based phishing training may help reduce, but not eliminate, phishing risk.
Kumaraguru et al., 2009	Empirical study via experiment	515	PhishGuru-embedded anti-training system	Participants that saw the anti-phishing training are less likely to click on real phishing messages than those that did not receive training.
Miranda, 2018	Literature review and synthesis		Phishing training best practices	Risks associated with phishing threat can be reasonably mitigated by a measurable phishing training program.
Sheng et al., 2007	Empirical study via experiment	42	Anti-Phishing Phil Interactive Game	Participants who played Anti-Phishing Phil performed better at identifying phishing websites than those that did not.

Table 3

Summary of Phishing End-User Training Literature – (continued)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wash & Cooper, 2018	Empirical study via experiment	1,945	Phishing training via email	Facts -and-advice training leads to lower likelihood of clicking on a phishing link when appearing to be from an expert than from a peer.

Phishing Email Filtering Tools and Warning Systems

There are several email filtering solutions available today as a way to warn users of signs of phishing in emails. Most warnings are visual popup windows and/or buttons to click 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).

Google attempts to warn users of suspicious emails in Gmail by utilizing visual alert banner messages that appear at the top of suspicious emails ("Can Gmail Detect Phishing Scams?" 2019). Microsoft Office 365 includes anti-phishing protection and warns users with visual alert messages and reporting buttons (Palarchio, 2016). Proofpoint is an integrated security application. Their anti-phishing solution utilized PhishAlarm, a tool that filters email and visually alerts the user to a sign of phishing email as a secondary image appears on the email screen ("PhishAlarm and PhishAlarm Analyzer Features and Benefits", 2019). Barracuda offers anti-fraud and anti-phishing protection. Their product will pop up a visual warning to users if the URL is incorrect ("Anti-Fraud and Anti-Phishing Protection", 2019).

Phishing Susceptibility and Demographics

Research has been performed in the area of demographics and the relationship to users being susceptible to phishing attempts against them. The results of this research are important as it helps researchers understand if there is a specific demographic that is more susceptible to phishing than others, and most likely needs either additional or more specific training to assist the user in noticing signs of phishing. According to Darwish et al. (2012), understanding user demographics and backgrounds can help improve security awareness efforts and reduce phishing susceptibility.

Age, gender, education, and personality are a few demographics to consider towards predicting user's susceptibility. Age appears to be a strong predictor in user susceptibility towards phishing attacks. Kumaraguru et al. (2009) found that participants in the 18-25 age group were most susceptible to phishing attacks during a study of their PhishGuru training system. During earlier work in 2007, Kumaraguru et al. (2007) tested an online gamification training system, Anti-Phishing Phil - discovering the age group of 18 and younger were more susceptible than older age groups. Sheng et al. (2010) conducted an online case study and survey indicating the age group 18-25 are more susceptible to phishing.

Gender has also been studied as a data point towards demographic analysis towards phishing susceptibility. Several studies have concluded that women are more susceptible than men (Jegatic et al., 2007; Kumaraguru et al., 2009; Olivera, 2017; Sheng et al., 2009). Other studies show conflicting information; Sheng et al. (2007) found no significant correlation between participants gender, age, education or race in relation to phishing susceptibility. Education and training for users has been determined to be an important data point towards the ability to notice signs of phishing in emails and was covered in a previous section of this literature synthesis. More research in this specific area could benefit the field of demographics as it relates to phishing attempts, and thus, reduce the gap in literature.

Table 4

Phishing Susceptibility and Demographics Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Darwish et al., 2012	Literature synthesis			Review determined need for a machine learning model to predict phishing susceptibility based on demographic traits.
Jagatic et al., 2007	Empirical study via experiment	487	Online form sent to determine if participants would provide personal information	Female students were more susceptible to phishing attacks than male participants.
Oliveira et al., 2017	Empirical study via experiment	158	Email of phishing emails over a 21-day period	Need for personal demographic personalization for phishing warnings, training, and educational tools for older users.

Table 4

Phishing Susceptibility and Demographics Literature – (continued)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Sheng et al., 2007	Empirical study via experiment	5182	Online phishing study using Anti-Phishing Phil and interactive game	Found no significant correlation between participants gender, age, education, or race and susceptibility to phishing.
Sheng et al., 2010	Case study and survey	1001	Online survey	Women are more susceptible than men to phishing, age group 18-25 are more susceptible to phishing.

Audio/Visual/Haptic Alerts and Warnings

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. A 2007 Department of Transportation study determined enhances seat belt reminder systems utilizing sound, icon, and text increased front occupant seat belt use.

Additionally, rear-end collision systems are also in place, and being researched (Scott & Gray, 2008). Such systems combine audio/visual/haptic methods to alert the driver to potential issues. Scott and Gray (2008) determined there is promise in the area of using tactile methods to draw attention to hazards for the driver. Blind spot warnings such as a blinking light shown in the rearview mirror can also alert the driver of a car in their blind spot (“Should Your New Car Have Blind Spot Monitoring”, 2019).

Several visual icons exist today for warning drivers of issues with the car or driving conditions (Greene, 2016). Dashboard icons alert the driver of engine issues, car running on auxiliary power or battery, slippery conditions or traction system, high temperature, gas tank low, and fasten seatbelt. There is also significant research dedicated to audio sounds and alerts played inside of vehicles (Krisher, 2016). According to Krisher (2016), the average car has 10-15 different sounds played for various alerts and warnings. Alerts and warnings are tested on drivers in research studies to determine if the sound is effective as a warning, or if the sound is distracting (Kirsher, 2016).

Jensen et al. (2011) concluded through a simulated driving experiment on 25 participants that steering wheel vibrations (or haptic feedback) provided an overall improvement in driver safety using steering wheel haptic feedback to avoid hitting obstacles. Vibrations can happen at increased intensity to alert the driver of increasingly urgent situations (Jensen et al., 2011). Vibrating seats are another use of haptic warnings for drivers. Steering wheel and seat vibrations are used by several automotive manufacturers today to warn drivers of potential danger such as lane departures and road hazards (Kane, 2012). Research by van der Heiden et al. (2016) discovered that audio/visual/haptic alerts and warnings should be given in a timely manner. Their study of 40 driver simulated participants indicated alerts and warnings are helpful for lane-change departures but must be given at least 500m before potential collision (van der Hidden et al., 2016).

Collision warning systems for vehicles using audio/visual/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 collisions by warning and alerting the driver of potential hazards (ACAS Program Final Report, 1998).

Other areas consumers benefit from audio/visual/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 ("Continuous Wireless Pressure Monitoring and Mapping with Ultra-Small Passive Sensors for Health Monitoring and Critical Care", 2019). 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).

Alerts and warnings containing audio/visual/haptic feedback for a user could reduce habituation to alerts and warnings but should be meaningfully interpreted by the user. This theory is derived from Kahneman (2011)'s theory of Thinking Fast and Slow related to the S2 thinking. Findling and Mayrhofer (2015) researched approaches to using haptic vibration as a feedback channel for consumers as it pertains to detecting if an electronic device is real or replaced by attackers. Participants were able to determine if the device was real by interpreting a vibration upon authenticating to the device. Hoggan et al. (2009) studied the meanings that can be conveyed through audio and haptic tactile feedback. For example: an audio and haptic combination should adequately convey urgency between a low phone battery warning, and a low heart rate warning (Hoggan et al., 2009). Hoggan et al. (2009) concluded that a thoughtful combination audio and tactile methods can be intuitively interpreted by the user. This finding stresses the importance of accurate representation of audio and tactile warnings that are suited properly for the urgency of the event.

Table 5

Alerts and Warnings in Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Findling & Mayrhofer, 2015	Empirical study via experiment	12	Android app	Vibration is a promising way to authenticate devices to users.
Freedman et al., 2007	Observational field data collection	40,000 passenger vehicles	Enhanced seat belt reminder system	Determined features were found to have significant effect on driver seat belt use.
Greene, 2016	Observational field data collection		Automotive dashboards	Collection of common automobile dashboard visual icons.
Hoggan et al., 2009	Empirical study via experiment	18	Stimulus ranking for audio and haptics	Combining audio and tactile methods information can be derived and urgency interpreted intuitively.

Table 5

Alerts and Warnings in Literature – (continued)

Jensen et al., 2011	Empirical study via experiment	25 simulator participants	Steering wheel haptic feedback	Overall improvement in driver safety using steering wheel haptic feedback to avoid hitting obstacles.
Krisher, 2016	Observational field data collection		Automotive sounds and alerts	The average car has 10-15 different sounds played for different reminders and alerts.
Lohr, 1974	Seatbelt warning system			Patent on seatbelt warning system.
Scott & Gray, 2008	Empirical study via experiment	16 simulator participants	Driving warning system	Tactile warnings show promise in reduced reaction time in rear-end collisions.
Van der Hidden et al., 2016	Field study via experiment	24 participants	Visual in-car warning system	Early visual in-car warning systems are effective.

User Use of Smartphones

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 (Nelson, 2017; van Rijn, 2019). Nelson (2017) 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.

Summary of What is Known and Unknown in Literature

It is known that most users are using smartphones and laptops to view and respond to emails daily (McLeod, 2018; van Rijn, 2019), and email phishing is the most common social engineering method (Hong, 2012). It is known that several signs of phishing in emails still exist today and continue to trick users into clicking links and divulge personal information to social engineers. Sense of urgency, requiring action from the recipient, promise of monetary gain, misspelling and grammar errors, greeting errors, signature errors, incorrect URL, requesting the recipient to click on links in the email, request for information from the recipient, spoofed content or sender, unsolicited or unexpected attachments in the email, threatening language, address mismatch, and highly personalized emails scams are continuing to lure users today.

It is known phishing training does work to lower the percentage of click rates on signs of phishing among users, however, phishing attacks remain a problem today (Abass, 2018). Visual alerting systems such as: Phishing training, phishing reporting buttons, alerting dashboards, phishing alert tools, and phishing warning systems, are showing promise of assisting users in noticing signs of phishing in emails sooner, and thus reducing the risk of business or personal financial loss through phishing attacks. A considerable gap in phishing alerting is noticeable regarding audio and haptic feedback as an alerting and warning mechanism for identifying signs of phishing in emails.

There is extreme importance placed on the ability for users to detect and respond to phishing attacks (Jensen et al., 2017). Anti-phishing training, yet effective, is not enough fully reduce phishing susceptibility. This research aims at improving ways to improve recognition time to signs of phishing in emails by alerting users to the signs of phishing in emails using audio/visual/haptic alerting on a smartphone and/or laptop. This study will also add to the body of knowledge surrounding demographics and phishing susceptibility, participant attention span, and the potential effect of phishing susceptibility.

It is known that alerts and warnings assist people in noticing danger in several areas of daily life sooner than if alerts and warnings were not present. Automobiles and vehicle warning examples such as blind spot indicators, lane departure warnings, seatbelt not fasted warnings are consistently being researched and improved. Applying alerts and warnings from automobiles to emails containing signs of phishing in emails could add to the body of research attempting to alert users to email danger sooner. It is unknown how users would respond to a combination of audio, visual, and haptic alerting for signs of phishing in email delivered on smartphones and laptops. It is also unknown if habituation would be an issue with over-alerting users to the signs of phishing in emails. This research study would examine and test this research area. Thus, it appears a gap in the literature would be reduced by performing a phishing alerting and warning study utilizing audio/visual/haptic alerts on the signs of phishing in emails with participants. By conducting preliminary questions regarding demographics and attention span, additional research to the body demographic indicators in phishing could be used. The PAWS mobile application could then be used to effectively test user reaction time to signs of phishing in emails after presented with audio/visual/haptic delivered alerts on mobile devices.

Chapter 3

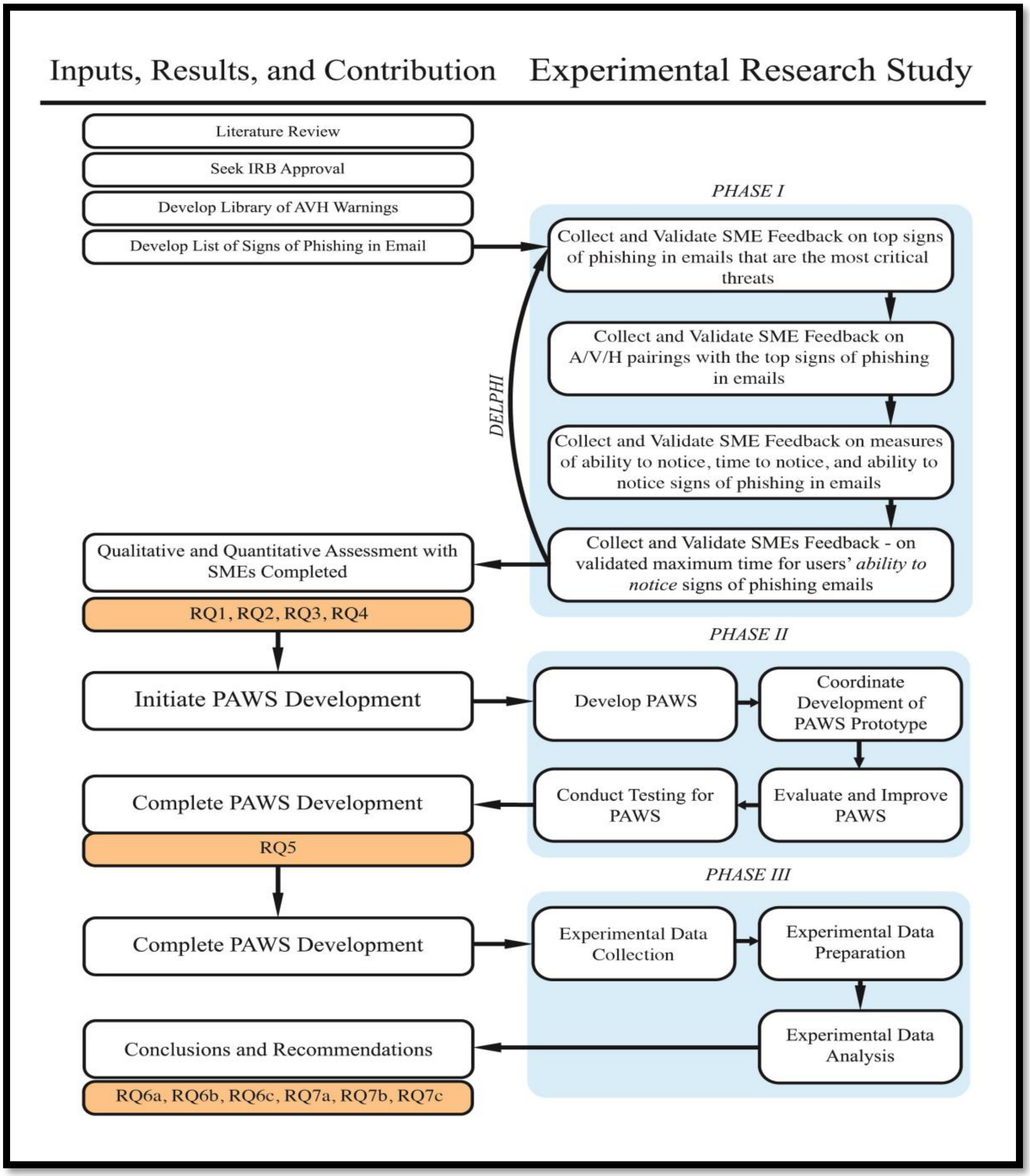
Methodology

Overview of Research Design

This research study was conducted in three phases as shown in Figure 15. The development and testing of the PAWS mobile app prototype assisted users in noticing signs of phishing in emails through alerting and warning by audio/visual/haptic alerts. Also defined as a "thing", the PAWS prototype addressed a problem, which is the foundation of developmental research (Ellis & Levy, 2009). Defined as sequential exploratory research by Creswell and Creswell (2017), this developmental research study empirically assessed participants' results through both qualitative and quantitative data analysis that built into sequential phases of a qualitative step followed by a quantitative data analysis step. The methodological research design for this study included sequential exploratory research design (Creswell, 2017). According to Ivankova et al. (2006), sequential exploratory research design is a valid methodology for developmental research, especially when conducting applied research.

Figure 15

Proposed Overview of the Research Design Process


Inputs, Results, and Contribution
Experimental Research Study
Literature Review
Seek IRB Approval
Develop Library of AVH Warnings
Develop List of Signs of Phishing in Email
PHASE I
Collect and Validate SME Feedback on top signs of phishing in emails that are the most critical threats
Collect and Validate SME Feedback on A/V/H pairings with the top signs of phishing in emails
Collect and Validate SME Feedback on measures of ability to notice, time to notice, and ability to notice signs of phishing in emails
Collect and Validate SMEs Feedback - on validated maximum time for users' ability to notice signs of phishing emails
DELPHI
Qualitative and Quantitative Assessment with SMEs Completed
RQ1, RQ2, RQ3, RQ4
PHASE II
Initiate PAWS Development
Develop PAWS
Coordinate Development of PAWS Prototype
Complete PAWS Development
Conduct Testing for PAWS
Evaluate and Improve PAWS
RQ5
PHASE III
Complete PAWS Development
Experimental Data Collection
Experimental Data Preparation
Conclusions and Recommendations
Experimental Data Analysis
RQ6a, RQ6b, RQ6c, RQ7a, RQ7b, RQ7c

The first phase of this research study utilized initial qualitative data collection phrase using Subject Matter Experts (SMEs) (Straub, 1989). The expert panel validated the initial signs of phishing in emails in ranked order, matched audio and visual warnings for each sign of phishing in email that (in the SMEs opinion) reflected the severity of the sign of phishing, and weighed in on an appropriate measures for *ability to notice* and *time to notice* phishing in emails by the users. The second phase of this research study encompassed the development and testing of PAWS. The third and final phase tested the effectiveness of audio, visual, and haptic alerting to the top signs of phishing in emails. This phases also included a qualitative and quantitative data collection with the PAWS mobile app participants (Straub, 1989).

This research study resulted in developing a mobile application, PAWS, that was used to conduct the research and testing of the effectiveness of audio/visual/haptic alerts and warnings to assist in reducing phishing susceptibility. As previously stated, users need improved ways to notice signs of phishing in emails, thus, preventing significant data and financial losses. Users are continuously clicking on phishing links and need better ways to alert them to not fall for phishing emails (Abass, 2018). PAWS mobile application development and testing adds to the body of research in this area.

Phase I

Utilizing the literature synthesis results in Chapter 2, a library of signs of phishing in email was developed into a list for the SMEs to rank the level of importance. Rank order and frequency analysis were used to determine what signs of phishing should be included in the PAWS mobile app. If all signs of phishing email screens include all alerts and warnings, or alert fatigue could result (Kesselheim, et al., 2011). Alert fatigue caused by excessive warnings could possibly be mitigated by highlighting the most important alerts and warnings (Kesselheim, et al., 2011). With user fatigue in mind, the top five signs of phishing were included in the programming of the PAWS mobile app.

The SMEs ranked what they felt the top signs of phishing in emails were. As indicated by Cooper (2014), narrowing down the top five (from 14 signs of phishing in email) are important as people summarize data in round ranking numbers as shown in Table 6. Isacc and Schindler (2014) described several top lists and indicated the importance of narrowing down "top" in categories. This listing and narrowing down of the top signs were utilized to reduce fatigue among PAWS mobile app participants. The initial survey instrument will be conducted using Survey Monkey, using Delphi methodology for expert feedback on this subject (Ramim & Lichvar, 2014), each SME received an email invitation to participate in the initial survey. Additional survey questions as well as the SME survey companion file examples are shown in Appendix A.

Table 6

SME Survey – List of Initial Signs of Phishing

Sign of Phishing	**Short Examples of Sign of Phishing**
Sense of urgency	Unusual log in activity/failed log in attempts – click here to log in Your account might be deleted Mailbox is almost full
Requiring action	Click here to review details Verify shipping address Routine action – password reset Update your account
Monetary gain	End user will receive a sum of money into their account if they help the sender Fill out a survey for $25.00

Table 6

SME Survey – List of Initial Signs of Phishing – (cont.)

Sign of Phishing	Short Examples of Sign of Phishing
Misspelling and grammar issues	Incorrect tense
	Misspelled body of text
	Misspelled sender
	Misspelled recipient
Greeting errors	Impersonal greeting – using “Hey” when the recipient expects “Hi”.
	Unexpected greeting – when expecting to be addressed differently
	Formal greeting – Dear Sir or Madam
Signature errors	Unexpected sign off – expecting Thank you, Mark
	Missing signature content – does not contain phone number, address
Incorrect URL	Target does not match the link text
	Misspelled url
	Shortened url
Request to click on links	Please click the following link
Request for information	Need your password, username
Spoofed sender or content	Email appearing to be from your boss
	Email appearing to be from your Friends list
	Email appearing to be from your LinkedIn connections
	Email appearing to be from Neflix, BoA or other accounts

Table 6

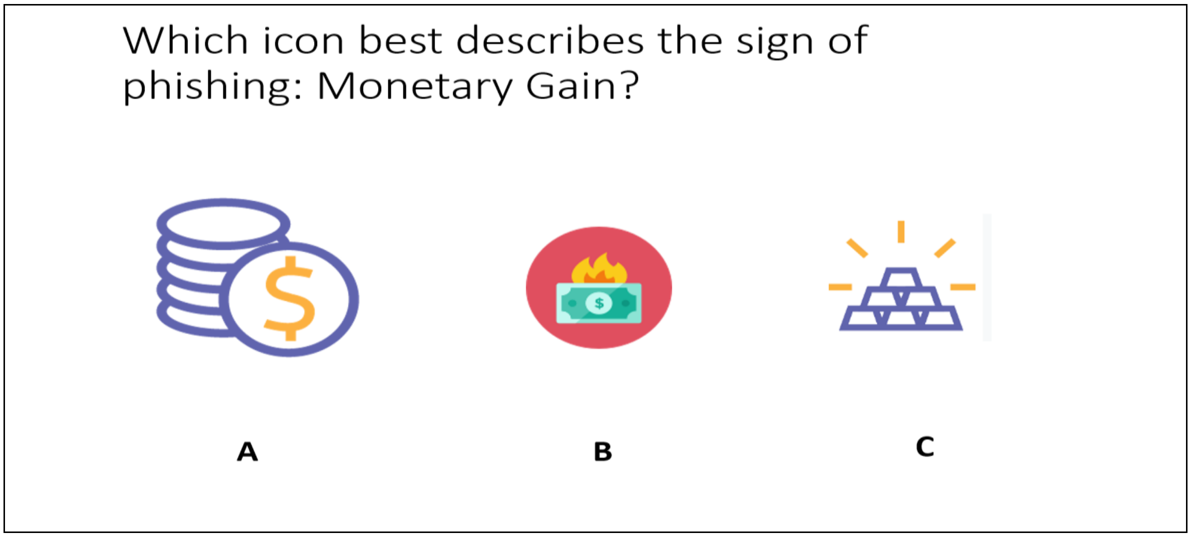
SME Survey – List of Initial Signs of Phishing – (cont.)

Sign of Phishing	Short Examples of Sign of Phishing
Unsolicited or unexpected attachments	Email with a file the end user did not ask for
Address mismatch	From address does not match the reply address
Threatening Language	You will have to pay X if you do not respond
Highly Personalized Emails	Spear phishing examples

The survey also included a library of icons and sounds for the SMEs to pair with the signs of phishing in emails that they find to be most important. The survey included visual icons and audio to assign to the top signs of phishing. An example of visual icon matching examples are shown in Figure 16. An example of audio matching is shown in Figure 17. This feedback assisted in pairing a sign of phishing in email to an icon and sound of matching severity. An example of the haptic pairing survey question is shown in Figure 18.

Figure 16

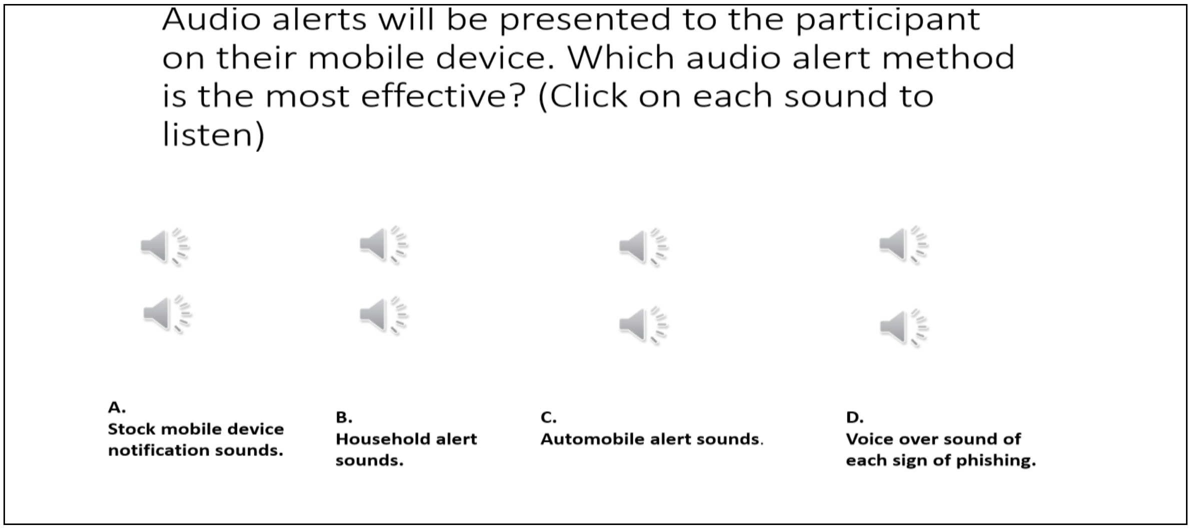
Example of SME Survey – Choose Visual Icon Alert



Which icon best describes the sign of phishing: Monetary Gain?

Figure 17

Example of SME Survey – Choose Audio Sound Warning



Audio alerts will be presented to the participant on their mobile device. Which audio alert method is the most effective? (Click on each sound to listen)

A.
Stock mobile device notification sounds.

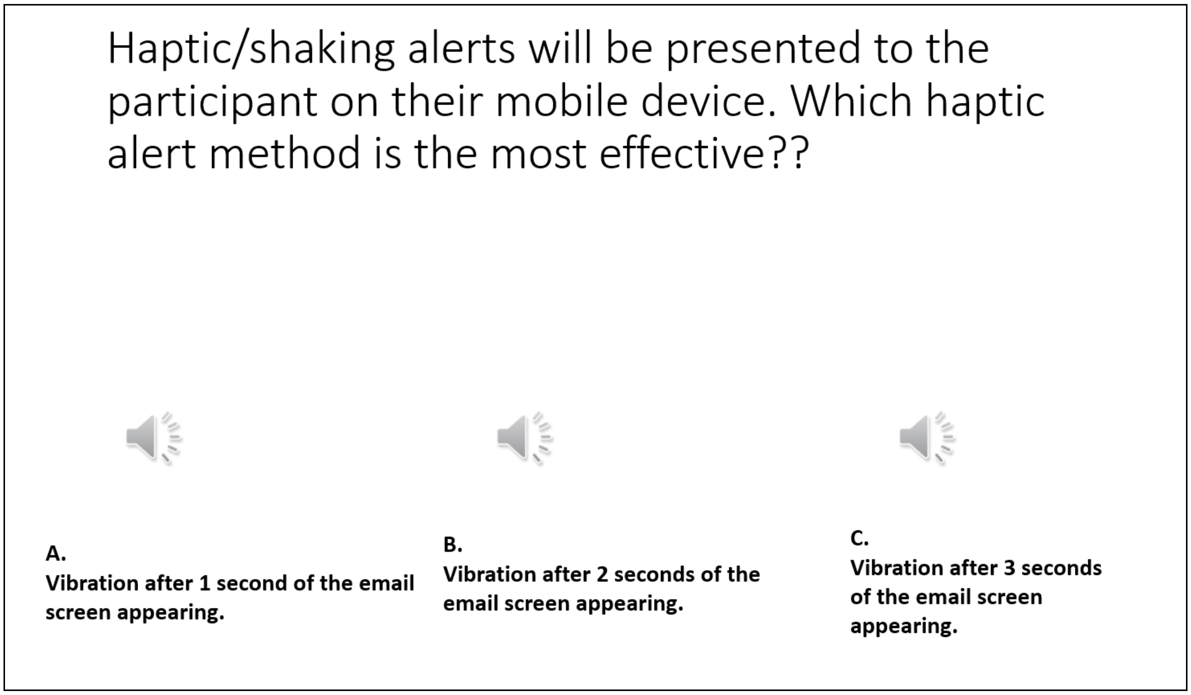
B.
Household alert sounds.

C.
Automobile alert sounds.

D.
Voice over sound of each sign of phishing.

Figure 18

Example of SME Survey – Choose Haptic Vibration Warning



Haptic/shaking alerts will be presented to the participant on their mobile device. Which haptic alert method is the most effective??

A.
Vibration after 1 second of the email screen appearing.

B.
Vibration after 2 seconds of the email screen appearing.

C.
Vibration after 3 seconds of the email screen appearing.

Also during this survey, the SMEs were asked their opinion on how long (in seconds) it should take a user to notice a sign of phishing in email. The SMEs were surveyed to include their opinion on characteristics of a user's ability to notice a sign of phishing in email. This assisted in finding a benchmark time to notice and ability to notice based on expert opinion.

Phase II

Phase II included the development of the PAWS mobile app prototype. SMEs feedback on the top signs of phishing in emails were paired with the SME feedback on audio, visual, and haptic signs that were used to alert the user of phishing. The SMEs characteristics of *ability to notice* and *time to notice* phishing in emails were included in the prototype design. A screen for participants to indicate what sign of phishing they saw was used after email screens when the participant clicked "Phishing" was added to the developmental design of PAWS. The data collected from this screen was analyzed to determine *ability to notice signs* of phishing in emails by the participants.

Pilot testing of the prototype was conducted in this phase. Testing functionality of applications is an important part of application design (Rubin & Chisnell, 2008). The pilot testing included five participants and data was verified to ensure proper capture of all data points were considered and recorded. Observations, scoring, and manual measurements of time were conducted to ensure the assessment by the PAWS mobile app prototype is accurate.

Phase III

Phase III encompassed the main research study with 205 participants. The participants answered a short demographic survey as shown in Appendix B. The participants then completed an attention span test as shown in Appendix C. The participants then entered the PAWS mobile app. Each participant saw several simulated emails verified from Phase 1 as the top signs of phishing in emails. Alerts and warnings accompanied the simulated emails as decided by the SMEs in Phase 1. The research design process is illustrated in Figure 15.

Instruments and Prototype Development

Instrument for SMEs Identification of Top Signs of Phishing in Emails

To identify SMEs feedback on the top signs of phishing in emails, a Survey Monkey survey was used. SurveyMonkey.com is a valid online survey and statistical analysis tool (Evans et al., 2009). Emails developed from literature were placed in a random order for the SMEs to rank. Survey Monkey's data tools were used as data collection and correlation to determine frequency and final ranking.

Instrument for SMEs Ranked Critical Threats, Paired with Unique A/V/H Alerts and Warnings

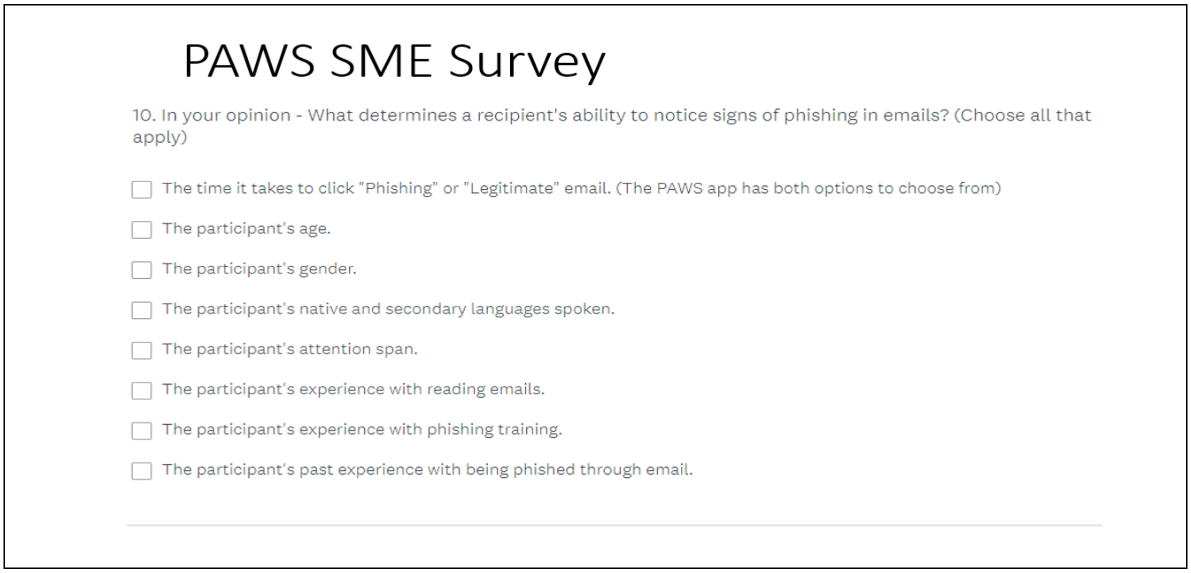
Included in the same survey for *SMEs Identification of Top Signs of Phishing in Emails*, survey questions pertaining to SMEs opinion on preferred and ranked pair of audio/visual/haptic alerts and warnings. Visual icons, audio sounds, and haptic vibration timing were presented for the SMEs to rank and pair.

Instrument for SMEs Feedback on Ability to Notice, Time to Notice, and Ability to Notice Signs of Phishing in Emails

Included in the same survey for *SMEs Identification of Top Signs of Phishing in Emails*, survey questions pertaining to SMEs feedback on *ability to notice, time to notice,* and *ability to notice signs* of phishing in emails were included as shown in Figures 19 and 20.

Figure 19

Example of SMEs Survey – Ability to Notice Signs of Phishing in Emails



PAWS SME Survey

10. In your opinion - What determines a recipient's ability to notice signs of phishing in emails? (Choose all that apply)

□ The time it takes to click "Phishing" or "Legitimate" email. (The PAWS app has both options to choose from)

□ The participant's age.

□ The participant's gender.

□ The participant's native and secondary languages spoken.

□ The participant's attention span.

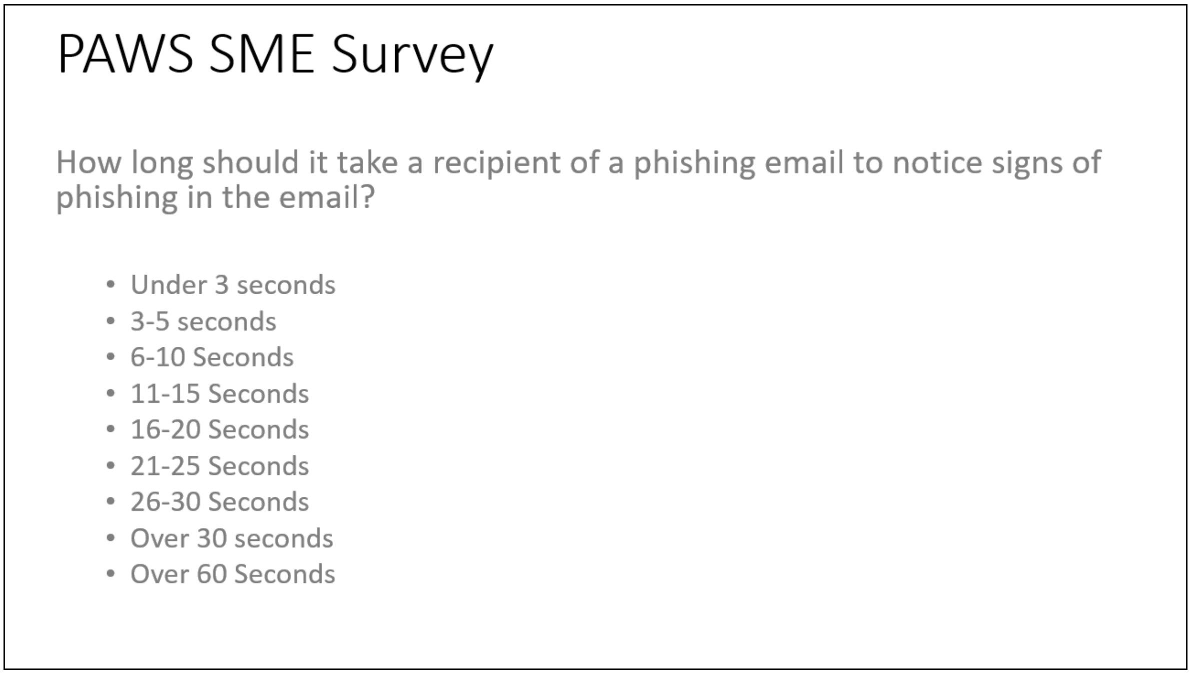
□ The participant's experience with reading emails.

□ The participant's experience with phishing training.

□ The participant's past experience with being phished through email.

Figure 20

Example of SMEs Survey – Time to Notice Signs of Phishing in Emails



PAWS SME Survey

How long should it take a recipient of a phishing email to notice signs of phishing in the email?

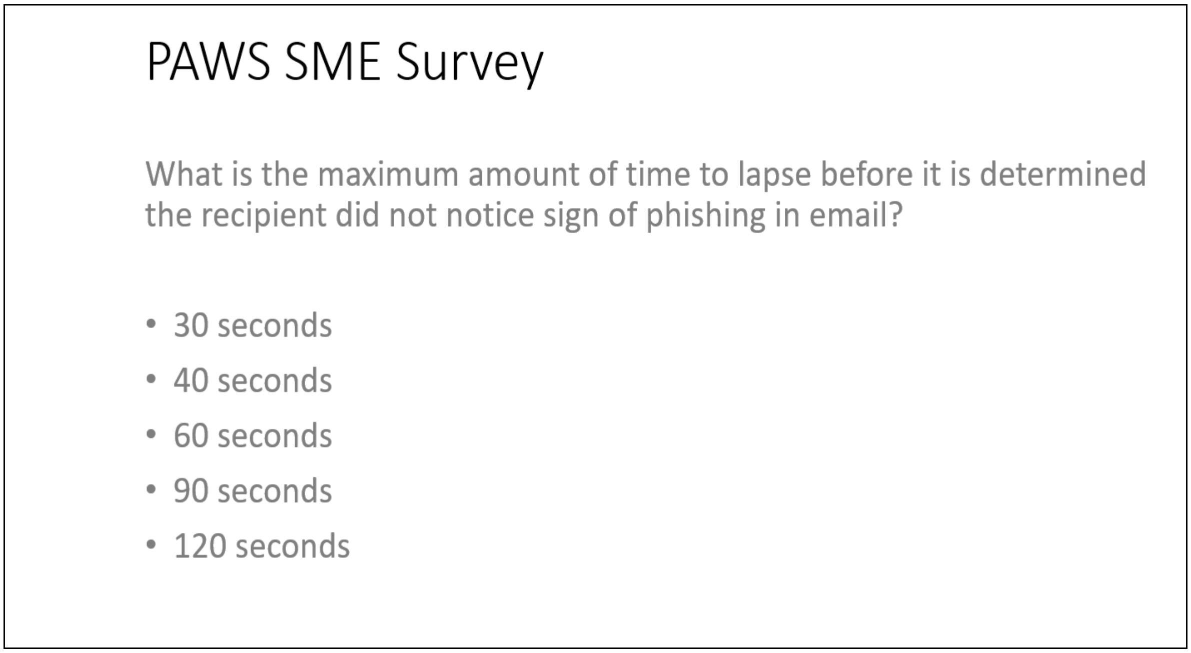
- Under 3 seconds
- 3-5 seconds
- 6-10 Seconds
- 11-15 Seconds
- 16-20 Seconds
- 21-25 Seconds
- 26-30 Seconds
- Over 30 seconds
- Over 60 Seconds

Instrument for SMEs Feedback on Validated Maximum Time to Notice Signs of Phishing in Emails

Included in the same survey for *SMEs Identification of Top Signs of Phishing in Emails*, a survey question pertaining to SMEs feedback on the maximum time to notice signs of phishing in emails was determined as shown in Figure 21.

Figure 21

Example of SMEs Survey – Max Time to Notice Signs of Phishing in Emails



PAWS SME Survey

What is the maximum amount of time to lapse before it is determined the recipient did not notice sign of phishing in email?

- 30 seconds
- 40 seconds
- 60 seconds
- 90 seconds
- 120 seconds

Instrument for Participant Demographic Information

Demographic questions for each participant were asked in the PAWS mobile application. Participants were assigned a unique number to ensure confidentiality of the participants. Qualifying questions were asked first in the demographic questions section. Each participant must be over the age of 18, have more than one email account, use a mobile device, and check email on their mobile device. Each participant ID was used to uniquely identify participants and PAWS data collection, however, no direct relationship between the individual who participated, and the data was tracked to follow anonymity requirements and be consistent with IRB requirements. An example of the demographic questions are shown in Appendix B. Additionally, the PAWS post survey questions appeared after the PAWS test. The questions asked if the user noticed if their phone vibrated during the test, as well as if they heard any audible alerts. The questions were aimed at determining if participants normally utilize their mobile device audio and haptic response features and also determined if the participant is utilizing mobile device accessibility features if needed.

Instrument for Participant Attention Span Information

Attention span testing for participants was conducted as a similar test to Psychology Today’s Attention Span Test: (https://www.psychologytoday.com/us/tests/personality/attention-span-test) and was contained in the PAWS Mobile App. After each attention span test, answers were summed for an attention span score for each participant. Participants were asked a six attention span questions. Answers were ranked on a five-point scale with values of: five for ‘quite often’, four for ‘often’, three for ‘sometimes’, two for ‘rarely’, and one point for ‘almost never’. Participants were assigned a unique number to ensure confidentiality of the participants. Each number was used to uniquely identify participants and PAWS Mobile App data collection, however, no direct relationship between the individual who participated, and the data will be tracked to follow anonymity requirement and be consistent with IRB requirements. An example of the PAWS attention span test is shown in Appendix C.

PAWS Prototype Development

After gathering SMEs responses in Phase 1, The PAWS Mobile App was developed as a mobile app for both Google Play Store and Apple App Store for the application to be downloaded on participant's mobile devices. Developmental design was utilized encompassing minimum requirements of the application as follows:

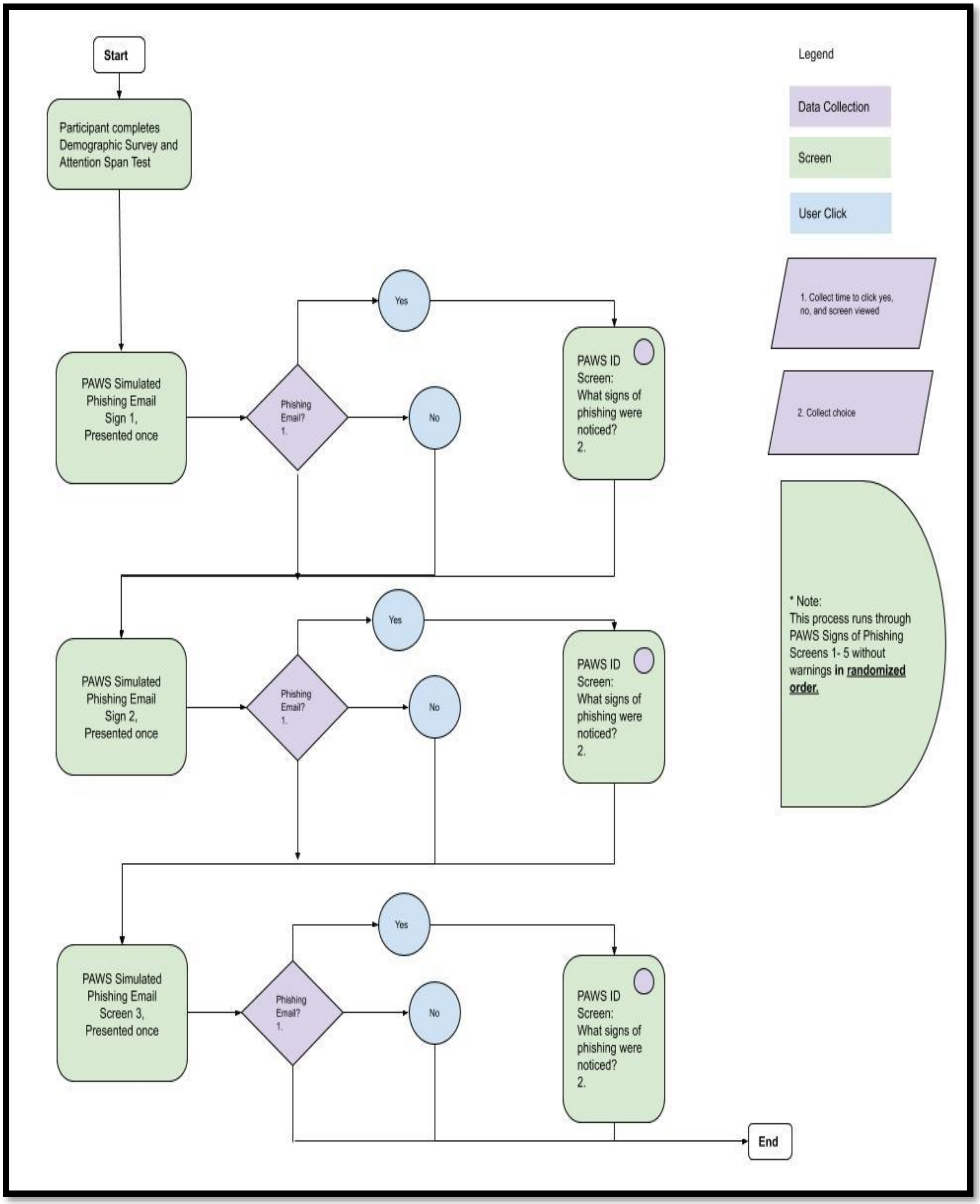
1. Application was a hard-coded screen delivery/slideshow format of simulated phishing emails. Participant email accounts were not used.
    a. Simulated emails by SMEs ranking of the top signs of phishing in emails with pairings of audio/visual/haptic warnings
2. Application was able to record user clicks and time in seconds for clicking legitimate or phishing for each email.
    a. To measure *ability to notice* signs of phishing in emails
    b. To measure *time to notice* phishing in emails per participant
3. Application displayed a "what sign did you notice" screen for participants to click the sign of phishing they saw in the email
    a. To measure *ability to notice signs* of phishing in emails
4. Application was able to vibrate or shake the device for specific simulated phishing emails
    a. Based on SMEs feedback, haptic vibrations were applied
5. Development of simulated phishing slides included:
    a. Simulated phishing email slides without signs of phishing
    b. Simulated phishing emails examples from published sources
6. Application records and formats all data for analysis tools

The PAWS mobile app prototype was delivered to the participants in two process flows, totaling four experiment groups. Process 1, as shown on Figure 22, included the top five signs of phishing presented as simulated phishing emails to the study participants without audio/visual/haptic alerts and warnings. This group (Group 1) did not contain audio, visual, or haptic alerting. Each simulated email was presented with a Legitimate and Phishing button at the bottom of the screen.

The elapsed time for each participant to click Legitimate or Phishing while viewing each simulated email screen was recorded. The elapsed time it took the participant to click was compared to the SMEs baseline time of 25 seconds and determined if the click time is considered acceptable. After clicking Legitimate or Phishing, a screen appeared asking the participant what signs of phishing they noticed on the previous screen. The screen also included an “I don’t know, it just looked like phishing”. All choices the users clicked were recorded and correlated in analysis tools.

Figure 22

Proposed Overview of PAWS Process 1

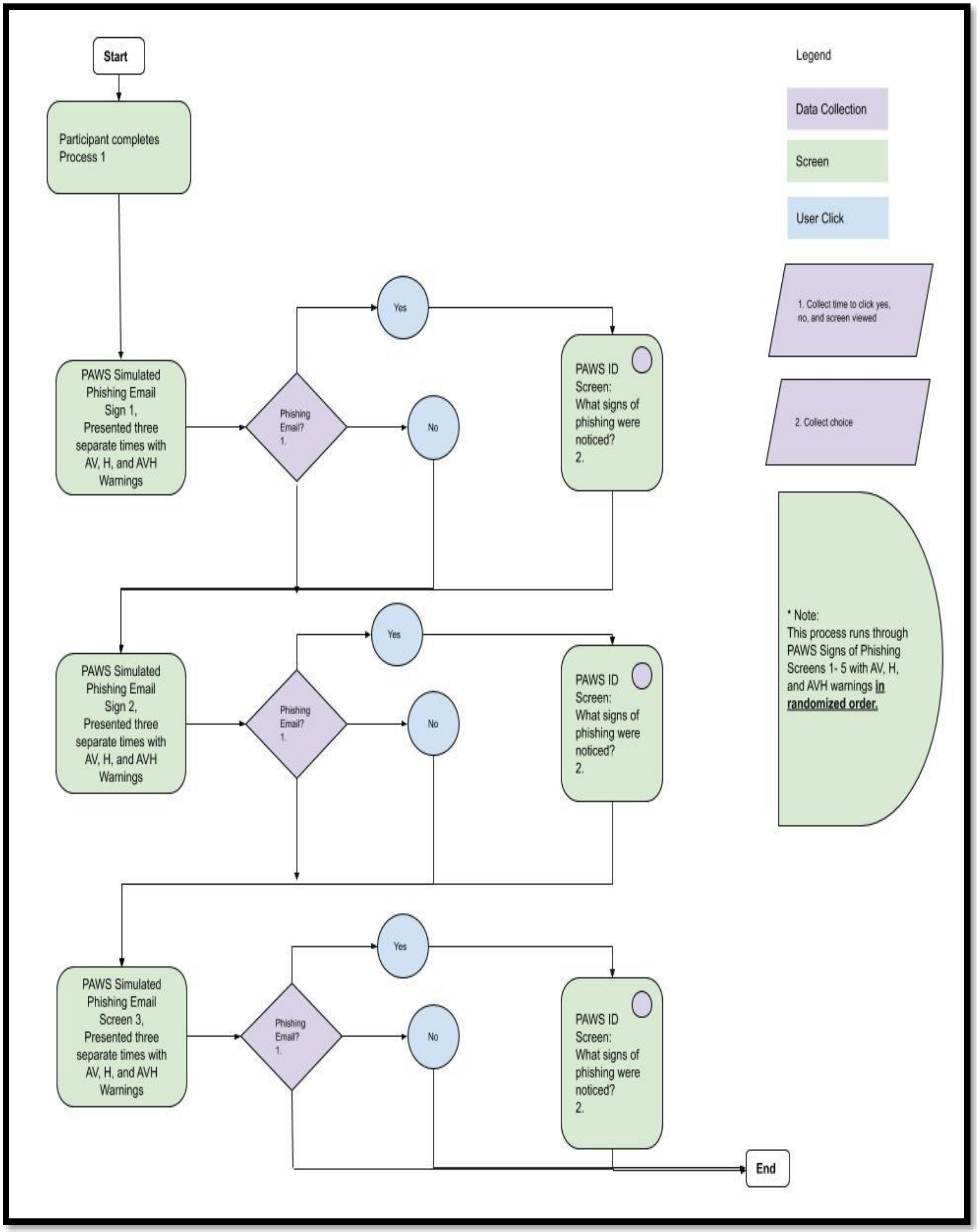

Start
Participant completes Demographic Survey and Attention Span Test
PAWS Simulated Phishing Email Sign 1, Presented once
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
PAWS Simulated Phishing Email Sign 2, Presented once
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
PAWS Simulated Phishing Email Screen 3, Presented once
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
End
Legend
Data Collection
Screen
User Click
1. Collect time to click yes, no, and screen viewed
2. Collect choice
* Note: This process runs through PAWS Signs of Phishing Screens 1- 5 without warnings in randomized order.

Process two, as shown on Figure 23 included randomized audio/visual/haptic warnings as determined from SMEs’ ranking of the top signs of phishing in emails, and audio/visual/haptic pairings from Phase I of this study. This process included Group 2, audio warnings and visual alerts (AV). Group 3, haptic alerts (H), and Group 4, audio, visual, and haptic alerts and warnings (AVH). Each simulated email was presented with a Legitimate and Phishing button at the bottom of the screen.

The elapsed time for each participant to click Legitimate or Phishing while viewing each simulated email screen was recorded. The elapsed time it took the participant to click was compared to the SMEs baseline time of 25 seconds and determined if the click time is considered acceptable. After clicking Legitimate or Phishing, a screen appeared asking the participant what signs of phishing they noticed on the previous screen. The screen also included an “I don’t know, it just looked like phishing”. All choices the users clicked were recorded and correlated in analysis tools.

Figure 23

Proposed Overview of PAWS Process 2


Start
Participant completes Process 1
PAWS Simulated Phishing Email Sign 1, Presented three separate times with AV, H, and AVH Warnings
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
PAWS Simulated Phishing Email Sign 2, Presented three separate times with AV, H, and AVH Warnings
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
PAWS Simulated Phishing Email Screen 3, Presented three separate times with AV, H, and AVH Warnings
Phishing Email? 1.
Yes
No
PAWS ID Screen: What signs of phishing were noticed? 2.
End
Legend
Data Collection
Screen
User Click
1. Collect time to click yes, no, and screen viewed
2. Collect choice
* Note: This process runs through PAWS Signs of Phishing Screens 1- 5 with AV, H, and AVH warnings in randomized order.

Randomization of simulated email screens, as well as user fatigue of email viewing was addressed in several ways for phase II. For each sign of phishing, four simulated emails examples were designed, utilizing literature review to validate signs of phishing contained in the email example. All designs were of varying length and randomized per experiment group as shown in Table 7.

Table 7

PAWS Simulated Email Screens - Length Randomization Table

SME Rank	Sign Description	Group 1 No AVH	Group 2 A/V	Group 3 H	Group 4 A/V/H
1	Sense of Urgency	UrgencyShort	Urgency1	UrgencyMed	UrgencyLong
2	Requiring Action	ActionLong	ActionShort	Action1	ActionMed
3	Request for Information	InfoMed	InfoLong	InfoShort	Info1
4	Misspelling and Grammar Issues	Spelling1	SpellingMed	SpellingLong	SpellingShort
5	Request to Click on Links	LinksShort	Links1	LinksMed	LinksLong

Randomization of experiment groups (AV, H, & AVH) was addressed by randomizing alert and warning examples as shown in Table 7. Each participant saw a total of 20 simulated emails during PAWS mobile app testing. Each experiment group contained an example of one of the top five signs of phishing. Group one, NAVH (no audio, visual, or haptic) was presented to all participants first for the first five simulated email screens shown to the participant. The randomization of both email length, alert, and warning groups are shown in Table 8.

Table 8

PAWS Experiment Groups - Randomization Table

Screen Order	Simulated Email Version	Group
1	UrgencyShort	No AVH
2	ActionLong	No AVH
3	InfoMed	No AVH
4	Spelling1	No AVH
5	LinksShort	No AVH
6	UrgencyLong	AVH
7	Action1	H
8	InfoLong	AV
9	SpellingShort	AVH
10	LinksMed	H
11	Urgency1	AV
12	ActionMed	AVH
13	InfoShort	H
14	SpellingMed	AV
15	LinksLong	AVH
16	UrgencyMed	H
17	ActionShort	AV
18	Info1	AVH
19	SpellingLong	H
20	Links1	AV

Effectiveness of the Prototype

The initial survey measured SMEs' response pertaining to the validity and provided ranking for the signs of phishing in emails, A/V/H pairings, and the tasks used for the measurements of (a) *ability to notice*, (b) *time to notice, and* (c) *ability to notice signs* of phishing in emails. Pilot testing of the PAWS mobile application was completed prior to PAWS participant study with five testers to ensure all measures were valid, and any data or performance issues were resolved. Multiple specifically testing was completed to ensure the PAWS mobile application properly recorded the score associated with the user's *ability to notice* and was compared with the pre-determined scores for the sampled emails available in the application. Moreover, multiple testing was completed to ensure the PAWS mobile app recorded the time (in seconds) associated with the user's *time to notice* and was compared to the time (in seconds) accurately. Several audio alerts were collected from warning systems, formatted to play as an audio clip with visuals, and then presented to the SMEs in a companion survey form for ranking preferences.

Validity and Reliability

To design a measure that has both high validity and reliability, this study utilized sequential exploratory developmental research combining both qualitative and quantitative methodologies along with the development of the PAWS mobile app. This research included three phases for development, testing, and data collection of the PAWS mobile application. The first data collection point was Phase I. SMEs were asked to (1) rank signs of phishing in order of importance, (2) Pair/match audio warnings with what they felt was the appropriate for each sign of phishing, (3) Pair/match visual warnings with what they felt was the appropriate visual icon for each sign of phishing, (4) Pair/match haptic warnings with what they felt was the appropriate haptic warning timing. (5) Provide their perspective on the tasks for the measure of *ability to notice* phishing in emails (6) Provide their perspective on the measure of *time to notice* phishing in emails, and (7) Provide their perspective on measurement of *ability to notice signs* of phishing in emails. The Delphi methodology of development and validation of Phase I initial list and library by SMEs was used as the input to Phase II (Tracy & Richey, 2007). Delphi methodology is a well-established qualitative and quantitative research elicitation process to enable a group of experts to reach consensus on specific set of requirements or prioritization process (Ramim & Lichvar, 2014). Data collection for Phase II included pilot user testing and qualitative feedback for improvements towards the PAWS mobile app prototype. This step also included the exploratory research design steps of building the PAWS mobile app prototype. Pre-analysis data screening was conducted in Phase II (See section “Pre-Analysis Data Screening” below). Phase III encompassed all of the participant data, qualitative and quantitative data collection, validity verification, and statistical analysis.

Reliability

During the first data collection in Phase I, $10.00 Amazon gift cards were awarded to the SMEs to ensure their participation. This was in effort to increase reliability in SME responses and commitment to the research study. To produce stable and accurate PAWS results, consistent object measurement was completed by hard coding the PAWS mobile application. Each participant saw exactly the same simulated email screens, in the same order. To ensure participant scores represent accurate variables, internal consistency was used to correlate reliable performance over all participant data (Salkind, 2003).

Validity

Validity was an important measure in this research process to ensure instrument measures (Straub, 1989). As indicated by Salkind (2003) content validity was addressed through the literature review of this research. The literature synthesis represents the body of knowledge surrounding available examples of signs of phishing in emails. This information formed the SME survey for the SME ranking of the top signs of phishing in emails. Criterion validity was addressed by utilizing SME feedback for (a) *ability to notice,* (b) *time to notice and (c) ability to notice signs* of phishing in emails. This information was the basis of measurement for participant criterion (Salkind, 2003). Construct validity (Salkind, 2003) was ensured by utilizing the literature synthesis of this research to establish a foundation for (a) prior studies with simulated and real phishing emails, (b) prior surveys regarding demographics, and (c) effects of end user phishing training, and (d) prior studies and tests founded upon attention span.

Bias can also be an issue with application development. Bias was controlled by ensuring only SME validated content appeared for the simulated phishing slides in the PAWS mobile application. Bias questions were addressed for the demographic surveys by using templated Survey Monkey demographic surveys as opposed to self-created questions and surveys (Sekaran & Bougie, 2013). Reliability and validity were critical to this research study. Mitigation steps were taken to reduce threats to the research data validity and reliability (Ellis & Levy, 2006).

Population and Sample

To achieve the required approximately 25 SMEs, for the SMEs survey, personal networks were contacted to solicit about 40 cybersecurity experts, with the anticipation that at least 25 of them would agree to participate. Screening for SMEs participation was verified by preliminary survey questions: Cybersecurity degree obtained, years in cybersecurity, professional cybersecurity/IT certifications, and current job position as shown in Appendix A. Participants were requested to participate in the study from the researcher’s LinkedIn contacts and through researcher’s email contacts. Amazon gift cards for $10.00 were awarded to the SMEs upon participation in the initial survey. A total of 32 SMEs participated in the survey.

For the PAWS mobile application study, a sample of the population was used to gather a representation of the general population (Sekaran & Bougie, 2013). At least 150 participants were recruited for the PAWS mobile application study, targeting a minimum 100 participants in order to show statistical power and significance (Cohen,1988). Sample of convenience method was used from personal networks to recruit the participants. This method was limited as more participants could have involved if socially linked to the researcher. Recruiting was done in English. Screening for study participants was verified by preliminary questions in the demographic survey as shown in Appendix B. Participants needed to be 18 years of age or older, have at least one email account, use a mobile device, and check their email on a mobile device.

Pre-Analysis Data Screening

Pre-analysis data screening was utilized on collected data before the full analyzation of collected data occurs. This step prevented the majority of data collection errors (Levy & Ellis, 2006). To verify inaccurate data entry, visual verification was performed before manual data entry of data collected. This study also used pre-analysis data screening methods (Mertler & Vannatta, 2013). Mertler and Vannatta (2013) indicated pre-analysis data screening is needed to ensure accuracy of data collected. Validation of this data included examining the variables to ensure no values are outside of the expected range. Test data was also be checked to ensure coded values had corresponding categories. Missing data, extreme values, and assumptions were analyzed to ensure data did not interfere with study results (Mertler & Vannatta, 2013).

Data Analysis

Data analysis for Phase I was conducted through Survey Monkey analysis tools. Semantic differential scale was used for the SMEs to rank the top signs of phishing. During the same survey, the SMEs frequency majority opinion of *ability to notice* and *time to notice* phishing in emails was be recorded. The highest rate of choice for each SMEs survey question will be used towards the PAWS mobile application. Each SME opinion on amount of time it should take a user to notice a sign of phishing in emails, and the length of time it should take to measure ability to notice signs of phishing in emails were anonymously recorded. Responses were recorded and analyzed determining frequency analysis for the top signs of phishing in emails, A/V pairings, *ability to notice*, *time to notice*, and *ability to notice signs* of phishing in emails – addressing research questions RQ1, RQ2, RQ3, and RQ4. Phase II data was recorded and analyzed through PAWS mobile app development and testing and answered RQ5. The final phase of this research study included data analysis from the participant actions during PAWS testing and answered RQ6a, RQ6b, RQ6c, RQ7a, RQ7b, and RQ7c. Data analysis was performed on the results of this study for each participant and compared to participant groups. The participant groups were coded into groups for specific analysis.

Participants were asked to click the corresponding buttons when they noticed a sign of phishing in any of the 20 simulated emails presented to them from the PAWS mobile app. Measurements included participants' *ability to notice* signs of phishing in emails, *time to notice* phishing in emails, age, gender, experience with phishing training, attention span, and *ability to notice signs* of phishing in emails.

Analysis of Variance (ANOVA) was used to test for significant differences between groups. One-Way ANOVA testing was used to answer RQ6a, RQ6b, and RQ6c as well as on the data collected following Mertler and Vannatta (2013) guidance for addressing RQ7a, RQ7b, and RQ7c.

Resources

This study was reviewed by the Institutional Review Board (IRB) as human participants are involved in the study. A Survey Monkey license was utilized for the initial survey. Information security and cybersecurity SMEs were needed for the initial survey. LinkedIn and was used to contact SMEs and PAWS mobile app participants. An application developer was needed for the development of the PAWS prototype and application. A graphic designer was needed for the creation of email screens and PAWS branding. This study also required an online database for data collection for survey and prototype data. SPSS software was needed for data analysis, coding, and presentation of results. Access to mobile devices was needed for testing. A set of 25 x $10.00 Amazon gift cards were needed for requested SME participation rewards.

Summary

An overview of the research methodology was provided in this chapter. Utilizing a mixed method approach, quantitative and qualitative data was used to develop, validate, test, and collect research data. This research answered the following research questions:

The main Research Question (RQ) that this study addressed was: What audio/visual/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 on mobile devices?

RQ1: What are the SMEs’ validated top signs of phishing in emails that are considered the most critical threats to users?

RQ2: What SMEs’ identified audio/visual/haptic alerts and warnings are most valid to pair with the top signs of phishing in emails?

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

RQ4: What is the SMEs’ validated maximum time for users’ *ability to notice* signs of phishing in emails?

RQ5: What validation and testing procedures should be considered in order to deliver a mobile app phishing alert and warning system prototype?

RQ6a: Do statistically significant mean differences exist among users’ *ability to notice* phishing in emails with or without PAWS?

RQ6b: Do statistically significant mean differences exist among users’ *time to notice* phishing in emails with or without PAWS?

RQ6c: Do statistically significant mean differences exist among *users’ ability to notice signs* of phishing in emails with or without PAWS?

RQ7a: Do statistically significant mean differences exist among users’ *ability to notice* phishing in emails with or without PAWS based on: (a) age, (b) gender, (c) experience with phishing awareness training, and (d) attention span?

RQ7b: Do statistically significant mean differences exist among users *time to notice* phishing in emails using PAWS based on: (a) age, (b) gender, (c) experience with phishing awareness training, as well as (d) attention span.?

RQ7c: Do statistically significant mean differences exist among users' *ability to notice signs* of phishing in emails with or without PAWS based on: (a) age, (b) gender, (c) prior phishing awareness training, as well as (d) attention span?

The RQs were addressed over three phases using developmental design, qualitative, and quantitative methods to construct and validate the PAWS mobile app. Phase one collected SMEs feedback, utilizing Delphi methodology towards the top signs of phishing in emails, SMEs chosen audio/visual/haptic warnings, as well as SMEs opinion on *ability to notice, time to notice,* and *ability to notice signs* of phishing in emails. Phase two encompassed the development and testing of the PAWS mobile app prototype utilizing findings from Phase one and pilot testing. Phase three included the study itself with the participants. Data collected included demographic information, attention span scores, data towards ability to notice, time to notice signs, and ability to notice signs of phishing in emails with and without audio, visual, as well as haptic alerts and warnings on the participants.

Chapter 4

Results

Overview

This chapter presents the results of the data collection and analysis from this research study. The main goal was to determine an audio/visual/haptic alert and warning system combination could be used to empirically assess users' (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails on mobile devices. For Phase I, results were presented from a one-round Delphi survey using a panel of 32 cybersecurity experts. The SMEs validated the top signs of phishing in emails, as well as: audio/visual/haptic warnings to pair with the emails. Phase I also identified SME opinion regarding *ability to notice*, *time to notice*, and *ability to notice signs* of phishing in emails that were then used towards development of the PAWS mobile app. Phase II utilized SME results from the SME survey, development, coding, and user testing of the PAWS mobile app prototype, as well as qualitative and quantitative feedback from pilot testers. The PAWS Mobile App is a custom, mobile application available on the Apple App Store, and Google Play Store. Phase III results are presented from the PAWS mobile app study with 205 participants utilizing ANOVA, ANCOVA, and frequency analysis of participant interaction.

Phase I – SME Survey Feedback and Findings

RQ1, RQ2, RQ3, and RQ4 were answered through s survey instrument during the first phase of this research study. Invitation emails to participate in the Subject Matter Experts (SMEs) 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 Method (Rahim & Lichvar, 2014) cycle with a 71.1% response rate, meeting consensus on the survey questions. Table 8 provides the descriptive statistics of the 32 respondents. Cybersecurity and information security experts included current college professors with classroom and industry experience (40.63%) and current cybersecurity industry professionals (59.39%). Industry professionals included C-level executive managers (9.37%), senior managers (18.74%), middle managers (9.38%) security analysts (9.38%), and other cybersecurity positions (12.50%). Over 56% of the respondents had over 10 years of cybersecurity or information security industry experience followed by 28% at five to 10 years of experience. SMEs with three to five years of experience (3.13%), one to three years of experience (6.25%), and one year or less (6.25%) also participated in the SME survey. Descriptive statistics of the SMEs are shown in Table 9.

Table 9

Descriptive Statistics of SMEs (N=32)

Demographic Item	**N**	**%**
Current Position:		
Owner/Executive/C-Level	3	9.37%
Senior Management	6	18.74%
Middle Management	3	9.38%
IT Security Analyst	3	9.38%
Professor	13	40.63%
Other	4	12.50%
Private Practice	(1)	
IT Senior Auditor	(1)	
IT Security Staff	(1)	
Cybersecurity Investigator	(1)	
Experience in Information Security:		
1 Year or Less	2	6.25%
1-3 Years	2	6.25%
3-5 Years	1	3.13%
5-10 Years	9	28.13%
10 Years or More	18	56.25%

Phase I - RQ1

To answer the research question: What are the SMEs' validated top signs of phishing in emails that are considered the most critical threats to users, SMEs ranked what they felt the top signs of phishing were in the SME survey. The SMEs' top signs of phishing in emails that they consider the most critical threats to users are shown in Table 10. All 32 of the SMEs ranked the top signs of phishing in emails. Frequency analysis was used to determine the highest frequency of ranking among the 32 SMEs. Sense of Urgency was the top sign of phishing (11.32%), followed by requiring action from the recipient (11.22%), ranking third highest was request for information from the recipient (8.87%), followed by misspelling and grammar issues in fourth rank (8.54%), and request to click on links as the number five sign of phishing in emails (8.34%).

Table 10

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

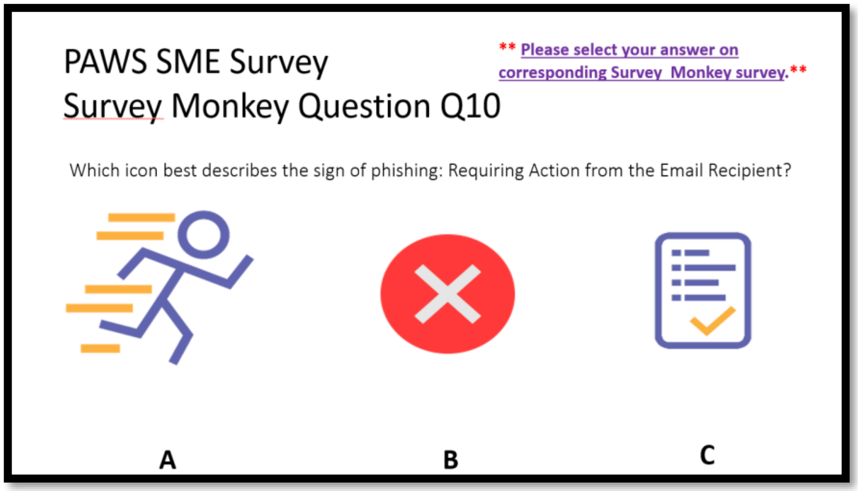
Survey Question	**Rank**	**%**
Rank Signs of Phishing:		
Sense of Urgency	1	11.32%
Requiring Action	2	11.22%
Request for Information	3	8.87%
Misspelling and Grammar	4	8.53%
Request to Click on Links	5	8.34%

Phase I - RQ2

To answer the research question: What SMEs' identified audio/visual/haptic alerts and warnings are most valid to pair with the top signs of phishing in emails, SMEs voted on their preferred pairings in the SME survey. The SMEs' identified audio/visual/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 24. Each sign of phishing had a corresponding figure for SMEs' voting of their most preferred icon in the survey. Table 11 illustrates frequency analysis performed toward SME consensus on visual icons for the PAWS mobile app.

Figure 24

SME Survey Question 10



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?

Table 11

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

Survey Question	N	%
Which Icon Best Represents the Sign of Phishing: Urgency:		
Purple Alarm with Yellow Lines	15	46.88%
Red Alarm	16	50.00%
Purple Stopwatch	1	3.12%
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	21.87%

Table 11

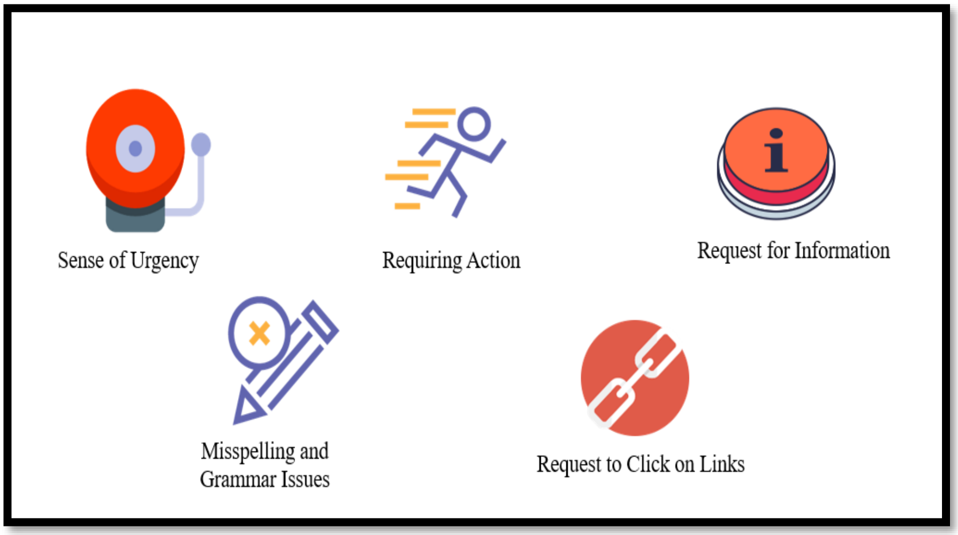
SME Rank of Icon Matching to Top Signs of Phishing in Emails (N=32) – (cont.)

Survey Question	**N**	**%**
Which Icon Best Represents the Sign of Phishing: Request for Information:		
Purple Icon and “i”	12	37.50%
Red Button with “i”	17	53.13%
Purple Arrow Over Text Box	3	9.37%
Which Icon Best Represents the Sign of Phishing: Misspelling and Grammar Issues:		
Purple and Yellow “Aa”	6	18.74%
Red and Black Circle “Aa”	11	34.38%
Purple Pencil with “x”	15	46.88%
Which Icon Best Represents the Sign of Phishing: Request to click on Links:		
Purple Link	7	21.88%
White Link on Red Background	21	65.63%
Purple Down Arrow	4	12.49%

SME pairing of visual icons for the top signs of phishing in emails resulted in 46.88% of SMEs choosing a red alarm as the best representation of the sign of phishing sense of urgency. Requiring action resulted in a running person icon as the chosen match from SMEs (43.75%). SME pairings for request for information was a red button “i” with 17 votes (53.13%). SMEs decided misspelling and grammar issues should be represented as a purple pencil with an “x” with 46.88% of SME votes. Request to click on links was determined to be paired with a white link on a red background with 21 SME votes (65.63%). Figure 25 illustrates the final icons paired with the top five signs of phishing in emails that were used in the PAWS Mobile App.

Figure 25

SME Visual Icon Matching to Top Signs of Phishing in Emails



SMEs ranking of the audio and haptic pairings as shown in Table 12 resulted in the consensus that the audio alerts would be most effective as a female voice over alert, receiving 34.38% of the SME consensus. Other audio choices were stock mobile device sounds (iPhone, Android alerts) (28.13%), household alert sounds (fire alarms, microwave sounds) (18.75%), and automobile alert sounds (seatbelt alerts, tire pressure warnings, check engine alerts) (18.75%). The SMEs panel also determined that shaking/vibration alerts should happen immediately upon the recipient seeing the simulated email on the mobile screen with SME consensus at 38.71%. Other haptic presentation choices included one second after the simulated email appears (29.03%), two seconds after the simulated email appears (16.13%), and three seconds after the simulated email appears (16.13%). Female voice over audible warnings, as well as haptic/vibration upon participants viewing simulated emails were used for the PAWS mobile app.

Table 12

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

Survey Question	**N**	**%**
Which Audio Alert Group Would Be the Most Effective in Alerting Participants to Signs of Phishing in Email:		
Stock Mobile Device Notification Sounds	9	28.13%
Household Alert Sounds (Fire alarm, Microwave sounds)	6	18.75%
Automobile Alert Sounds (Seatbelt ding)	6	18.75%
Voice Over Description of The Sign of Phishing	11	34.38%
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%

Phase I - RQ3

The SMEs' validated tasks for the measures of: (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails was answered by SME survey questions. The SMEs' validated tasks for users' demographic indicators of *ability to notice* signs of phishing in emails are illustrated in Table 13. The highest rank of ability to notice include the email recipient's experience with phishing training (90.63%), followed by the email recipient's experience with being phished (84.38%), experience reading emails (75%), attention span (59.38%), age (56.25%), native language spoken (46.88%), clicking "Legitimate" or "Phishing" buttons (34.38%), and gender (3.13%). SME consensus answers were integrated into the development of PAWS mobile app demographic questions to analyze the effects of age, gender, experience with phishing training, and attention span.

Table 13

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

Survey Question	N	%
What Determines a Recipient's Ability to Notice Signs of Phishing in Emails:		
Ability to Click "Legitimate "or "Phishing"	11	34.38%
Age	18	56.25%
Gender	1	3.13%
Native Language Spoken	15	46.88%
Attention Span	19	59.38%
Experience with Emails	24	75.00%
Experience with Phishing Training	29	90.63%
Past Experience with Being Phished	27	84.38%

SMEs determined that participant's ability to notice top signs of phishing they saw in emails is the key indicator of ability to notice signs of phishing in emails with a consensus of 90.32% as shown in Table 14. Ability to correctly click legitimate or phishing buttons (41.94%), and the time it takes to click legitimate or phishing buttons (38.71%) were also measured towards the ability to notice signs of phishing in emails. Table 13 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.

Table 14

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

Survey Question	N	%
What Are Some Tasks That Determine a Recipient's Ability to Notice Signs of Phishing in Emails:		
The ability to correctly to Click "Legitimate "or "Phishing"	12	38.71%
Time it Takes to Click "Legitimate "or "Phishing" Buttons	13	41.94%
The Ability to Identify What Signs of Phishing They Saw	28	90.32%

Phase I - RQ 4

SMEs' validated maximum *time for users' ability to notice* signs of phishing in emails was answered by SME survey question. As illustrated by Table 15, the SMEs indicate 25 seconds (28.13%) is the maximum time to lapse before it is determined the email recipient did not notice signs of phishing in the email. Other SME responses included 15 seconds (15.63%), more than 90 seconds (12.50%), and 60 seconds (18.75%).

Table 15

SME Rank of Maximum Time to Notice Top Signs of Phishing in Emails (N=32)

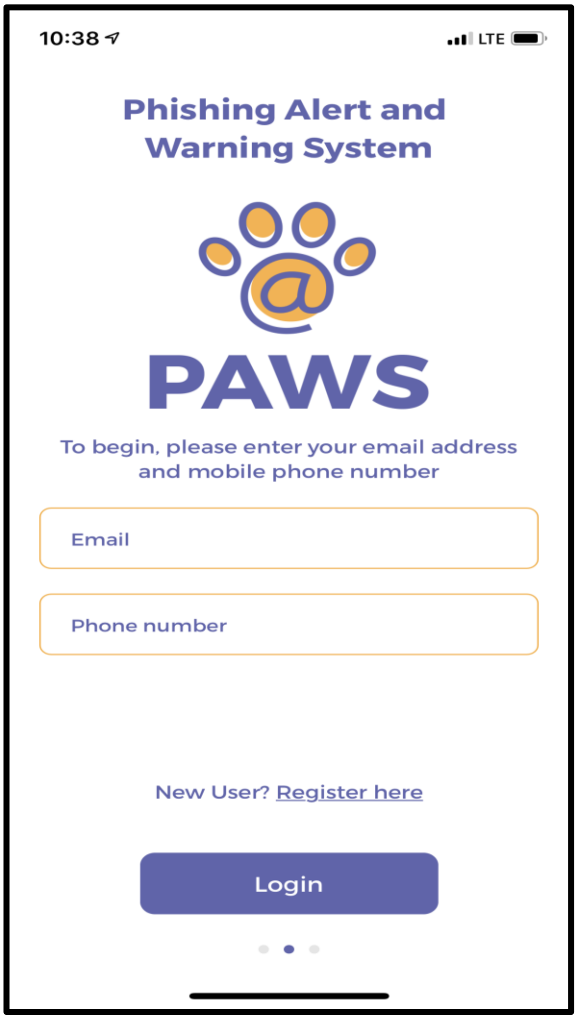
Survey Question	N	%
What Is the Maximum Time to Lapse Before It Is Determined the Recipient Did Not Notice Signs of Phishing in the Emails:		
5 Seconds	2	6.25%
15 Seconds	5	15.63%
25 Seconds	9	28.13%
35 Seconds	6	18.75%
45 Seconds	2	6.25%
55 Seconds	0	0.0%
60 Seconds	3	9.38%
65 Seconds	0	0.0%
70 Seconds	0	0.0%
75 Seconds	0	0.0%
80 Seconds	1	3.13%
85 Seconds	0	0.0%
More Than 90 Seconds	4	12.50%

Phase II - PAWS Mobile App Development

Phase II included the development of PAWS, the mobile prototype and study application. SME consensus on audio, visual, haptic feedback, top signs of phishing, ability to notice signs of phishing measures, time to notice measures, ability to notice signs of phishing in email measures, and order of appearance of simulated emails were used. Development of the application involved programming two factor authentications to ensure participant validity and uniqueness. The initial login screen shown in Figure 26.

Figure 26

PAWS Mobile App Screen – Login Screen Example



Phishing Alert and Warning System

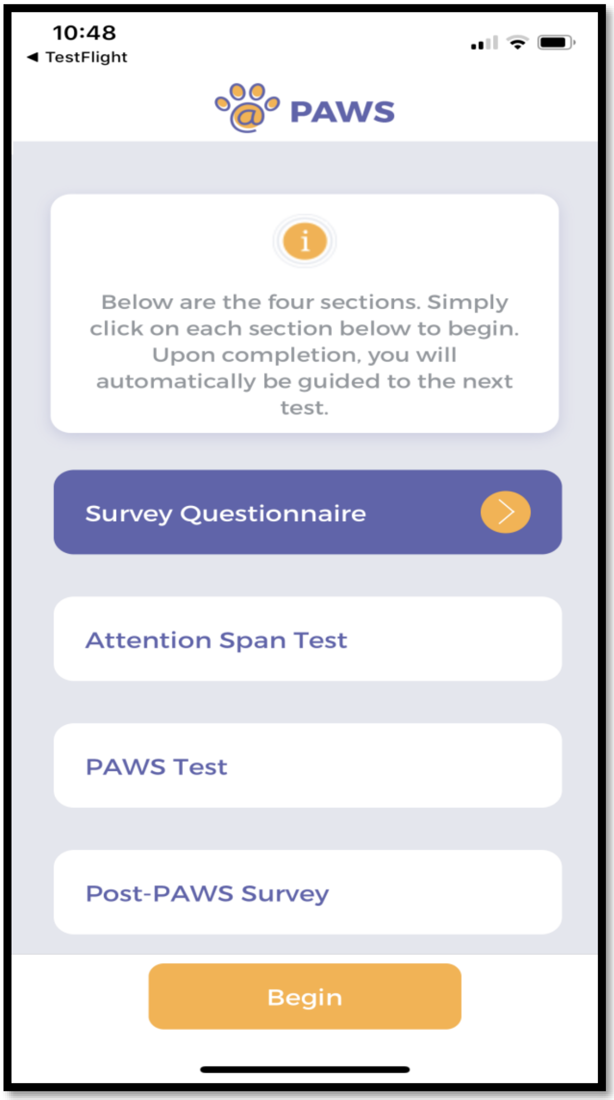
PAWS

To begin, please enter your email address and mobile phone number

Demographic questions, and attention span questions were asked of the participants and reviewed by the NSU IRB board. Simulated emails for the PAWS test were programmed and organized based on SME consensus. The PAWS mobile app was organized into four parts for the participants. Demographic Survey, Attention Span Test, PAWS Test, and Post- PAWS survey. The PAWS mobile app four sections were presented to the participants as shown in Figure 27.

Figure 27

PAWS Mobile App Screen – Four Sections Screen Example



Below are the four sections. Simply click on each section below to begin. Upon completion, you will automatically be guided to the next test.

Phase II - RQ5

The Phase I SMEs survey, as well as a pilot test of the PAWS mobile app was utilized to answer the research question: What validation and testing procedures should be considered to deliver a mobile app phishing alert and warning system. Table 16 further identifies SMEs feedback towards an audio/visual/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 four email alert and warning groups: no alerts or warnings (NAVH), audio and visual alerts and warnings (AV), haptic alerts and warnings (H), and audio/visual/haptic alerts and warnings (AVH), should be presented in a specific manner 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 resulted in 20 simulated email screens for the alert and warning system. Combined with feedback regarding the top signs of phishing, audio/visual/haptic alerts and warnings, constructs for an audio/visual/haptic phishing alert and warning system were created.

Table 16

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

Survey Question	**N**	**%**
How Should Emails Without Audio, Visual, or Haptic Alerts and Warnings be Presented:		
Show the Top 10 Signs of Phishing Emails in 1-10 Order	7	21.88%
Show the Top 5 Signs of Phishing Emails in 1-5 Order	20	62.50%
Show the Top 5 First, and 6-10 after AVH Warnings are Presented	5	15.63%
How Should Emails with Haptic Alerts and Warnings Be Presented:		
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%
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%

Table 16

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

Survey Question	N	%
How Should Emails with Audio and Visual Alerts and Warnings Be Presented:		
Show the Top 10 Signs of Phishing Emails in 1-10 Order	9	28.13%
Show the Top 10 Signs of Phishing in Randomized Order	5	15.63%
Show the Top 5 Signs of Phishing Emails in 1-5 Order	12	37.50%
Show the Top 5 Signs of Phishing Emails in Randomized Order	6	18.75%
How Should Emails with Audio/visual/haptic Alerts and Warnings Be Presented:		
Show the Top 10 Signs of Phishing Emails in 1-10 Order	6	18.75%
Show the Top 10 Signs of Phishing in Randomized Order	9	28.13%
Show the Top 5 Signs of Phishing Emails in 1-5 Order	13	40.63%
Show the Top 5 Signs of Phishing Emails in Randomized Order	4	12.50%

Phase II - PAWS Development and Pilot Testing

As previously shown, randomization of emails by alert group and by email length were considered while coding and programing the PAWS mobile app prototype. All participants saw the same, randomized order of PAWS screens. The top five signs of phishing were represented by signs one through five being shown to the participant in a randomized order for the group NAVH (no audio, visual, or haptic alerts and warnings), followed by randomization of the other three alert and warning groups (totaling 15 simulated email screens) for AV (audio/visual alerts and warnings), H (haptic alerts and warnings), and AVH (audio/visual/haptic alerts and warnings).

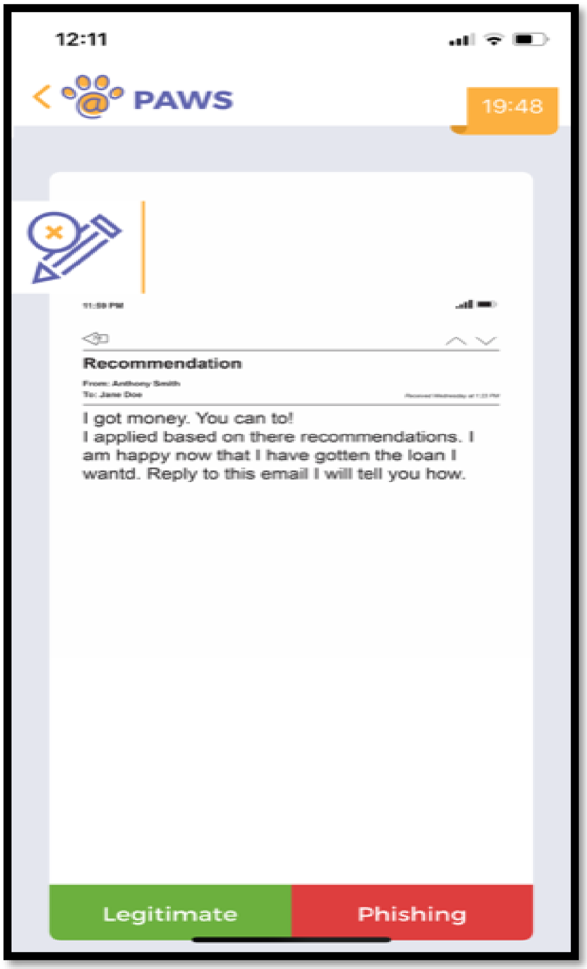
Qualitative and quantitative measures were used to test the prototype. Functions and effectiveness were measured with binary scores (Sauro & Lewis, 2012). Backend database data recording accuracy was verified by in-person user testing observation. This method was used to ensure accuracy of the database recording of how long the participant took to click “Phishing” or “Legitimate” in seconds matched the actual action by the participant. User testing observation was also utilized to verify database accuracy when participants were clicking what sign of phishing they saw on the simulated email screen.

Several issues were documented, corrected, and retested during Phase II of the study. Audible feedback to the researcher was used during the testing phase as an issue tracking mechanism (Rubin & Chisnell, 2008). Primarily, several signs of phishing were able to be clicked on the “what signs of phishing did you notice” screen. The issue was corrected to allow only one click and retested. User testing also indicated simulated phishing emails screens text was too small. All screens were redesigned with larger text to increase legibility. User testing also revealed a “Back” button was available allowing participants to review the last email viewed. This was removed to rely on participant memory to “match” the sign of phishing they believed they saw with the choices of signs of phishing. Additionally, visual icons for both the AV and AVH groups were appearing at the same time as the simulated email screen. This feature was reprogrammed to appear after the email was displayed for one second for the icon to look like an alert rather than part of the email. Figure 28 is shown with a visual icon, and short text version of the spelling and grammar issues sign of phishing. Participants were asked to click “Legitimate” or “Phishing” upon seeing each simulated email, and then choose what sign of phishing they saw if “Phishing” was clicked. Figure 29 is shown with the final design after user testing and additional corrective programming and adjustment. Final designs for all groups (NAVH, AV, H, & AVH) included audio sounds for all AV and AVH signs of phishing upon opening of the simulated email screen. H and AVH groups included haptic vibration when the simulated email screen appeared.

A Post-PAWS survey was added as the fourth part of the PAWS test to increase validity and reduce errors for individual participation. Participants were asked if their mobile device shook, made any audible sounds, and if they experienced any delays (phone calls, notifications) while taking the PAWS test. This information could be analyzed for individual results to explain potential outliers and skewed data. A free-form text box was also added as the last participant question for the participants to add any questions or concerns they might have had. This also helped researcher feedback in real-time as the mobile app was being delivered to the participants.

Figure 28

PAWS Mobile App Screen – AVH Example



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.

Phase III – PAWS Mobile App Delivery

Phase III included the application study of PAWS with participants. Data collection occurred from June 1, 2020 to June 24, 2020. The participants were personal and professional contacts of the and participants recruited through LinkedIn social media posts. A total of 214 participants downloaded the PAWS Mobile App and participated in the study.

Phase III – Pre-Analysis Data Screening

There were 214 total participants for this study. Eight participants did not complete the study and were removed from the final participant data list. SPSS Statistics™ version 25 was used to conduct analysis on the PAWS Mobile App participants answers. Mahalanobis Distance procedure (Mertler & Reinhart, 2017) determined one multivariate outlier with value 130.78. This outlier was removed from further analysis. The final sample size for this study was 205.

Phase III – Participant Demographics Characteristics

The 205 participants included several demographic areas. Demographic information is shown on Table 17. There were six age groups for the study. Group 1 (18-20) included 11.2% of the participants with a value of 23 participants. Group 2 (21-29) was 26.8%, Group 3 (30-39) was 21.5% with 44 participants. Group 4 (40-49) was 20.5%, Group 5 (50-59) was 12.7%. Group 6 (60 and older) included 7.3% of the study population. Gender was almost evenly distributed with 100 female participants, 101 male participants, and four participants that chose not to answer the gender demographic question. Experience with phishing training was also asked in the demographic question set. Participants that had experience training included 49.3% of the participants, 42.9%

did not have prior phishing training, 6.8% were not sure if they have had prior phishing training, and 1.0% preferred to not answer the question. Attention span scores were also recorded from the attention span portion of the PAWS study.

Table 17

Descriptive Statistics of PAWS Participants (N=205)

Demographic Item	**N**	**%**
Age Group:		
1. 18-20	23	11.2%
2. 21-29	55	26.8%
3. 30-39	44	21.5%
4. 40-49	42	20.5%
5. 50-59	26	12.7%
6. 60+	15	7.3%
Gender:		
1. Female	100	48.8%
2. Male	101	49.3%
3. Prefer to not answer	4	2.0%
Experience with Phishing Awareness Training:		
1. Yes	101	49.3%
2. No	88	42.9%
3. Not Sure	14	6.8%
4. Prefer to not answer	2	1.0%
Attention Span Score:		
1. 3,7,9	(3)	1.5%
2. 10	2	1.0%
3. 11	8	3.9%
4. 12	5	2.4%
5. 13	10	4.9%
6. 14	17	8.3%
7. 15	18	8.8%
8. 16	21	10.2%
9. 17	16	7.8%
10. 18	23	11.2%
11. 19	19	9.3%
12. 20	11	5.4%
13. 21	18	8.8%
14. 22	13	6.3%
15. 23	6	2.9%
16. 24	8	3.9%
17. 25	3	1.5%
18. 26	4	2.0%

Phase III - RQ6a

To answer if any statistically significant mean differences exist among users' *ability to notice* phishing in emails with or without PAWS, Analysis of Variance (ANOVA) was used to test for significant differences between groups. The results of the one-way ANOVA showed there were significant differences among all PAWS groups for ATN, TTN, and ATNS. ATN ($F(3,816) = 7.53$, $p < 0.001$), TTN ($F(3,816) = 6.39$, $p < 0.001$), and ATNS ($F(3,816) = 115.7$, $p < 0.001$). The *p*-values of the *F*-test were less than .05 level of significance. Results are shown in Table 18.

Table 18

ANOVA Results of Difference in PAWS Groups (N=205)

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
ATN	11.72	3	3.90	7.53	***0.000****
TTN	59064.31	3	19688.10	6.39	***0.000****
ATNS	456.51	3	1.31	115.7	***0.000****

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

This section represents the results of descriptive statistics between groups for ATN, TTN, and ATNS among all 205 participants for Group 1 (NAVH), Group 2 (AV), Group 3 (H), and Group 4 (AVH). Descriptive statistics for RQ6 are shown in Table 19. Based on mean comparisons shown in Table 19 and graphical representation in Figure 29 for analysis on *ability to notice* phishing. Group 2, AV (audio and visual alerting) was the best performing group and shows the strongest ability to notice phishing among the participants.

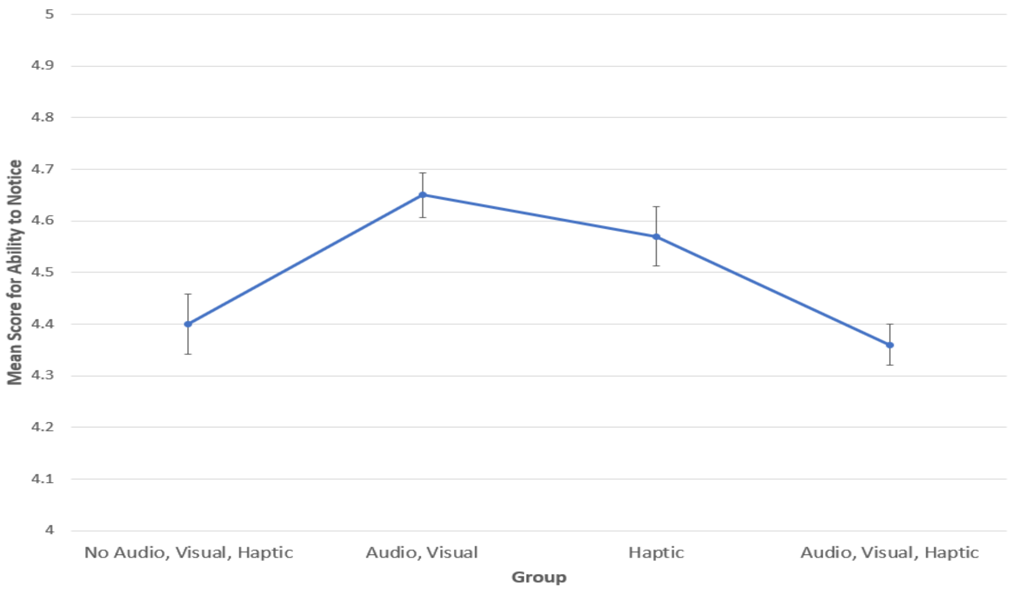
Table 19

Descriptive Statistics of ATN, TTN, and TTNS (N=205)

DV	Group	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
						Lower Bound	Upper Bound
ATN	NAVH	205	4.40	.826	.058	4.29	4.51
	AV	205	4.65	.620	.043	4.57	4.74
	H	205	4.57	.835	.058	4.45	4.68
	AVH	205	4.36	.557	.039	4.28	4.44
TTN	NAVH	205	112.61	51.690	3.610	105.49	119.73
	AV	205	90.75	59.039	4.123	82.62	98.88
	H	205	95.58	52.530	3.669	88.34	102.81
	AVH	205	105.35	58.380	4.077	97.31	113.39
ATNS	NAVH	205	1.08	.928	.065	.96	1.21
	AV	205	2.90	1.388	.097	2.71	3.09
	H	205	2.00	.929	.065	1.87	2.13
	AVH	205	2.87	1.269	.089	2.70	3.05

Figure 29

Mean Score for Ability to Notice Phishing Emails by NAVH, AV, H, and AVH (N=205)

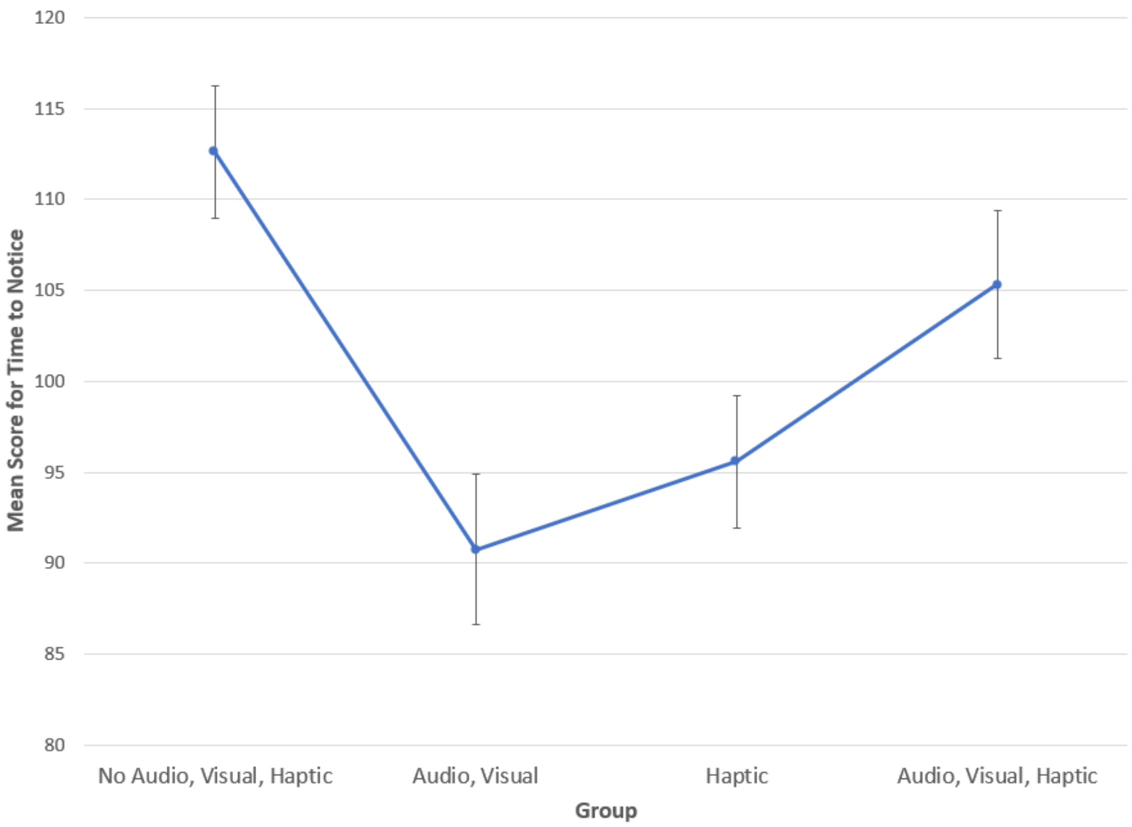


Phase III - RQ6b

Statistically significant mean differences among users' *time to notice* phishing in emails with or without PAWS is represented in Figure 31. Based on mean comparisons shown in Table 19 and graphical representation in Figure 30 for analysis on *time to notice* phishing. Group 2, AV (audio and visual alerting) was the best performing group and shows the least amount of time to notice phishing among the participants.

Figure 30

Mean Score for Time to Notice Phishing in Emails by NAVH, AV, H, and AVH (N=205)



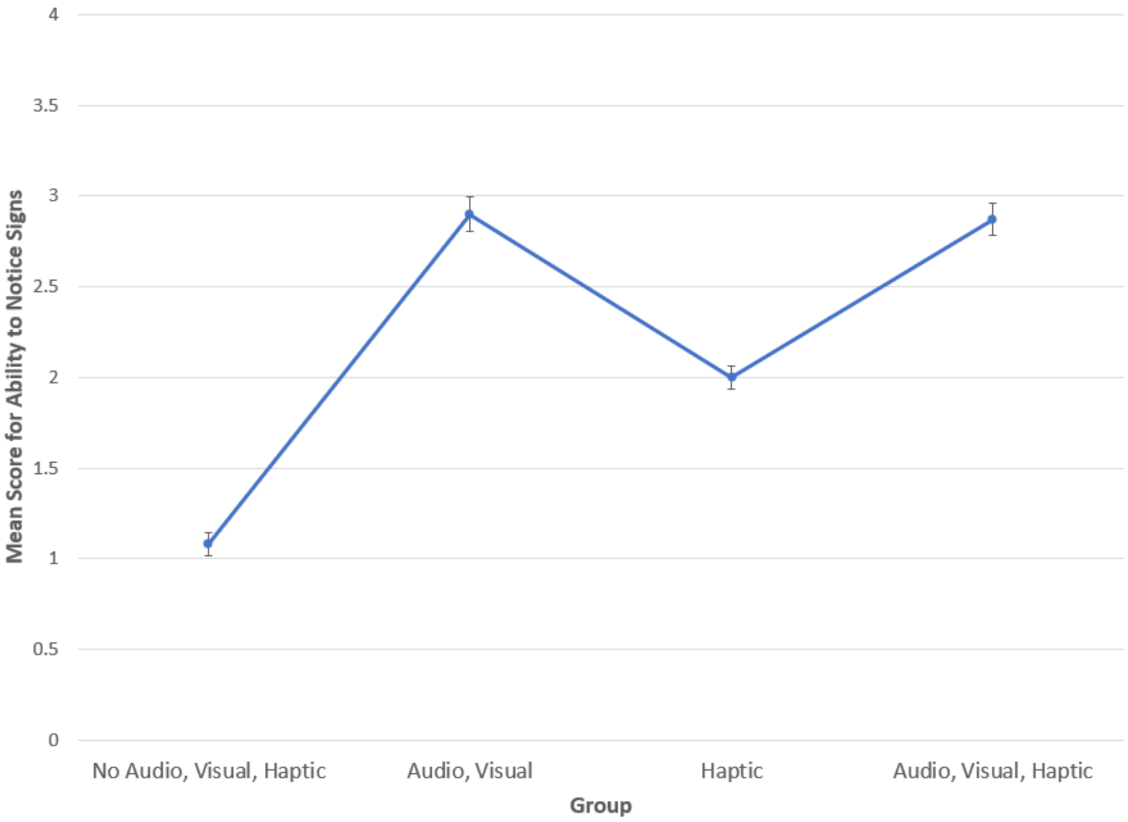
Phase III - RQ6c

To discover if statistically significant mean differences among users' *ability to notice signs* of phishing in emails with or without PAWS is represented in Figure 31.

Based on mean comparisons shown in Table 19 and graphical representation in Figure 31 for analysis on *ability to notice* phishing. Group 2, AV (audio and visual alerting) was the best performing group and shows the strongest ability to notice signs of phishing among the participants.

Figure 31

Mean Score for Ability to Notice Signs of Phishing in Emails by NAVH, AV, H, and AVH (N=205)



Phase III - RQ7a, RQ7b, RQ7c

Statistically significant mean differences among users' *ability to notice, time to notice*, and *ability to notice signs* phishing in emails with or without PAWS based on: (a) age, (b) gender, (c) prior phishing awareness training, and (d) attention span are were determined through ANCOVA analysis.

Phase III – RQ7 – Age Group

Table 20 summarizes the results of ANCOVA to determine if there were significant differences among all four PAWS experiments groups and age groups. The results indicated there were significant differences among age groups (18-20, 21-29, 30-39, 40-49,50-59, 60+) for ATN (*ability to notice*) ATN, (*F*(5,814) = 7.72, *p* <0.001). There were also significant differences among age groups for TTN (*time to notice*), (*F*(5,814) = 8.10, and significant differences for ATNS *(ability to notice signs*) (*F*(5,814) = 2.20, *p* = 0.052).

Table 20

ANCOVA Results of Difference in ATN, TTN, and ATNS by Age Group (N=205)

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
ATN	19.71	5	3.94	7.72	***0.000****
TTN	121999.53	5	24399.90	8.10	***0.000****
ATNS	20.46	5	4.09	2.20	***0.052****

* p <0.05, ** p <0.01, *** p <0.001

Descriptive statistics between groups as well as mean comparisons for age group are represented by mean in Table 21, and Figures 32-34. The highest performing age group among the 205 study participants was 50-59-years old with a mean score of 4.65 for ability to notice phishing, followed closely by 40-49 and 30-39 years old groups with a mean score of 4.59. Age group two, or 21-29 years old were able to notice signs of phishing in the least amount of time by mean (82.09), and 40-49-years old were the best performing group for noticing signs of phishing in emails with the PAWS Mobile App by mean (2.43), followed by 21-29 years old with a mean score of 2.32 among PAWS experiment groups.

Table 21

Descriptive Statistics of ATN, TTN, and TTNS by Age Group (N=205)

DV	Age Group	Mean	Std.Dev.	Std. Error
ATN	18-20	4.13	.773	.081
	21-39	4.41	.803	.054
	30-39	4.59	.671	.051
	40-49	4.59	.650	.050
	50-59	4.65	.650	.064
	60+	4.57	.673	.087
TTN	18-20	105.50	52.671	94.59
	21-29	82.09	52.590	75.10
	30-39	109.69	52.502	101.88
	40-49	104.55	50.694	96.83
	50-59	105.63	66.828	92.64
	60+	120.93	61.297	105.10
ATNS	18-20	1.98	1.334	.139
	21-39	2.32	1.487	.100
	30-39	2.07	1.294	.098
	40-49	2.43	1.369	.106
	50-59	2.11	1.238	.121
	60+	2.18	1.295	.167

Figure 32

Mean Score for Ability to Notice Phishing Emails by Age Group (N=205)

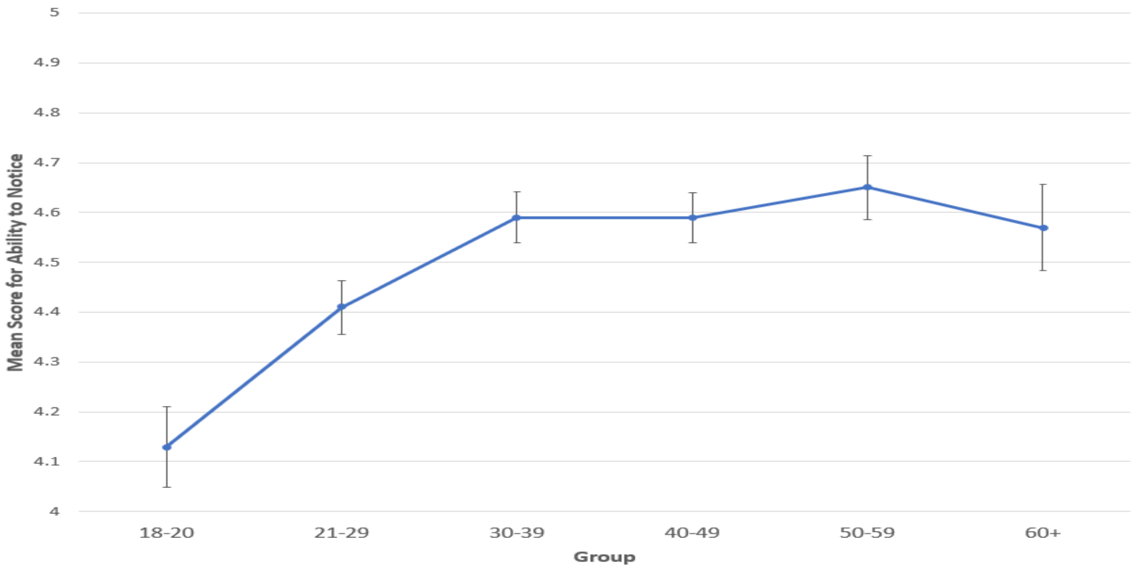


Figure 33

Mean Score for Time to Notice Phishing in Emails by Age Group (N=205)

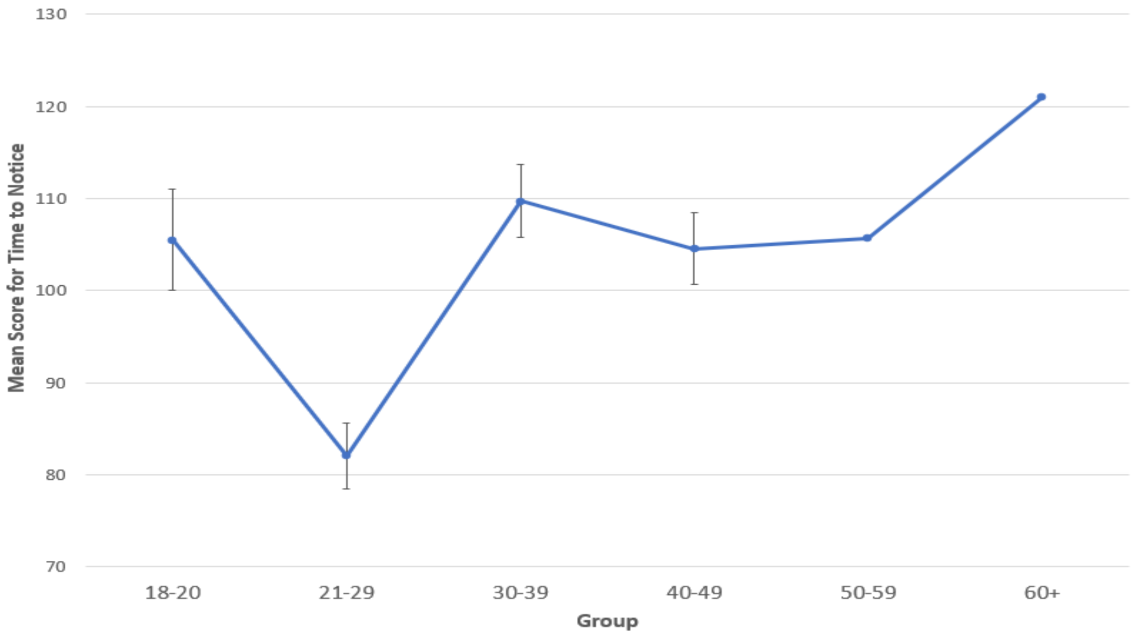
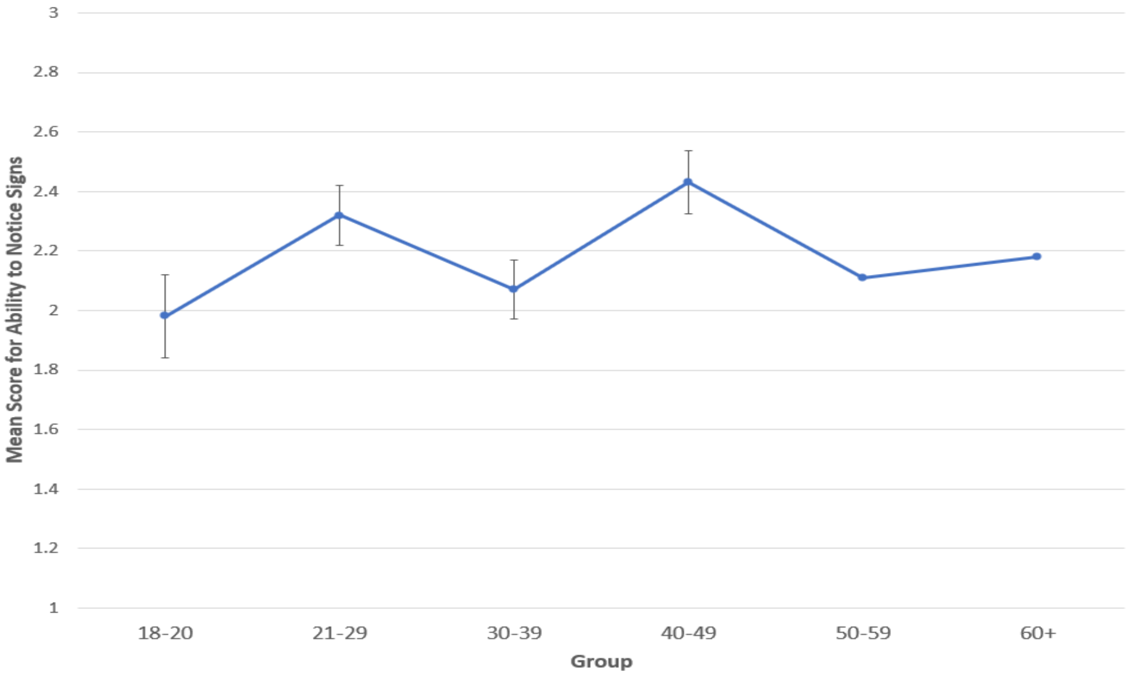


Figure 34

Mean Score for Ability to Notice Signs of Phishing in Emails by Age Group (N=205)



Phase III – RQ7 – By Gender Group

Table 22 summarizes the results of ANCOVA to determine if there were significant differences among all four PAWS experiment groups and gender. The results indicated there were no significant differences among gender groups (female, male, and choose to not answer) for ATN (*ability to notice*), (*F*(2,817) = 1.957, *p* =0.142). Significant differences were shown for TTN (*time to notice*), (*F*(2,817) = 3.970, *p* =0.019), and no significant differences for ATNS (*ability to notice signs*) by gender (*F*(2,817) = 1.597, *p* =0.203).

Table 22

ANCOVA Results of Difference in ATN, TTN, and ATNS by Gender Group (N=205)

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
ATN	2.074	2	1.037	1.957	0.142
TTN	24768.196	2	12384.098	3.970	***0.019****
ATNS	5.957	2	2.979	1.597	0.203

* p <0.05, ** p <0.01, *** p <0.001

Descriptive statistics between groups as well as mean comparisons for gender group are represented by mean in Table 23, and Figures 35-37. Ability to notice phishing mean scores were female at 4.45, male at 4.54 and N/A at 4.63 with no significant statistical significance. Mean analysis for *time to notice* phishing indicated the four participants that chose to not answer the gender identification question were able to notice signs of phishing in less time among the gender groups. Ability to notice signs of phishing in emails analysis among gender groups indicated female mean scores at 2.24, male at 2.16 and N/A at 2.75 with no significant statistical significance among PAWS experiment groups.

Table 23

Descriptive Statistics of ATN, TTN, and ATNS by Gender Group (N=205)

DV	Gender	Mean	Std.Dev.	Std. Error
ATN	Female	4.45	.764	.038
	Male	4.54	.698	.035
	N/A	4.63	.500	.125
TTN	Female	99.61	54.654	2.733
	Male	103.94	57.743	2.873
	N/A	65.19	29.492	7.373
ATNS	Female	2.24	1.361	.068
	Male	2.16	1.343	.067
	N/A	2.75	1.949	.487

Figure 35

Mean Score for Ability to Notice Phishing Emails by Gender Group (N=205)

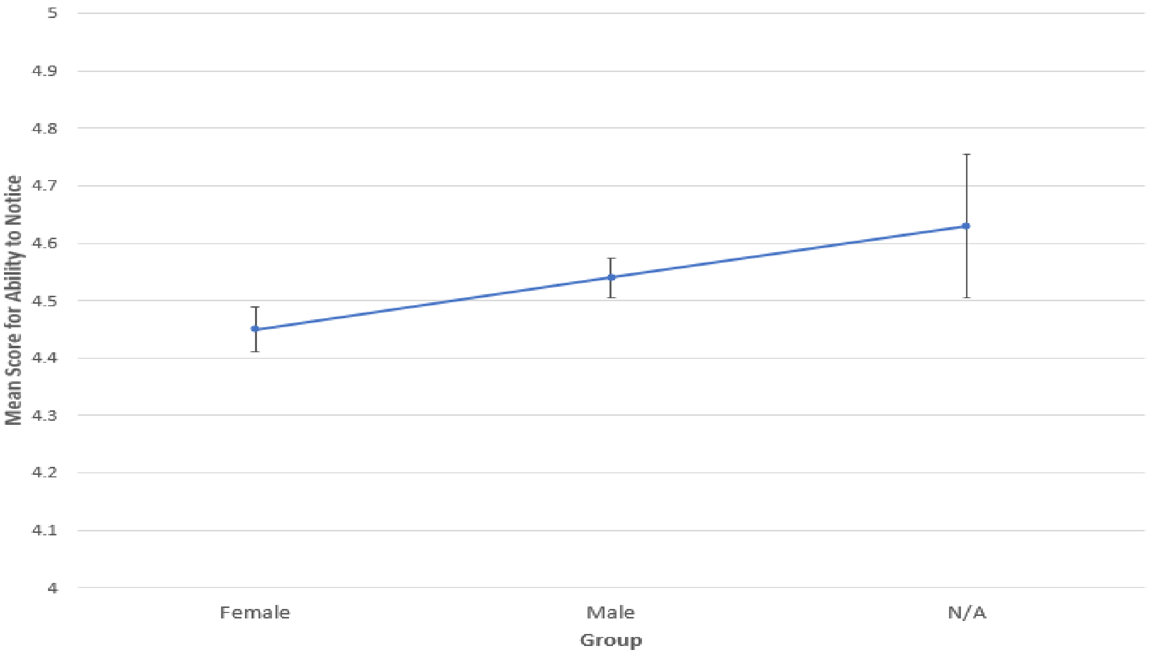


Figure 36

Mean Score for Time to Notice Phishing in Emails by Gender Group (N=205)

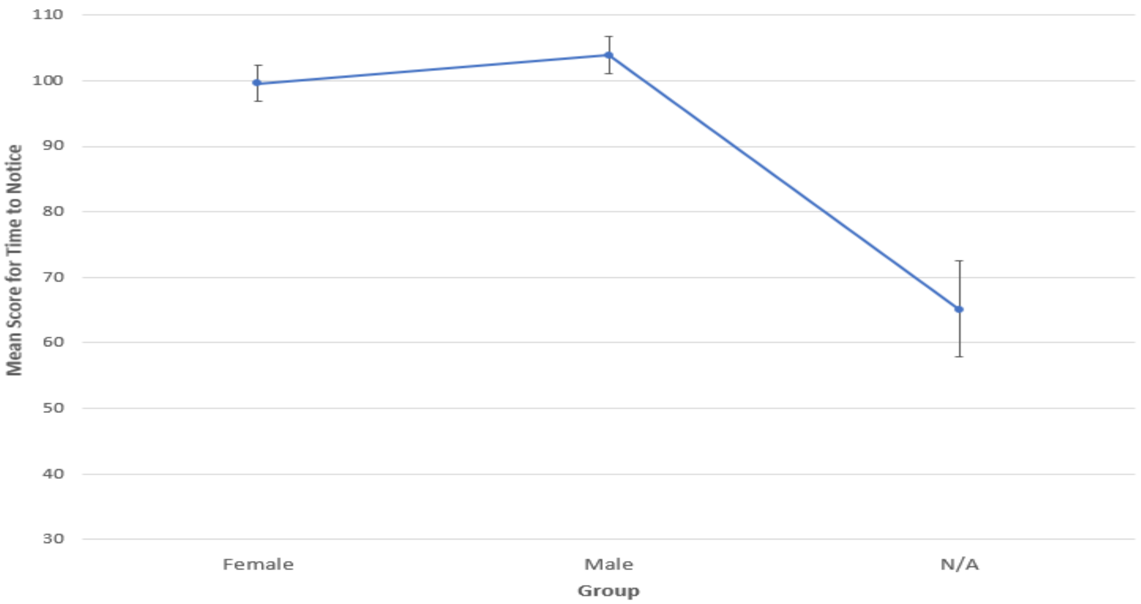
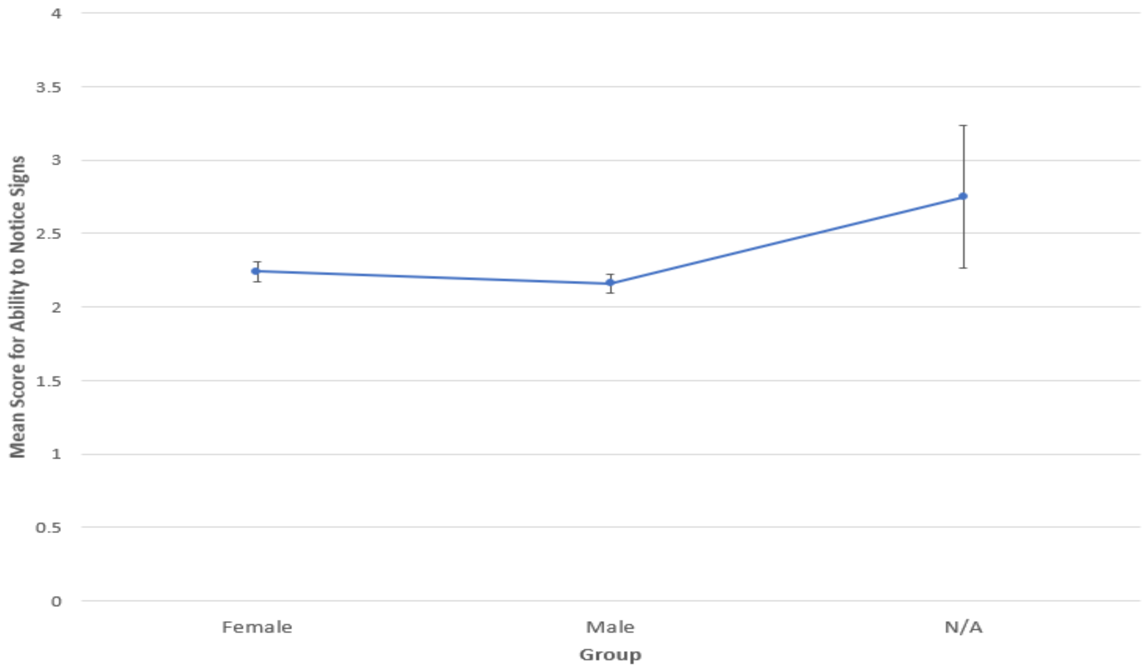


Figure 37

Mean Score for Ability to Notice Signs of Phishing in Emails by Gender Group (N=205)



Phase III – RQ7 – By Prior Experience with Phishing Training Group (N=205)

Table 24 summarizes the results of ANCOVA to determine if there were significant differences among all four PAWS experiment groups and prior phishing training among the participants. and The results indicated there were significant differences among phishing training groups (prior training, no prior training, not sure if training was received, and choose to not answer) for ATN (*ability to notice*), (*F*(3,816) = 8.319, *p* <0.001), no significant differences for TTN *(time to notice*), (*F*(3,816) = 1.517, *p* = 0.209), and significant differences for ATNS (*ability to notice signs*) by phishing training group (*F*(3,816) = 4.925, *p* = 0.002).

Table 24

ANCOVA Results of Difference of ATN, TTN, and ATNS by Prior Experience with Phishing Training Group (N=205)

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
ATN	12.908	3	4.303	8.319	***0.000****
TTN	14275.368	3	4758.456	1.517	0.209
ATNS	27.203	3	9.068	4.925	***0.002***

* p <0.05, ** p <0.01, *** p <0.001

Descriptive statistics between groups as well as mean comparisons for prior phishing training group are represented by mean in Table 25, and Figures 38-40. Participants with prior phishing training totaled a mean score of 4.41 and those without prior phishing training at 4.63 indicating phishing training made a minimal difference on noticing phishing emails among the 205 participants. Mean scores for time to notice phishing were 98.87 for those with training, 103.82 for those without training, and 105.00 and 68.25 for those not sure if they have had phishing training in the past, and those choosing not to answer among PAWS experiment groups.

Table 25

Descriptive Statistics of ATN, TTN, and ATNS by Prior Experience with Phishing Training Group (N=205)

DV	Training	Mean	Std.Dev.	Std. Error
ATN	Training	4.41	.788	.039
	No training	4.63	.604	.032
	Not sure	4.23	.853	.114
	No answer	4.63	.744	.263
TTN	Training	98.78	60.347	.067
	No training	103.82	48.818	.071
	Not sure	105.00	67.183	.192
	No answer	68.25	30.946	10.941
ATNS	Training	2.08	1.355	.067
	No training	2.35	1.333	.071
	Not sure	2.13	1.440	.192
	No answer	3.50	1.852	.655

Figure 38

Mean Score for Ability to Notice Phishing Emails by Prior Experience with Phishing Training Group (N=205)

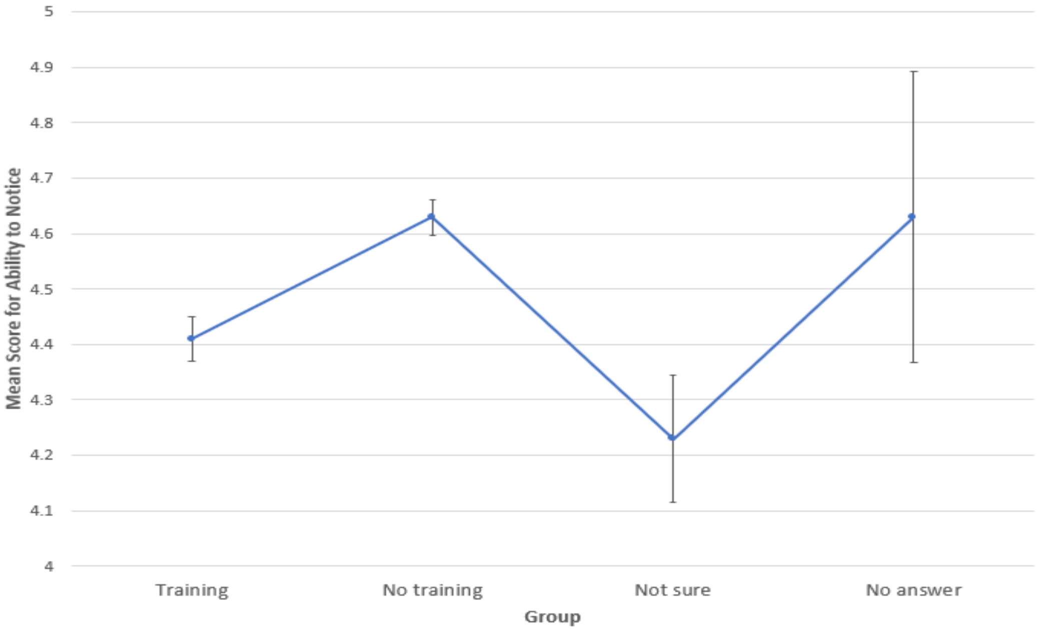


Figure 39

Mean Score for Time to Notice Phishing in Emails by Prior Experience with Phishing Training Group (N=205)

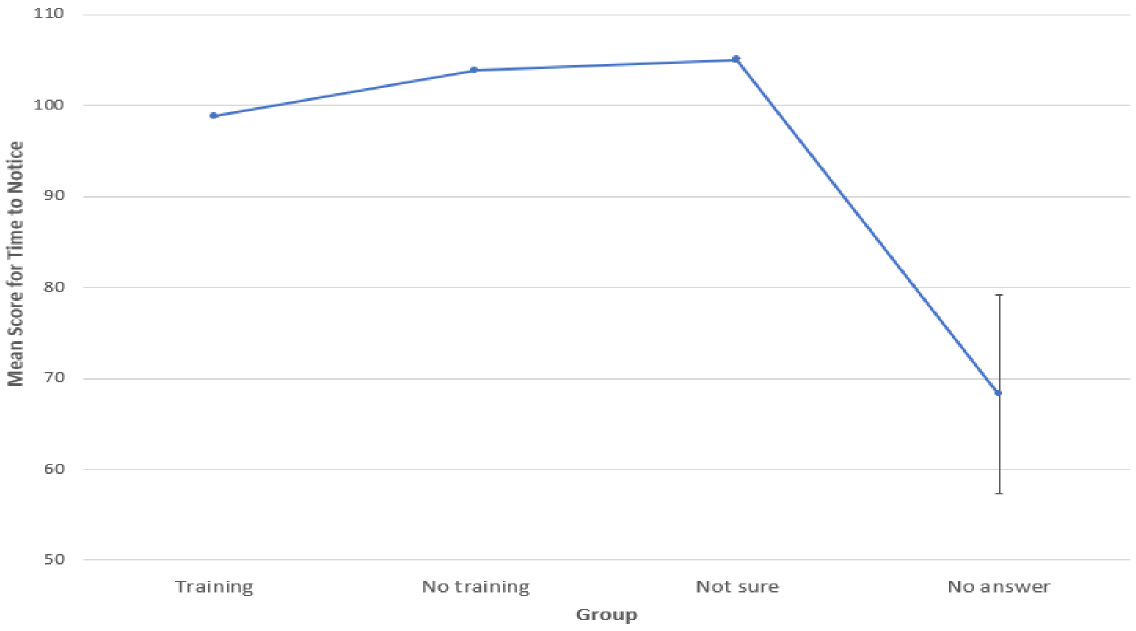
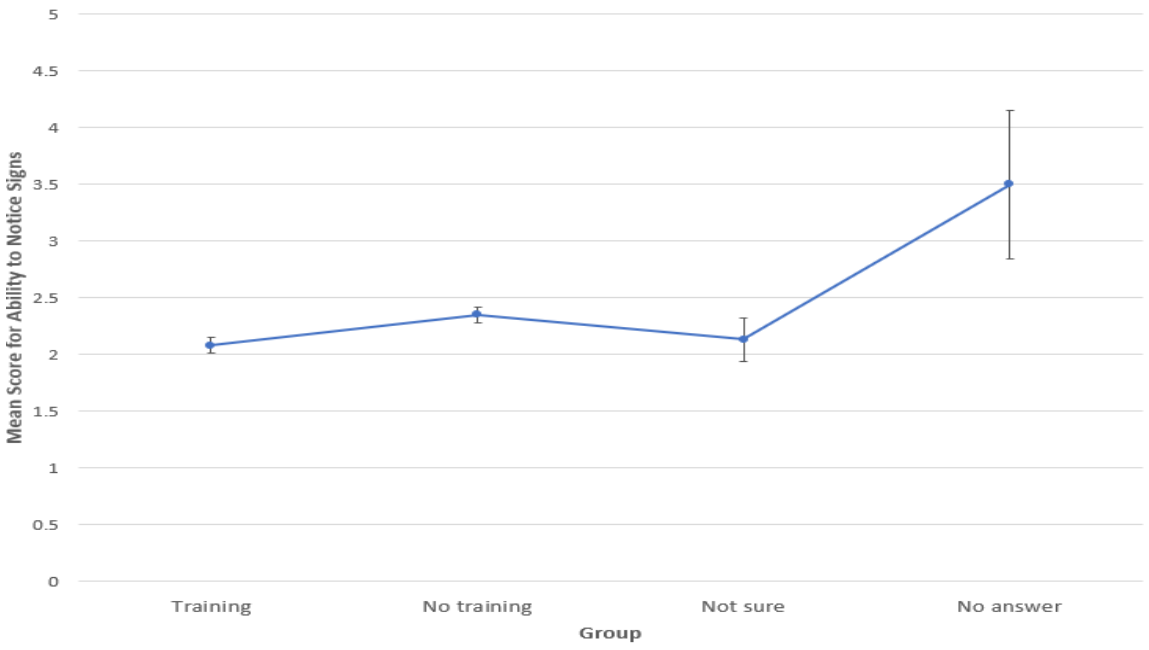


Figure 40

Mean Score for Ability to Notice Signs of Phishing in Emails by Prior Experience with Phishing Training Group (N=205)



Phase III – RQ7 – By Attention Span Score Group (N=205)

Table 26 summarizes the results of ANCOVA to determine if there were significant differences among all four PAWS experiment groups and attention span scores among the participants. The results showed there were significant differences among attention span scores among the participants for ATN (*ability to notice*), (*F*(19,800) = 2.038, *p* <0.006). There were significant differences for TTN (*time to notice*), (*F*(19,800) = 3.456, *p* <0.001), and no significant differences for ATNS (*ability to notice signs*) by attention span score (*F*(19,800) = 0.714, *p* =0.807.

Table 26

ANCOVA Results of Difference of ATN, TTN, and ATNS by Attention Span Score Group (N=205)

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
ATN	20.081	19	1.057	2.038	***0.006*****
TTN	195196.490	19	10273.499	3.456	***0.000******
ATNS	25.509	19	1.343	0.714	0.807

* p <0.05, ** p <0.01, *** p <0.001

Descriptive statistics between groups as well as mean comparisons for attention span score are represented by mean in Table 27, and Figures 41-43. Among PAWS experiment groups. Attention span score of nine (high-attention span) with a mean score of 5.0 were able to notice the most phishing emails among the 205 participants and were also able to notice phishing in less time than the other attention span score groups. Attention span score nine group also noticed the most signs of phishing among all PAWS experiment groups.

Table 27

Descriptive Statistics of ATN, TTN, and ATNS by Attention Span Score Group (N=205)

DV	Attn. Score	Mean	Std.Dev.	Std. Error
ATN	3	4.25	.500	.250
	7	4.25	.957	.479
	9	5.00	.000	.000
	10	4.75	.463	.164
	11	4.84	.369	.065
	12	4.70	.470	.105
	13	4.53	.716	.113
	14	4.57	.698	.085
	15	4.32	.819	.097
	16	4.50	.768	.084
	17	4.69	.531	.066
	18	4.55	.581	.061
	19	4.55	.737	.085
	20	4.30	.795	.120
	21	4.49	.787	.093
	22	4.37	.768	.106
	23	4.42	.717	.146
	24	4.13	.942	.166
	25	4.33	.888	.256
	26	4.38	.957	.239
TTN	3	108.00	25.742	12.871
	7	83.00	11.195	5.598
	9	44.75	12.659	6.329
	10	78.50	28.046	9.916
	11	80.09	35.572	6.288
	12	107.05	39.046	8.731
	13	81.05	43.242	6.837
	14	92.78	30.533	3.703
	15	115.38	74.867	8.823
	16	110.46	61.761	6.739
	17	92.50	45.161	5.645
	18	128.41	67.425	7.029
	19	98.88	57.598	6.607
	20	117.00	68.737	10.363
	21	98.28	56.445	6.652
	22	87.10	41.674	5.779
	23	94.46	48.704	9.942
	24	77.72	37.957	6.710
	25	111.50	57.205	16.514
	26	85.75	22.413	5.603

Table 27

Descriptive Statistics of ATN, TTN, and ATNS by Attention Span Score Group (N=205) – (cont.)

DV	Attn. Score	Mean	Std.Dev.	Std. Error
ATNS	3	2.00	.816	.408
	7	2.50	1.732	.866
	9	3.00	1.414	.707
	10	2.38	1.685	.596
	11	2.41	1.500	.265
	12	2.40	1.273	.285
	13	2.13	1.488	.235
	14	2.04	1.215	.147
	15	2.24	1.369	.161
	16	2.19	1.322	.144
	17	2.36	1.289	.161
	18	2.23	1.384	.144
	19	2.33	1.341	.154
	20	1.64	1.163	.175
	21	2.24	1.429	.168
	22	2.29	1.499	.208
	23	2.13	1.296	.265
	24	2.22	1.601	.283
	25	2.42	1.621	.468
	26	2.25	1.291	.323

Figure 41

Mean Score for Ability to Notice Phishing Emails by Attention Span Score Group (N=205)

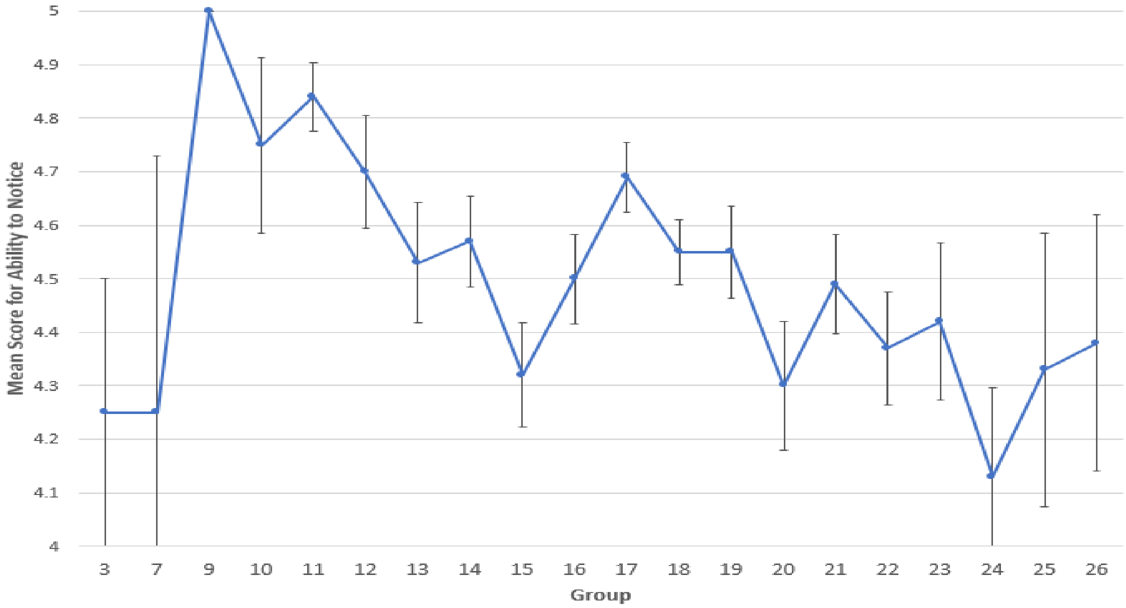


Figure 42

Mean Score for Time to Notice Phishing in Emails by Attention Span Score Group (N=205)

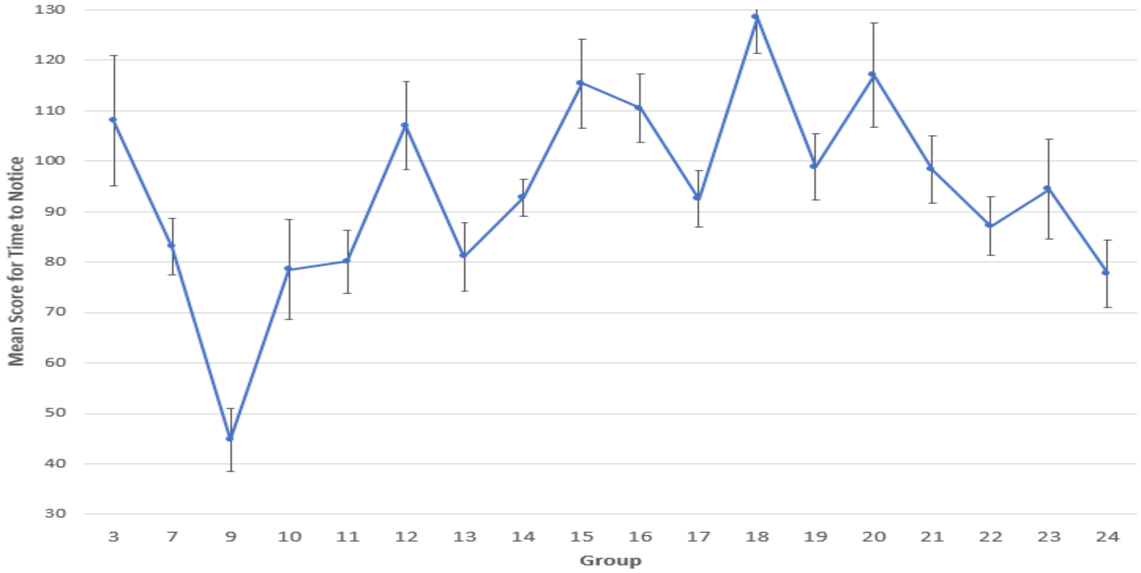
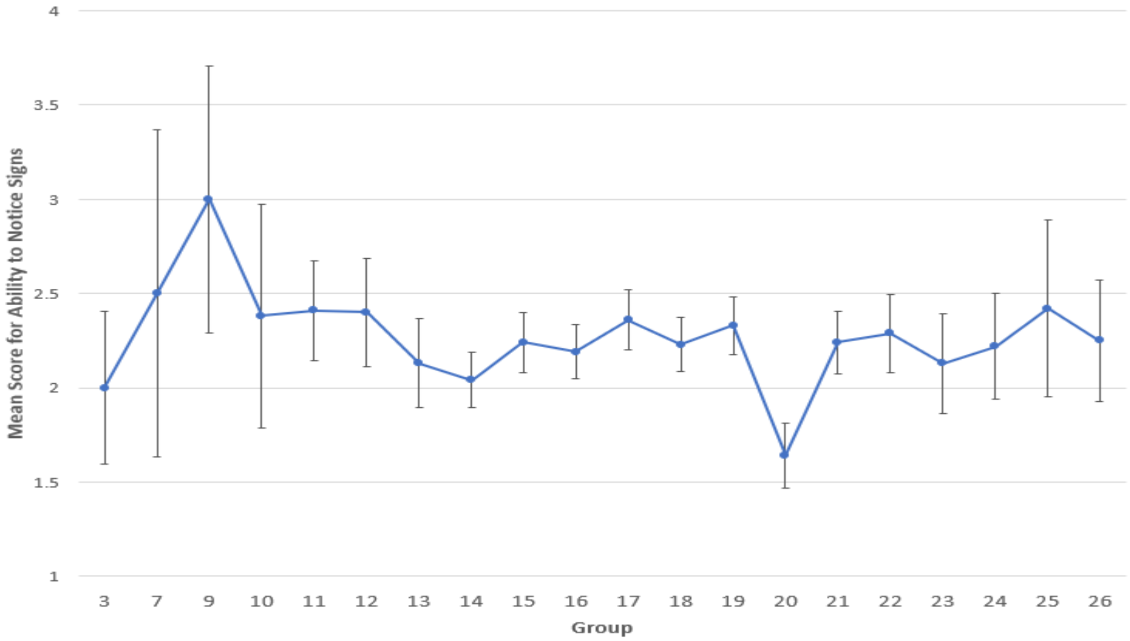


Figure 43

Mean Score for Ability to Notice Signs of Phishing in Emails by Attention Span Score Group (N=205)



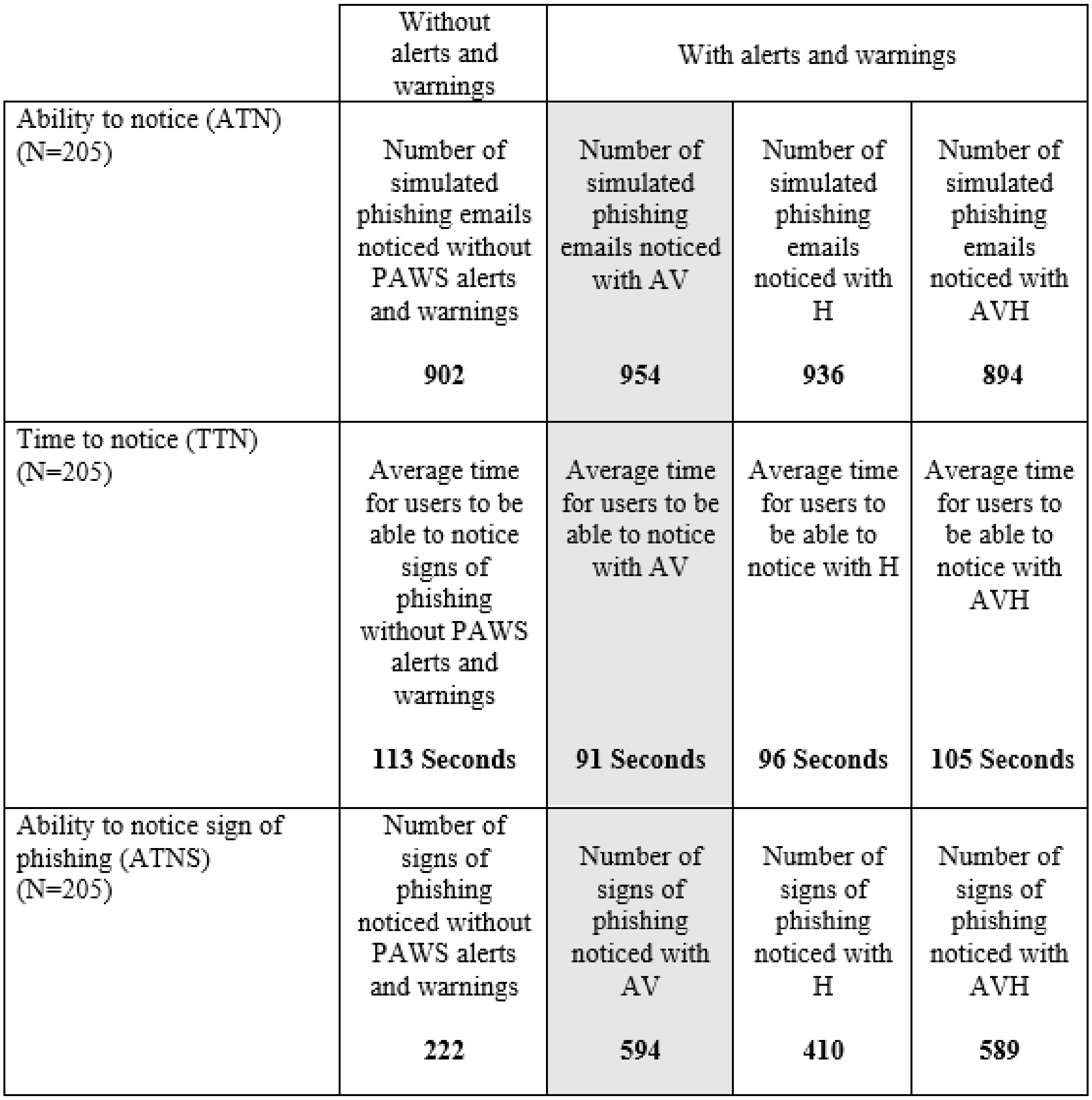
Phase III – RQ6, RQ7 – Additional Analysis

Additional analysis of all PAWS simulated email screens was also performed. As noted previously, 20 simulated emails were presented to the participants via mobile app downloaded to their personal mobile device. The simulated screens were presented in randomized group order (NAVH, AV, H, & AVH) and random email length by group. Data collected on individual participant performance included *ability to notice* phishing (clicking “Phishing” or “Legitimate”), *time to notice* phishing (time in seconds to click “Legitimate” or “Phishing”), and *ability to notice signs* of phishing in emails (clicking what sign of phishing the participant saw) for each of the 20 simulated email screens.

Figure 44 illustrates the indication of the AV (audio and visual alerting) group was the best-performing group of the PAWS groups for *ability to notice, time to notice,* and *ability to notice signs* of phishing in emails. The number of simulated emails screens notices as phishing by the participants was 954 for the AV group, 902 for NAVH, 936 for H, and 894 for AVH group. Time to notice phishing for the AV group was an average of 91 seconds, with NAVH averaging 113 seconds, H averaging 96 seconds, and AVH at 105 seconds. Ability to notice signs of phishing in emails were 594 for the AV group, 222 for NAVH, 410 for H, and 589 for AVH groups.

Figure 44

Sums and Averages for ATN, TTN, and ATNS for All Participants (N=205)



	Without alerts and warnings	With alerts and warnings		
Ability to notice (ATN) (N=205)	Number of simulated phishing emails noticed without PAWS alerts and warnings **902**	Number of simulated phishing emails noticed with AV **954**	Number of simulated phishing emails noticed with H **936**	Number of simulated phishing emails noticed with AVH **894**
Time to notice (TTN) (N=205)	Average time for users to be able to notice signs of phishing without PAWS alerts and warnings **113 Seconds**	Average time for users to be able to notice with AV **91 Seconds**	Average time for users to be able to notice with H **96 Seconds**	Average time for users to be able to notice with AVH **105 Seconds**
Ability to notice sign of phishing (ATNS) (N=205)	Number of signs of phishing noticed without PAWS alerts and warnings **222**	Number of signs of phishing noticed with AV **594**	Number of signs of phishing noticed with H **410**	Number of signs of phishing noticed with AVH **589**

Table 28 itemizes each PAWS simulated email screen by correct clicks by the participant, number of TTN below the SME agreed time of 25 seconds for maximum time to notice phishing in emails, and correct clicks by the participant towards identification of signs of phishing in the specified simulated email screen. Figure 45 illustrates Table 28.

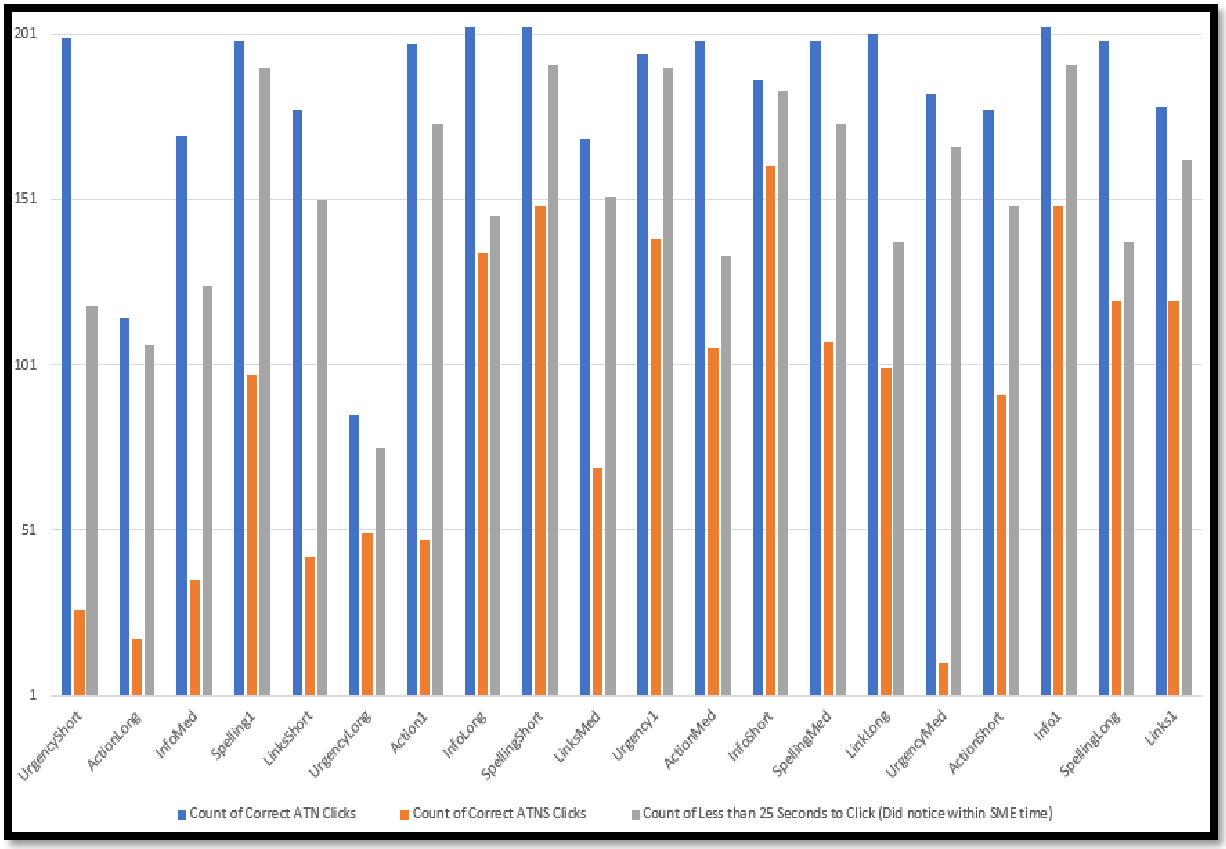
Table 28

Sums and Averages for PAWS Simulated Email Screens by Participant (N=205)

PAWS Screen Version		Group	ATN Clicks	TTN < = 25	ATNS
1	UrgencyShort	NAVH	200	119	27
2	ActionLong	NAVH	115	107	18
3	InfoMed	NAVH	170	125	36
4	Spelling1	NAVH	199	191	98
5	LinksShort	NAVH	178	151	43
6	UrgencyLong	AVH	86	76	50
7	Action1	H	198	174	48
8	InfoLong	AV	203	146	135
9	SpellingShort	AVH	203	192	149
10	LinksMed	H	169	152	70
11	Urgency1	AV	195	191	139
12	ActionMed	AVH	199	134	106
13	InfoShort	H	187	184	161
14	SpellingMed	AV	199	174	108
15	LinkLong	AVH	201	138	100
16	UrgencyMed	H	183	167	11
17	ActionShort	AV	178	149	92
18	Info1	AVH	203	192	149
19	SpellingLong	H	199	138	120
20	UrgencyShort	AV	179	163	120

Figure 45

Sum and Averages for PAWS Simulated Email Screens by Participant (n=205)



Summary

The results and data collection were described in this chapter. Phase I results from the SME survey. SMEs voted on each question thus answering RQ1, RQ2, RQ3, and RQ4. Answers from the survey validated constructs for the PAWS Mobile App. Phase II developed, designed, and tested the PAWS Mobile App. Phase III included the PAWS Mobile App study with participants.

The results of Phase I indicated the top signs of phishing, according to SMEs for this study were: sense of urgency, requiring action from the recipient, request for information from the recipient, misspelling and grammar issues in the email, and request for the recipient to click on links. Findings from the SMEs survey also included visual icon matching for each sign of phishing, and a voice over warning announcing each sign of phishing. SMEs also indicated the mobile device should shake/vibrate upon seeing a phishing email to alert the recipient of a phishing email.

Phase II successfully built the PAWS Mobile App from combining constructs determined by the SMEs in Phase I, and qualitative and quantitative testing, as well as pilot testing and user observation testing. Two rounds of testing were completed to ensure validity and accuracy of the study, and to ensure performance of the mobile app on both the Apple App Store and the Google Play Store.

Phase III encompassed all of the PAWS Mobile App results based on data from 205 participants. Participants downloaded the PAWS Mobile App to their personal mobile devices and participated in demographic questions, an attention span test, 20 simulated phishing email screens, and post-PAWS questions. The results from the study indicated visual alerts and audible warnings help participants notice phishing emails, assist the participant in lessening the time it takes to notice phishing in emails, and to notice specific signs of phishing more accurately in emails.

Statistically significant demographic results among the study participants indicated, 50-59 years old (12.7% of the participants) noticed more signs of phishing than other age groups, 21-29 years old (26.8%) of the participants noticed signs of phishing in the least amount of time. The female gender group (48.8% of the participants) and those choosing not to answer gender (2.0% of the participants) noticed phishing emails faster among gender groups. Participants without prior phishing training (42.9% of the participants) were able to identify more phishing emails than those without, unsure or choosing not to answer if they have received prior training. Participants with high attention span scores among the 205 participants noticed signs of phishing in emails and in less time than those with lower attention span scores.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Alerts and warnings help people identify phishing emails sooner than if not presented with alerts and warnings. Audio alerts and visual warnings help participants notice what sign of phishing they saw in an email than without audio and visual alerts and warnings. Additionally, the number of participants clicking “Phishing” in under 25 seconds was higher among the PAWS alert and warning groups than without.

The main goal of this study was achieved by creating a phishing alert and warning system that utilizes audio/visual/haptic alerts to assess participants’ ability to notice phishing emails and assess the time to notice the emails. The alert and warning system successfully measured both ability and time to notice phishing emails with favorable data indicating alerts and warnings helped participants both notice phishing and reduce the time it takes to notice phishing emails.

Discussion

Several limitations surrounded this study. This study was delivered during the COVID-19 pandemic. It is possible the pandemic affected the final participation numbers as participants were not readily accessible or able to be communicated with in order to explain the nature of the study. Increased participation for this version of the PAWS Mobile App could have been improved. Some participants felt the intro dissertation request looked like spam. A pre-request email could have possibly prevented this misunderstanding. Some participants were also wary of submitting their phone number to register as a participant of PAWS. These issues were attempted to be prevented by repeated text indicating the participants information will not be stored or used for any other purpose. For future iterations of PAWS, the de-identification of data text should be prominent in the invitational emails and on the PAWS mobile app itself.

Some simulated email screens did not perform well among all 205 participants. Simulated email screen six, UrgencyLong with audio, visual, and haptic alerting was not a top performing email based on the length of time participants spent viewing the email, low click rates on “Phishing” and low click rates on identification of the sign of phishing. This could also be linked to the possibility of simulated screen placement, as it was number six in the screen order. This simulated email screen would have been the first time the participants saw a visual icon, heard the voice over warning, and felt the haptic/vibration feedback. Several participants noted post-study that they were surprised and/or freighted by the alerts and warnings upon first hearing and seeing them. This is a notable finding as it is possible this simulated email screen jolted participants into System 2 thinking, and all reactions were slower, and more deliberate. Another explanation of this reaction from the participants (as it was the first time the participants heard an audible voice and were started) is the “Oh Shoot” syndrome. The participants’ reaction is an interesting finding as the participants found a voice-over to be a “novel” and “unexpected” alert or warning. Analyzing the participant reaction could be an area for future research.

Simulated email screen 16 showed promising results as the majority of participants clicked “Phishing”, however, a low click rate of 11 for sign of phishing among the participants indicates this simulated email did not contain enough of the elements of urgency in the body of the email. Furthermore, this email screen was included in the haptic only group, therefore not assisting the participant with noticing the sign of phishing in the email through audio or visual assistance. It is recommended that additional analysis on the email screens for future iterations of the PAWS mobile app in order to accommodate for the potential for simulated email screen understandability, as well as tracking of the first email the participants "see and hear" to note if click rates are statistically differing from other simulated email screen click rates. Additionally, a text screen completely explaining that the PAWS Mobile App measures phishing identification and timing among participants may be helpful. Several participants indicated they were unsure what the app's purpose was, or what the participant was supposed to be performing. Several issues were noticed in this study. Potential issues with confusion regarding why a voice was audibly saying the sign of phishing to the participant on the first audio alert. Other possibilities include the simulated email did not look "phishy" enough to the participant.

Implications

There are several implications for cybersecurity, social awareness, and phishing susceptibility reduction. This study implicates phishing email alerts and warnings applied and configured to email applications may play a significant role in the reduction of phishing susceptibility. This study also implicates training for an organization in phishing awareness as well as phishing training with alerts and warnings may play a significant role in the reduction of phishing susceptibility.

Implications for Practice

Corporations could potentially reduce the severity of phishing for both corporate and personal data loss by implementing alerts and warnings on corporate email servers.

User phishing awareness training is also important to reduce phishing susceptibility. Corporations could also perform deeper analysis on their demographic characteristics to determine more high-risk groups among age group, gender, prior phishing training, and attention span.

Implications for Research

Implications for research indicate additional discovery on what audio/visual/haptic alerts and warning combinations could be created to further increase ability to notice, time to notice, and ability to notice signs of phishing among users. Deeper analysis on audio tone, frequency, voice, urgency, and character could identify with users with differing preferences on alerting. Visual icon analysis could also be investigated to improve visual feedback for the email recipient. Haptic vibrations could be researched to determine if frequency and intensity could assist the user more appropriately. Demographic studies could be performed to investigate deeper patterns within age group, gender, effects of phishing training, and attention span.

Recommendations and Future Research

A deeper analysis on audio/visual/haptic alerts and warnings for the PAWS Mobile App should be further performed. Customization for specific groups are also being constructed. Customization includes email, audio/visual/haptic pairings with demographics and background in mind. An addition of artificial intelligence to the PAWS Mobile App is also underway. Email filtering with alerts and warnings could be helpful towards combating the issue of phishing and social engineering. Additionally, hovering ability and link analysis could also be used for future research of the audio/visual/haptic alert and warning technology.

The “Oh Shoot” syndrome, or the moment a participant realized they clicked on a phishing link can be more deeply explored as this research unexpectedly found the first simulated phishing email (In Group 2 - AVH) with audio, visual, and haptic alerting started participants and “slowed down” their reaction time. Those participants that followed up with the researcher after their experience with the PAWS Mobile App indicated they paid more attention after the first audio and visual alert and began questioning the steps they took for the rest of the simulated emails. Additional research or visual observation may add to this body of knowledge.

Summary

In summary, alerts and warnings help users notice phishing emails more easily, and within less time than without alerts and warnings. This study indicates voice over combined with a visual alert is the best combination of alert and warning.

The main research question (RQ) that this study addressed was: What audio/visual/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 on mobile devices and included RQ1, RQ2, RQ3, and RQ4:

RQ1: What are the SMEs’ validated top signs of phishing in emails that are considered the most critical threats to users?

RQ2: What SMEs’ identified audio/visual/haptic alerts and warnings are most valid to pair with the top signs of phishing in emails?

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

RQ4: What is the SMEs’ validated maximum time for users’ *ability to notice* signs of phishing in emails?

Phase I answered RQ1 as the top signs of phishing were identified according to SMEs. RQ2 was answered by pairing SME choices of audio/visual/haptic alerts and warnings with the top signs of phishing according to SMEs. RQ3 was answered as tasks for participants to perform during the study were collected and added to the PAWS Mobile App as data points. RQ4 was answered as 25 seconds was determined as the SMEs maximum time for ability to notice phishing in emails.

Phase II included the construction, programming, testing, and coding of the PAWS Mobile App and answered the following research question:

RQ5: What validation and testing procedures should be considered in order to deliver a mobile app phishing alert and warning system prototype?

RQ5 was answered by utilizing observation testing among pilot testers to determine data accuracy for the PAWS App. Qualitative observation and quantitative analysis and observation were combined to ensure accuracy of PAWS participant clicks and time (in seconds) to click “Phishing” or “Legitimate”. The PAWS Mobile App was successfully built, validated, tested, and delivered on the Apple App Store and the Google Play Store for participant download to their mobile device.

Phase III included the delivery and participation of the PAWS Mobile App and answered the following research questions:

RQ6a: Do statistically significant mean differences exist among users’ *ability to notice* phishing in emails with or without PAWS?

RQ6b: Do statistically significant mean differences exist among users' *time to notice* phishing in emails with or without PAWS?

RQ6c: Do statistically significant mean differences exist among users' *ability to notice signs* of phishing in emails with or without PAWS?

RQ7a: Do statistically significant mean differences exist among users' *ability to notice* phishing in emails with or without PAWS based on: (a) age, (b) gender, (c) experience with phishing awareness training, and (d) attention span?

RQ7b: Do statistically significant mean differences exist among users *time to notice* phishing in emails using PAWS based on: (a) age, (b) gender, (c) experience with phishing awareness training, as well as (d) attention span?

RQ7c: Do statistically significant mean differences exist among users' ability to notice *signs of phishing* in emails with or without PAWS based on: (a) age, (b) gender, (c) prior phishing awareness training, as well as (d) attention span?

RQ6a, RQ6b, and RQ6c were answered by successfully indicating differences in PAWS groups with or without audio and visual warnings. Audio and visual warnings assisted participants in noticing signs of phishing, lessened the time to notice phishing among the participants, and increased the amount signs of phishing noticed.

RQ7a, RQ7b, and RQ7c were answered by indicating some statistical mean differences among participants. Ability to notice signs of phishing was highest among the 50-59 years old age group. Time to notice phishing in emails was fast among the 21-29 years old age group. Time to notice phishing emails was faster among females and those choosing not to answer the gender demographic question. Ability to notice signs of phishing appeared stronger among those that had prior phishing training. Ability to notice phishing was stronger among those with high attention span scores. Time to notice phishing was faster among those with higher attention span scores as well.

Overall, this study developed a phishing alert and warning system utilizing constructs determined by subject matter experts. The study results show statistically significant differences among participants presented with alerts and warnings on simulated phishing emails as compared to no alerts and warnings. Participants were able to notice phishing emails with the assistance of alerts and warnings, notice the phishing emails in less time, and correctly identify what sign of phishing they saw in the simulated email with the use of PAWS Mobile App alerts and warnings.

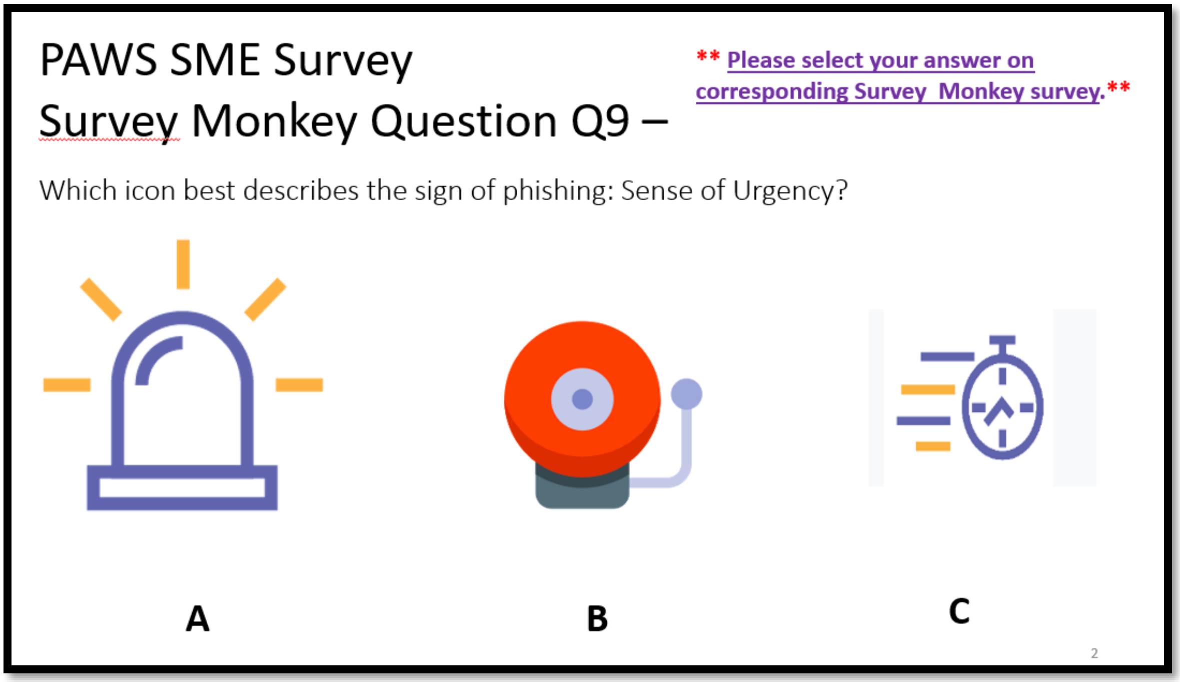
Appendix A

Example of SME Participant Demographic Survey – Survey Monkey and PowerPoint Companion File Screenshots

1. Which of the following describes your current job level?
2. Owner/Executive/C Level
    - Senior Management
    - Middle Management
    - Analyst
    - Instructor/Professor
    - Other
3. How many years of experience do you have in information security?
    - Less than one year
    - At least one year, but less than 3 years
    - At least three years, but less than 5 years
    - At least 5 years, but less than 10 years
    - 10 years or more
4. In your opinion, how significant of an issue is phishing?
    - Not at all significant
    - Low significance
    - Slightly significant
    - Neutral
    - Moderately significant
    - Very significant
    - Extremely significant
5. Please rank the following signs of phishing in emails
    - 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 attachment
    - Threatening language
    - Address mismatch
    - Highly personalized
6. How long should it take a recipient of a phishing email to notice signs of phishing in the email?

- 5 seconds
- 15 seconds
- 25 seconds
- 35 seconds
- 45 seconds
- 55 seconds
- 60 seconds

7. What is the maximum amount of time to lapse before it is determined the recipient did not notice signs of phishing in the email?
    - 5 seconds
    - 15 seconds
    - 25 seconds
    - 35 seconds
    - 45 seconds
    - 55 seconds
    - 60 seconds
    - 65 seconds
    - 70 seconds
    - 75 seconds
    - 85 seconds
    - More than 90 seconds



PAWS SME Survey

Survey Monkey Question Q9 –

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

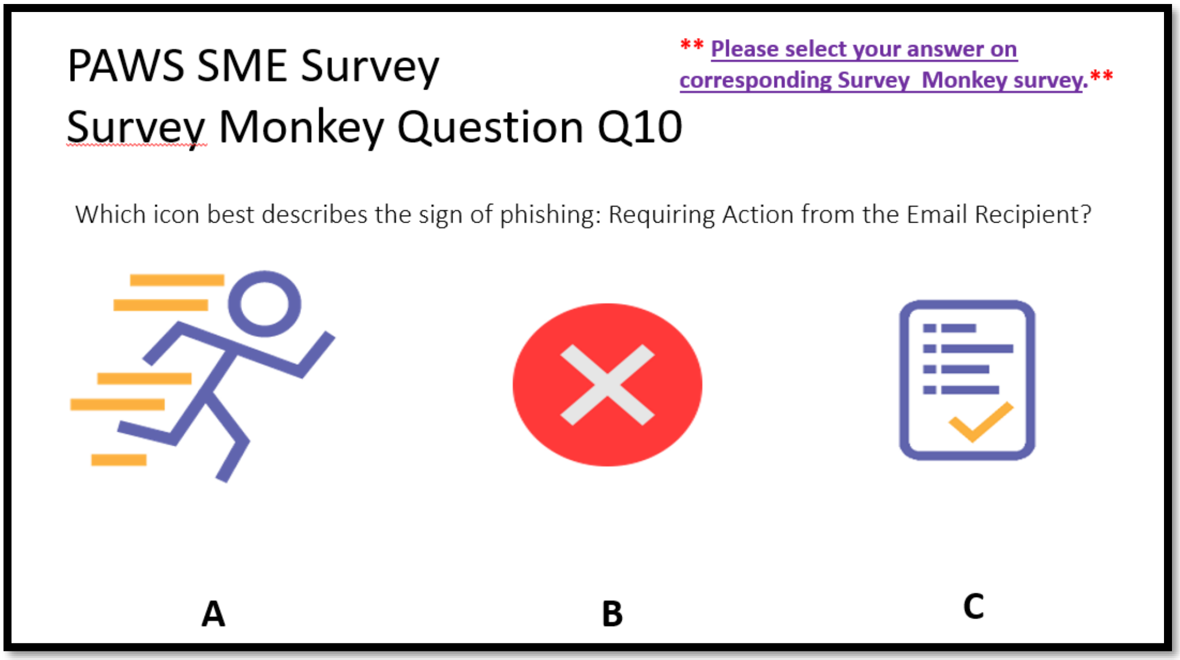
Which icon best describes the sign of phishing: Sense of Urgency?

A

B

C

2



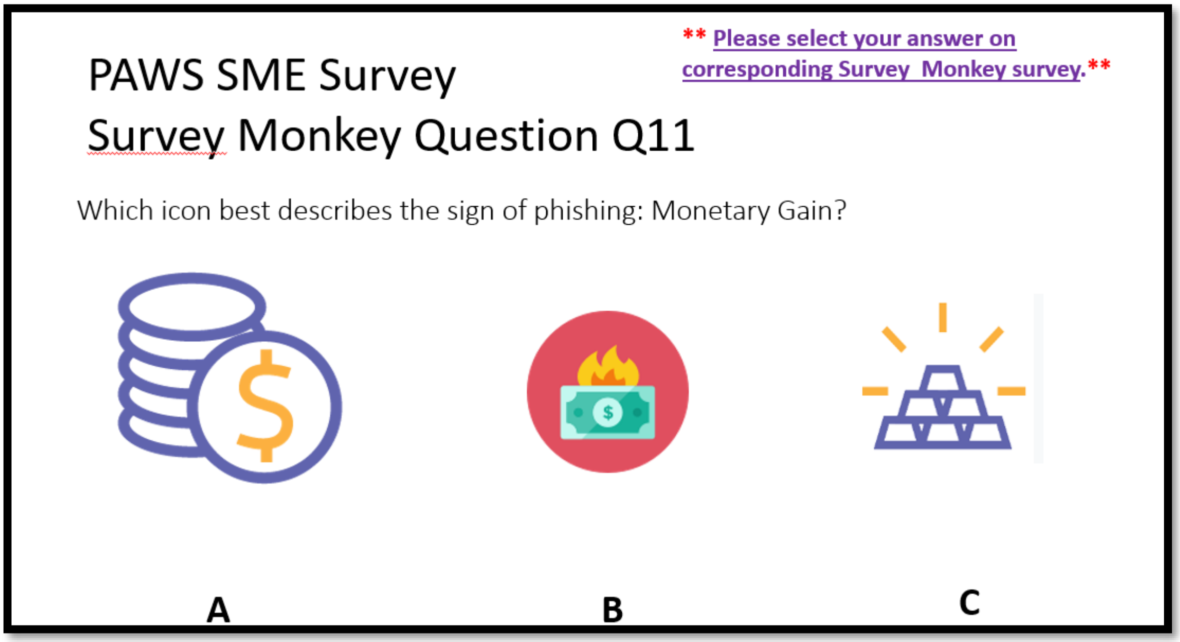
PAWS SME Survey

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?

A **B** **C**



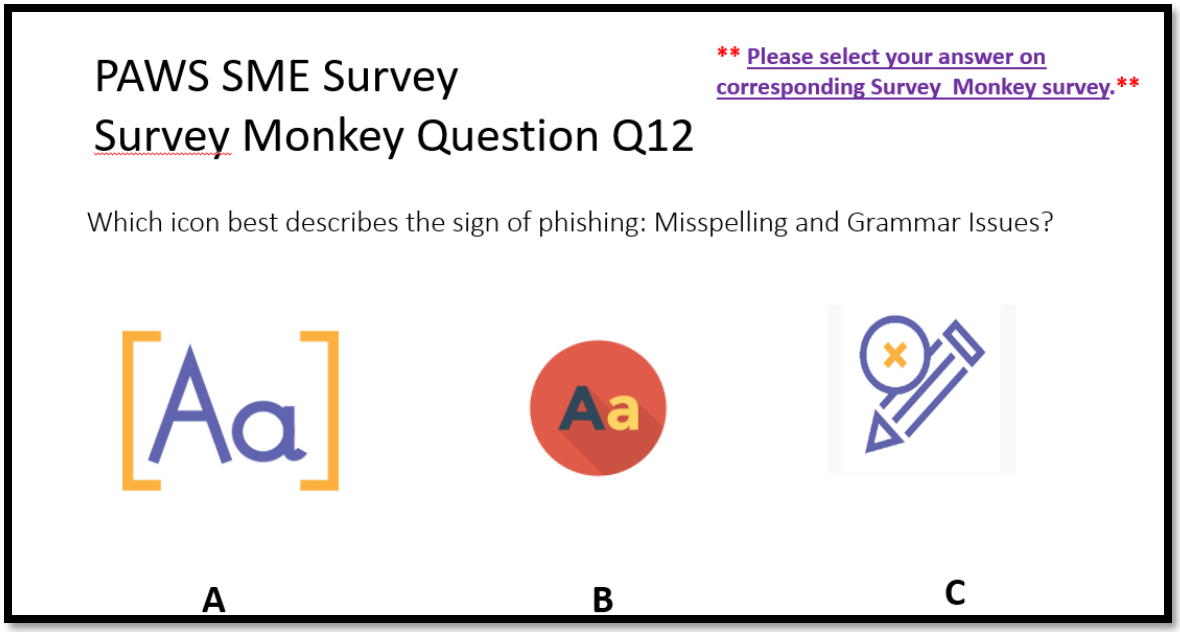
PAWS SME Survey

Survey Monkey Question Q11

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

Which icon best describes the sign of phishing: Monetary Gain?

A **B** **C**

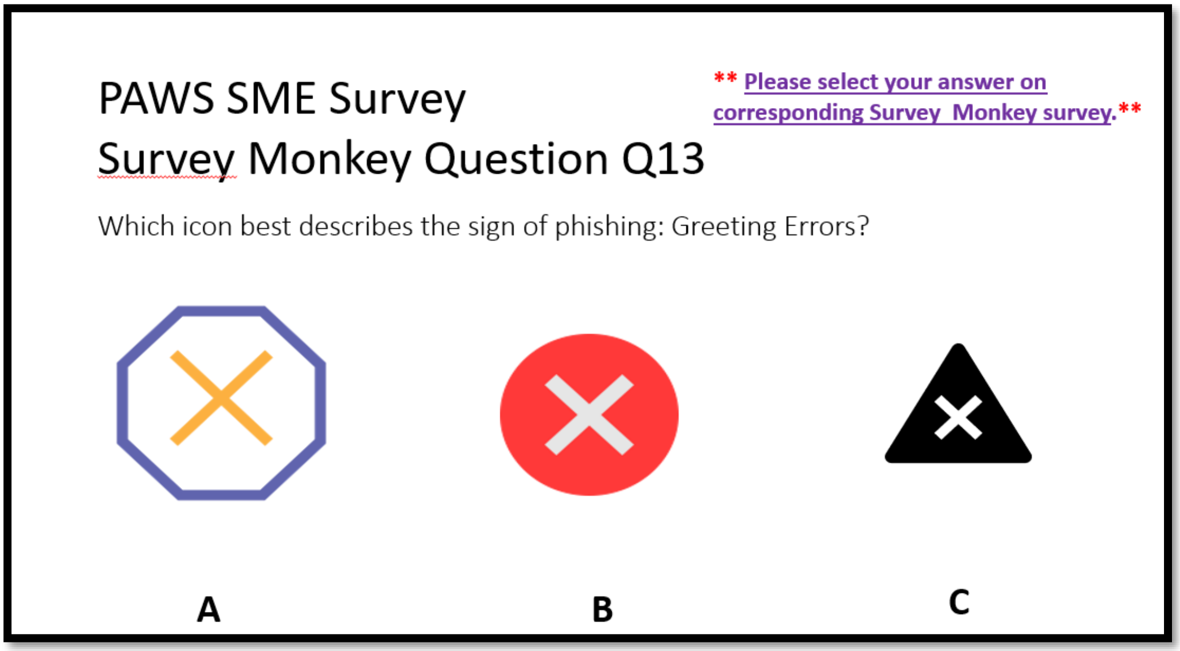


PAWS SME Survey
Survey Monkey Question Q12

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

Which icon best describes the sign of phishing: Misspelling and Grammar Issues?

A B C

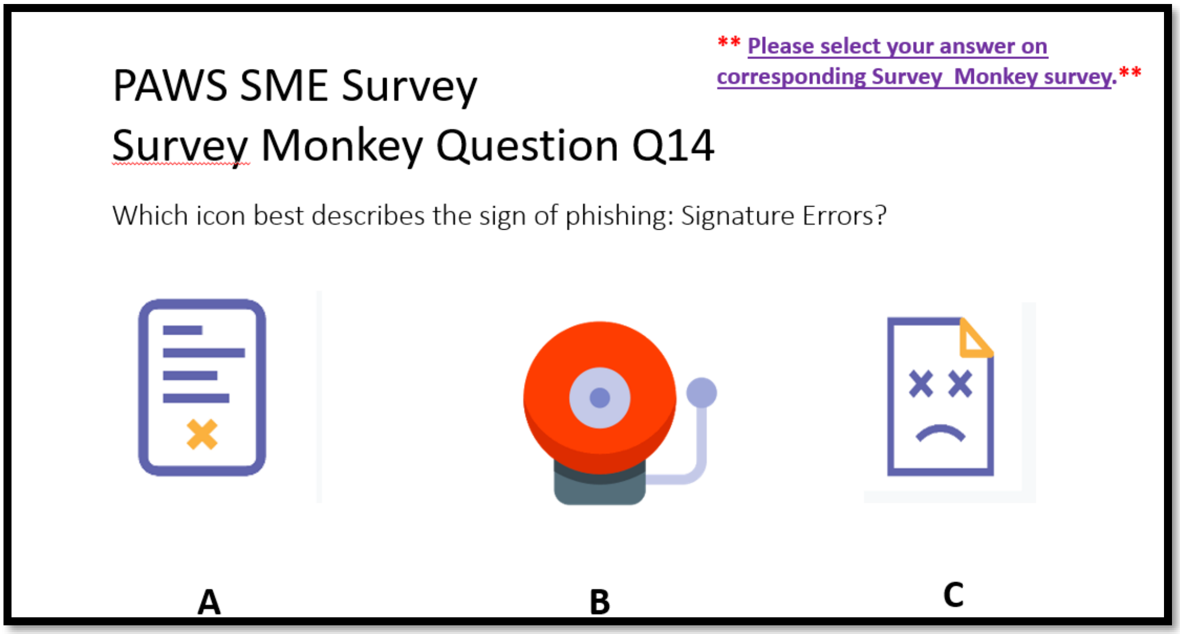


PAWS SME Survey
Survey Monkey Question Q13

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

Which icon best describes the sign of phishing: Greeting Errors?

A B C



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

PAWS SME Survey

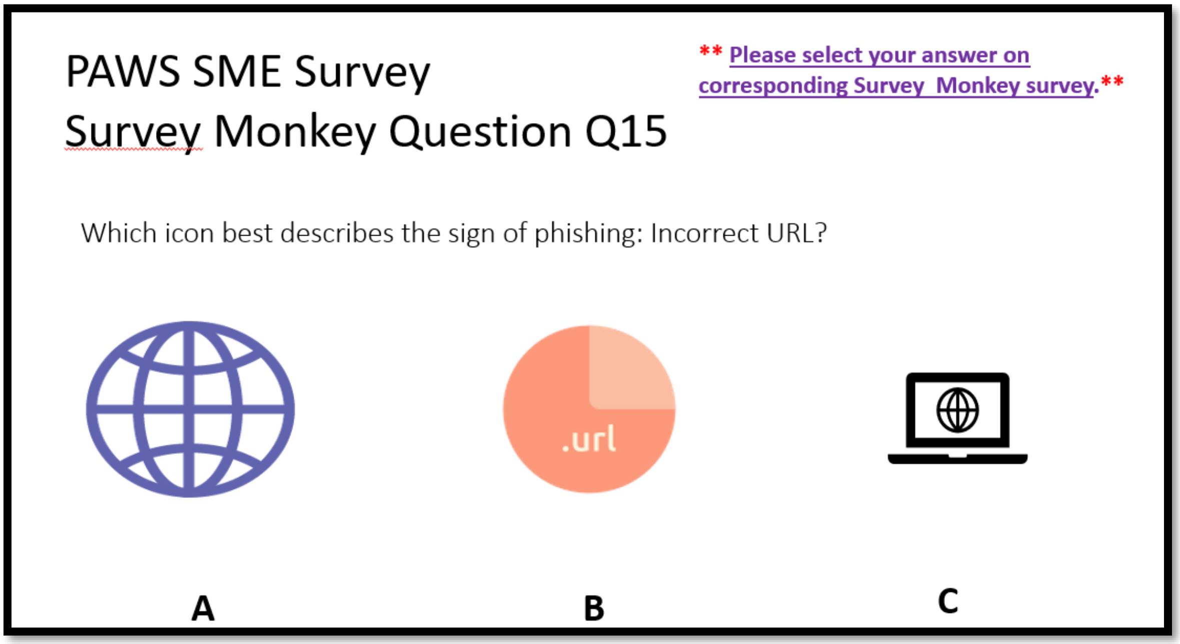
Survey Monkey Question Q14

Which icon best describes the sign of phishing: Signature Errors?

A

B

C



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

PAWS SME Survey

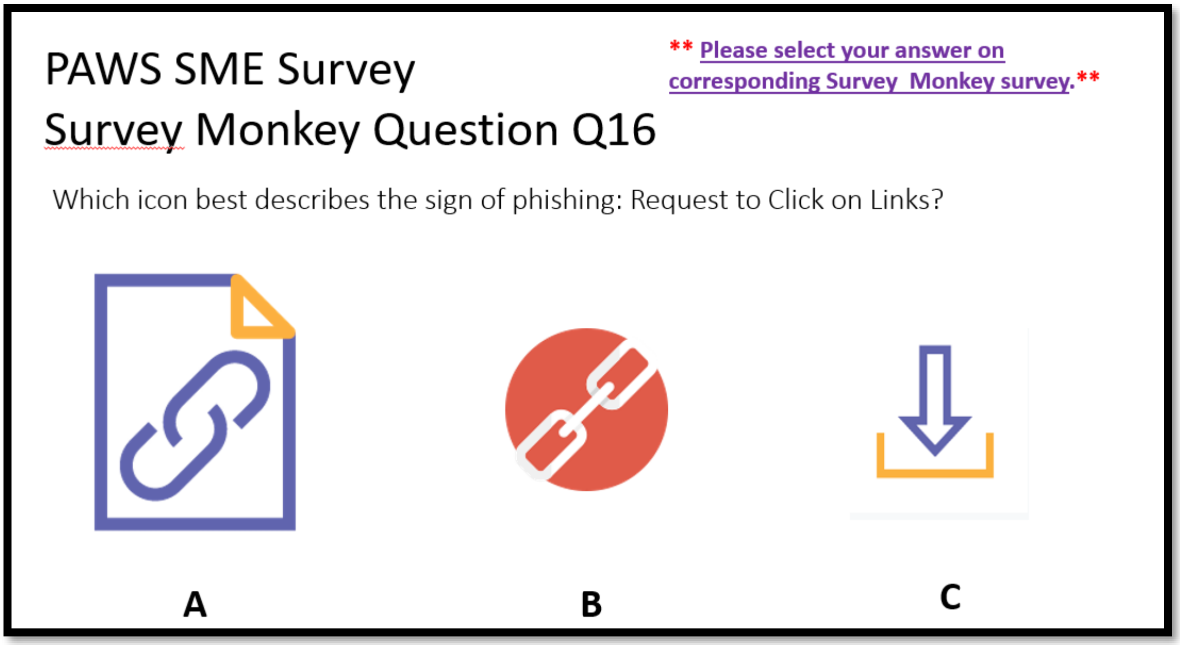
Survey Monkey Question Q15

Which icon best describes the sign of phishing: Incorrect URL?

A

B

C



PAWS SME Survey

Survey Monkey Question Q16

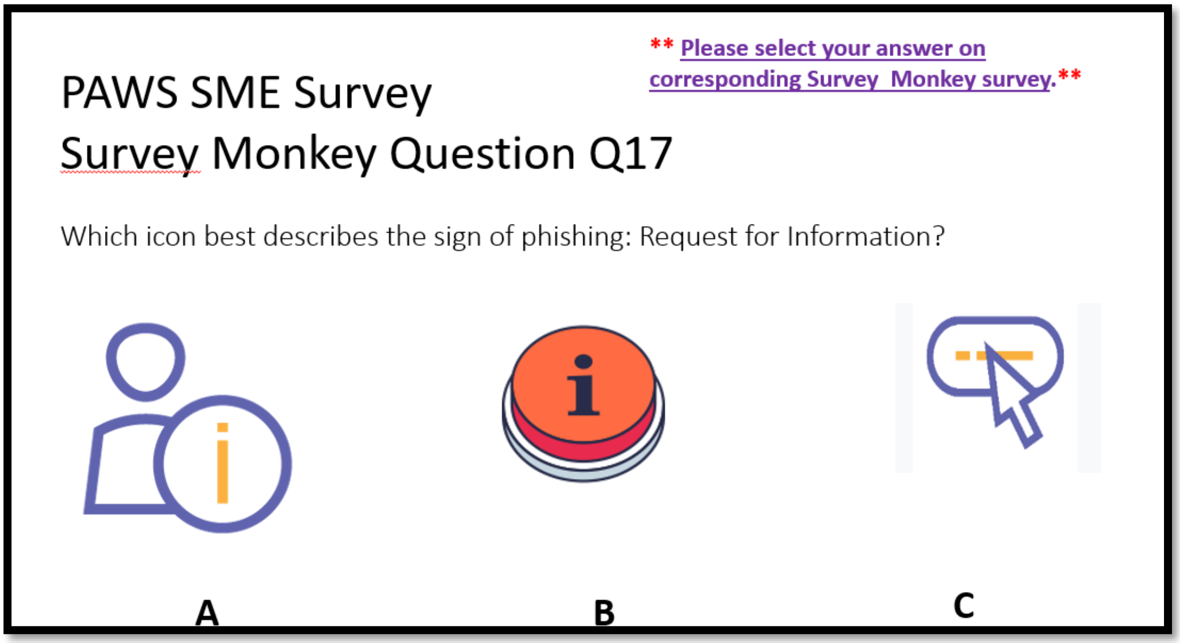
** Please select your answer on corresponding Survey Monkey survey.**

Which icon best describes the sign of phishing: Request to Click on Links?

A

B

C



PAWS SME Survey

Survey Monkey Question Q17

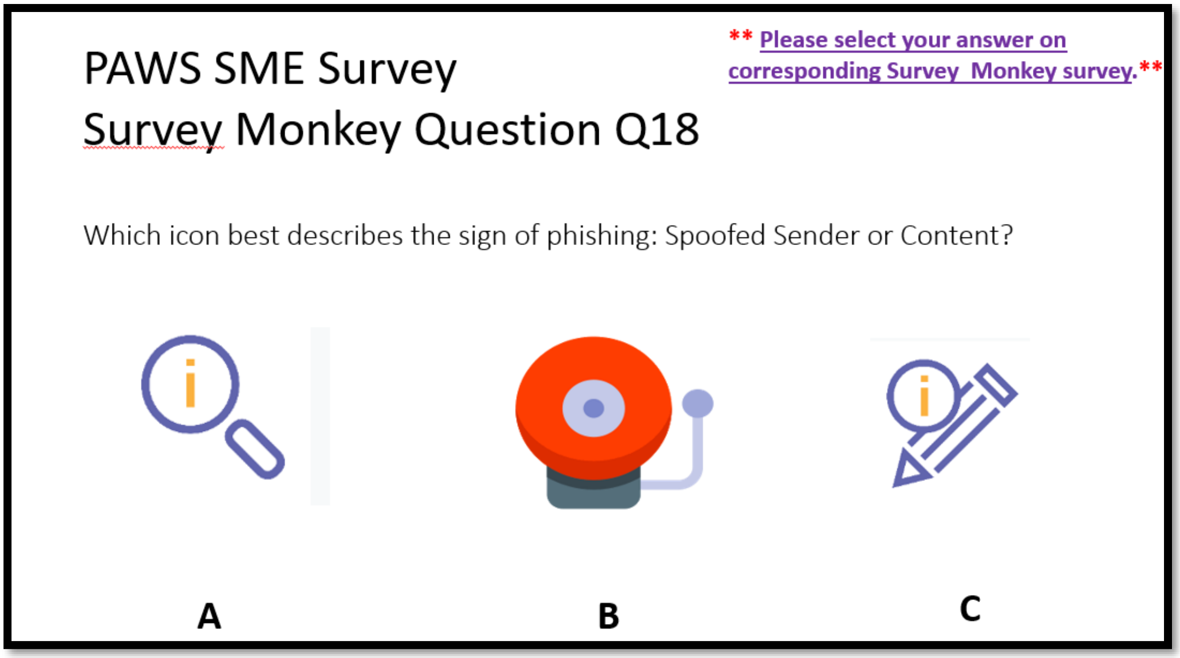
** Please select your answer on corresponding Survey Monkey survey.**

Which icon best describes the sign of phishing: Request for Information?

A

B

C

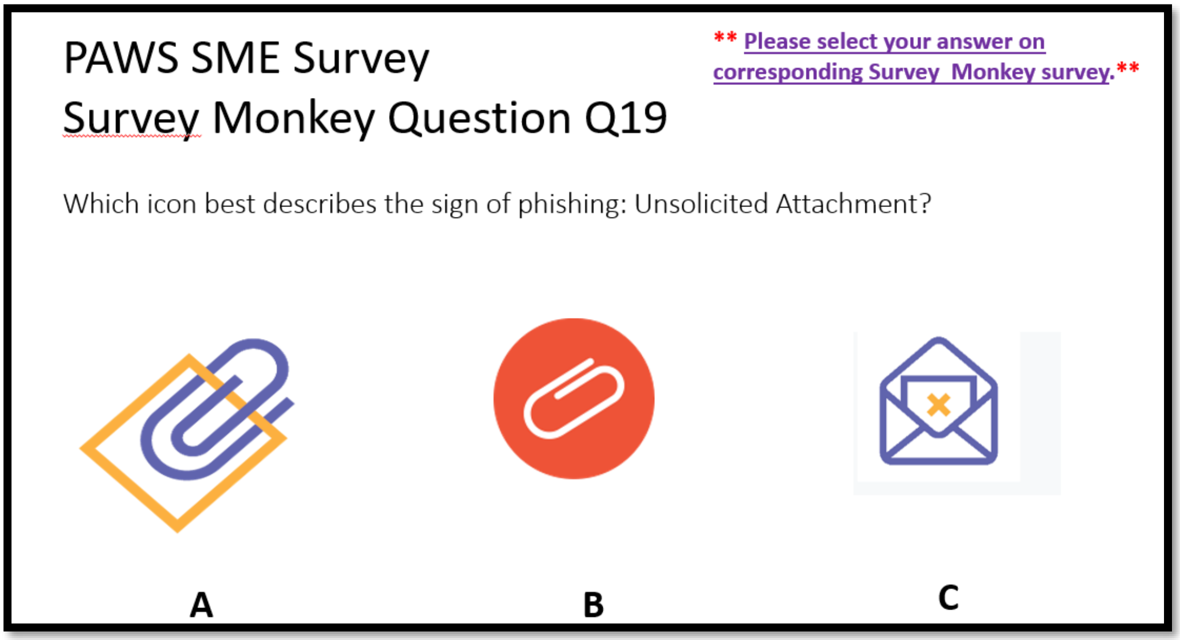


** Please select your answer on corresponding Survey Monkey survey.**

PAWS SME Survey
Survey Monkey Question Q18

Which icon best describes the sign of phishing: Spoofed Sender or Content?

A B C

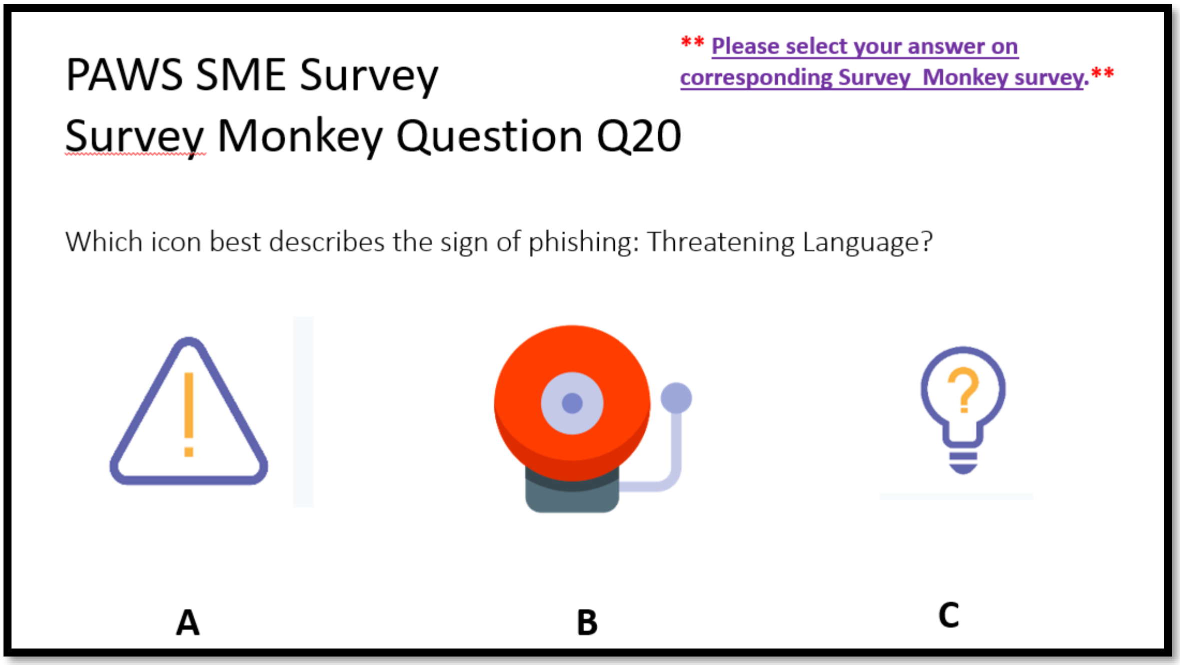


** Please select your answer on corresponding Survey Monkey survey.**

PAWS SME Survey
Survey Monkey Question Q19

Which icon best describes the sign of phishing: Unsolicited Attachment?

A B C

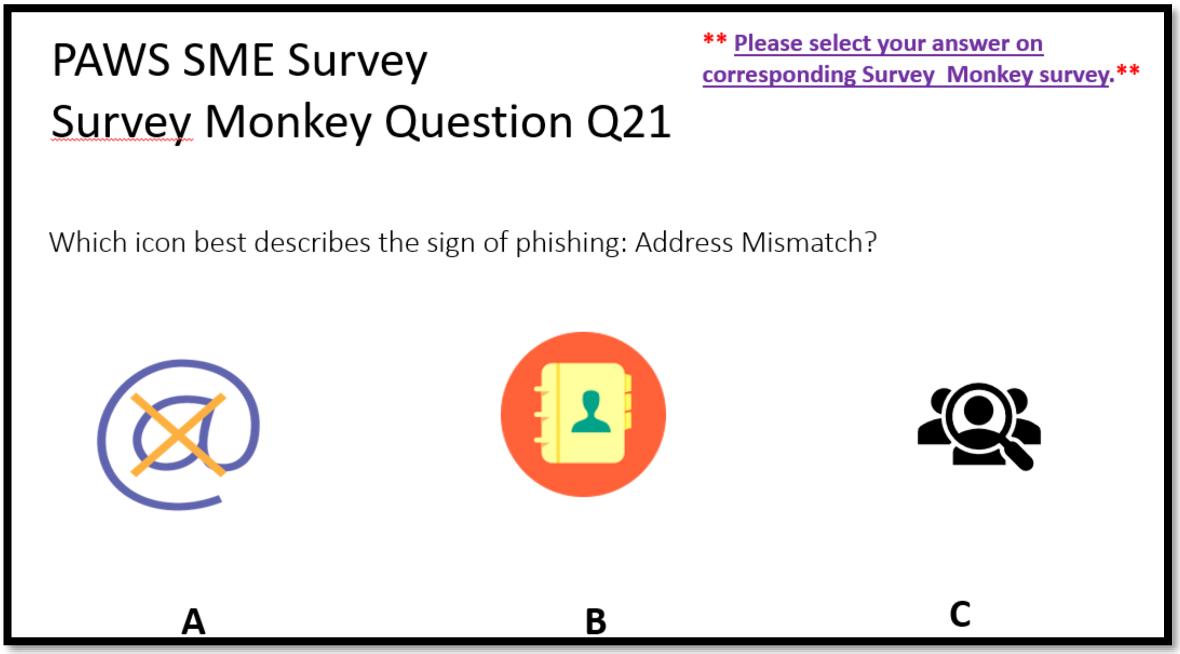


** Please select your answer on corresponding Survey Monkey survey.**

PAWS SME Survey
Survey Monkey Question Q20

Which icon best describes the sign of phishing: Threatening Language?

A B C

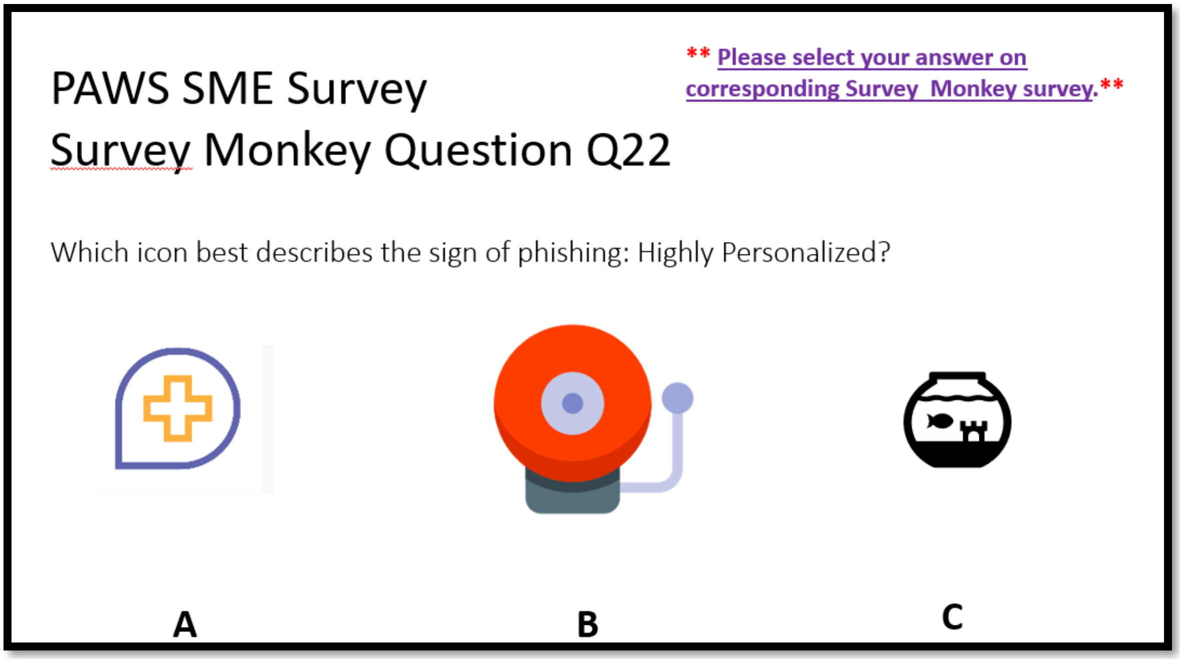


** Please select your answer on corresponding Survey Monkey survey.**

PAWS SME Survey
Survey Monkey Question Q21

Which icon best describes the sign of phishing: Address Mismatch?

A B C



PAWS SME Survey
Survey Monkey Question Q22

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

Which icon best describes the sign of phishing: Highly Personalized?

Appendix B

Example of PAWS Participant Demographic Survey

1. Which category includes your age?
    - 18-20
    - 21-29
    - 30-39
    - 40-49
    - 50-59
    - 60 or older
2. Do you have at least one email account?
    - Yes
    - No
3. Do you use a mobile device to check your email?
    - Yes
    - no
4. What is your gender?
    - Male
    - Female
    - Prefer to not answer
5. What is your primary written language?
    - English
    - Spanish
    - Hindi
    - Arabic
    - Other – input field
6. How many years have you used a mobile device?
    - 0-1
    - 1-3
    - 3-5
    - 5-7
    - 7-10
7. Have you participated in phishing training in the past?
    - Yes
    - No
    - Not sure
    - Prefer to not answer

Appendix C

Example of PAWS Participant Attention Span Test

1. Do you get distracted easily by conversations taking place around you?
    - Yes
    - Sometimes
    - No
2. Are you late for appointments often?
    - Yes
    - Sometimes
    - No
3. How difficult is it to concentrate on a friend talking to you while your favorite show is on?
    - Difficult
    - Moderately difficult
    - Not difficult
4. How difficult is it for you to concentrate on what you are reading without re-reading the page?
    - Difficult
    - Moderately difficult
    - Not difficult
5. Do you have a knack for noticing details?
    - Yes
    - Sometimes
    - No
6. Do you lose your patience easily?
    - Yes
    - Sometimes
    - No
7. Do you interrupt people when they are talking?
    - Yes
    - Sometimes
    - No

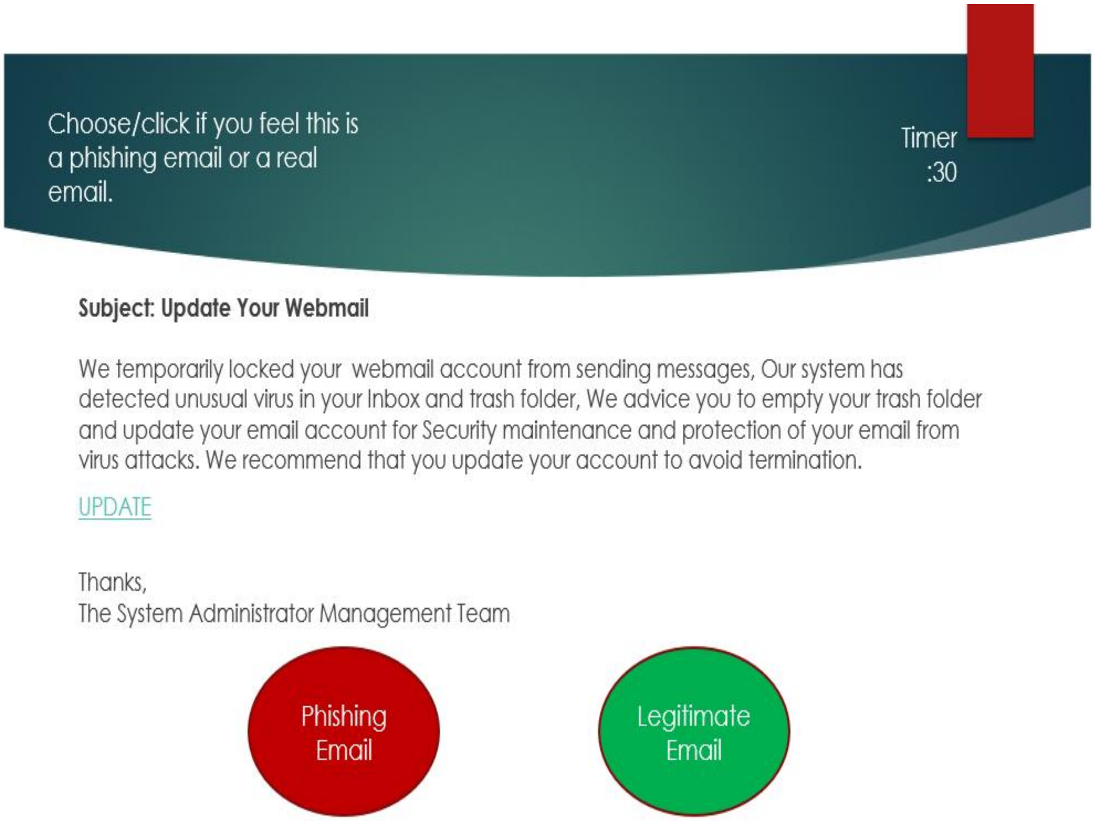
Appendix D

Example of PAWS Participant Post-PAWS Test

1. Did your mobile device shake at all during the PAWS test?
    - Yes
    - No
2. Did you hear any sounds during the PAWS test?
    - Yes
    - No
3. Did you experience any delays during the PAWS test (phone calls, notifications)?
    - Yes
    - No
4. Do you have any questions or concerns?
    - Yes
    - No
    - (Free-form text response)

Appendix E

Original PAWS Prototype (TEMPLATE): Example of Email Phishing Simulation Message without Alerts and Warnings



Choose/click if you feel this is a phishing email or a real email.

Subject: Update Your Webmail

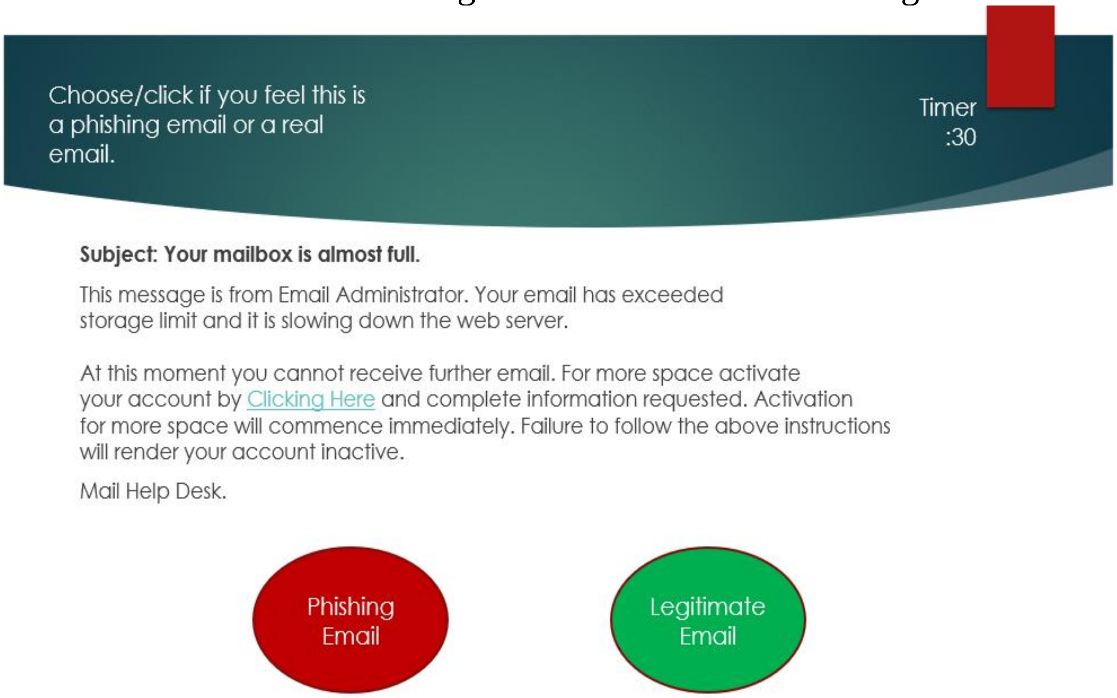
We temporarily locked your webmail account from sending messages, Our system has detected unusual virus in your Inbox and trash folder, We advice you to empty your trash folder and update your email account for Security maintenance and protection of your email from virus attacks. We recommend that you update your account to avoid termination.

UPDATE

Thanks,
The System Administrator Management Team

Appendix F

Original PAWS Prototype (TEMPLATE): Example of Email Phishing Simulation Message without Alerts and Warnings



Choose/click if you feel this is a phishing email or a real email.

Timer :30

Subject: Your mailbox is almost full.

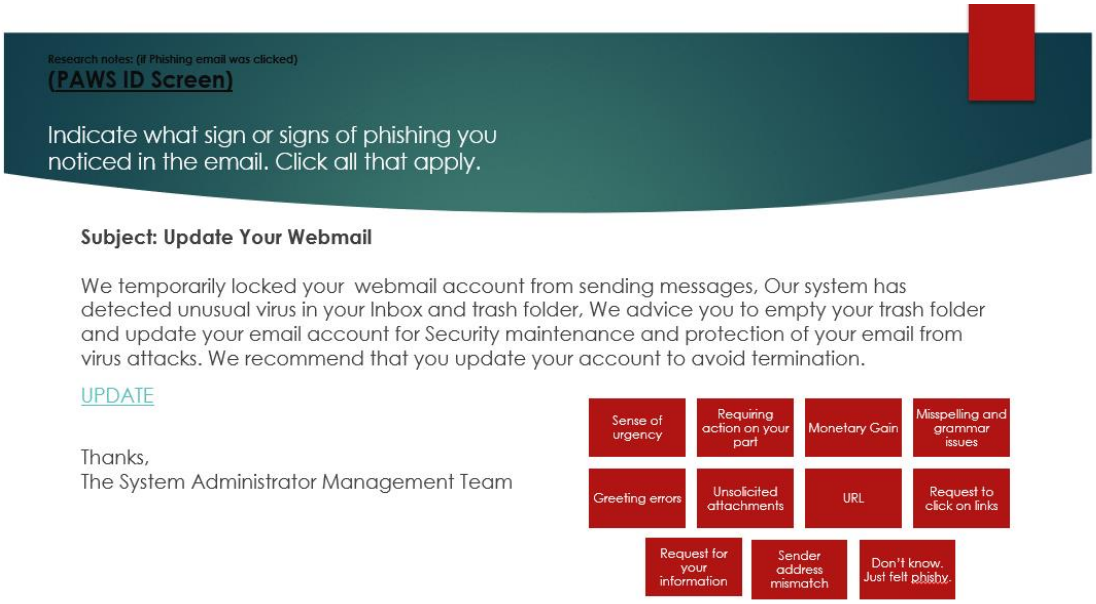
This message is from Email Administrator. Your email has exceeded storage limit and it is slowing down the web server.

At this moment you cannot receive further email. For more space activate your account by Clicking Here and complete information requested. Activation for more space will commence immediately. Failure to follow the above instructions will render your account inactive.

Mail Help Desk.

Appendix G

Original PAWS Prototype (TEMPLATE): Example PAWS ID Screen



Research notes: (if Phishing email was clicked)

(PAWS ID Screen)

Indicate what sign or signs of phishing you noticed in the email. Click all that apply.

Subject: Update Your Webmail

We temporarily locked your webmail account from sending messages, Our system has detected unusual virus in your Inbox and trash folder, We advice you to empty your trash folder and update your email account for Security maintenance and protection of your email from virus attacks. We recommend that you update your account to avoid termination.

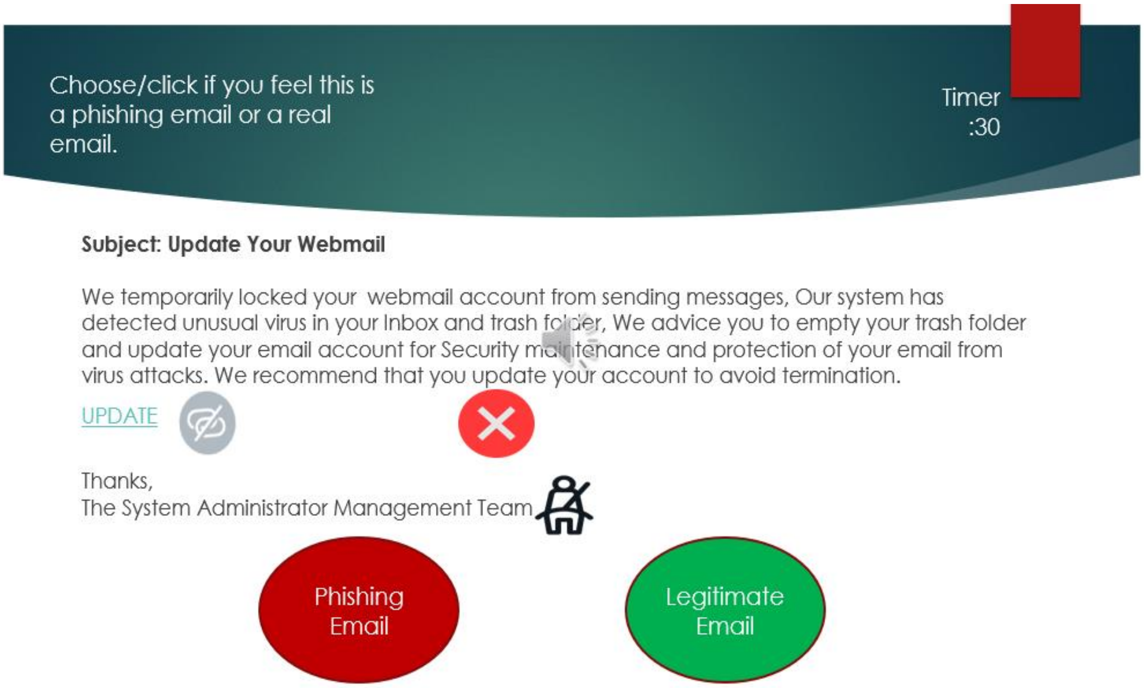
UPDATE

Thanks,
The System Administrator Management Team

Sense of urgency
Requiring action on your part
Monetary Gain
Misspelling and grammar issues
Greeting errors
Unsolicited attachments
URL
Request to click on links
Request for your information
Sender address mismatch
Don't know. Just felt phishy.

Appendix H

Original PAWS Prototype (TEMPLATE): Example of Email Phishing Simulation Message with Alerts and Warnings



Choose/click if you feel this is a phishing email or a real email.

Subject: Update Your Webmail

We temporarily locked your webmail account from sending messages, Our system has detected unusual virus in your Inbox and trash folder, We advice you to empty your trash folder and update your email account for Security maintenance and protection of your email from virus attacks. We recommend that you update your account to avoid termination.

UPDATE

Thanks,
The System Administrator Management Team

Appendix I

Example of SME Recruitment Message

SME Recruitment Letter
Dear Information Security Subject Matter Expert (SME),

I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy Cylab Projects (http://CyLab.nova.edu/). My research study is seeking to determine if audio, visual, and haptic alerting can reduce susceptibility of phishing emails.
The experiment that I am seeking assistance with is aimed to develop an application comprised of audio, visual, and haptic alerting. The study will be a mobile application that participants download to their mobile device and partake in a simulated phishing test. The test consists of various screens. The screens are designed to look like phishing emails. Various sounds, visual icons, and shaking will occur to assist the participant in noticing signs of phishing in emails.
I am requesting your help in a few areas of the PAWS design:

1. Your ranking of the Top Signs of Phishing in Emails
2. Your opinion regarding the most appropriate audio, visual, and haptic alerting elements to pair with signs of phishing in emails
3. Your opinion on the appropriate time it should take for a participant to notice signs of phishing in emails
4. Your opinion on the design of screens presented to the participant

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. As a token of appreciation for your security expert contribution to this research study you will receive a $10 Amazon digital gift card to your email address upon completing the survey instruments required to initiate this research study.

I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.
Please let me know if you would like to participate in my SME survey.

Best Regards,
Molly Cooper, PhD Candidate in Information Systems and Cybersecurity
Nova Southeastern University
Email: mc3300@mynsu.nova.edu

Appendix J

Example of Participant Recruitment Message

I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy Cylab Projects (http://CyLab.nova.edu/). I am seeking participants for my dissertation study.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time.

If you would like to participate, please go to:
Pawstest.com to download the PAWS Test App.
Following download, the test should not take more than 20 minutes.

Best Regards,
Molly Cooper, PhD Candidate in Information Systems and Cybersecurity
Nova Southeastern University
Email: mc3300@mynsu.nova.edu

Appendix K

Data Collection Detail

No	Research Question	Collection Instrument	Specific Data Collection Question or Screen	Analysis
RQ1	What are the SMEs' validated top signs of phishing in emails that are considered the most critical threats to users?	SME anonymous survey	Question: Please rank the signs of phishing from most important to least.	Likert Scale Ranking Highest percentage of choice among the SMEs will be chosen for the PAWS Mobile App.
RQ2	What SMEs' identified audio/visual /haptic alerts and warnings are most valid to pair with the top signs of phishing in emails?	SME anonymous survey	Question: A series of choice questions in the SME Survey: • The SMEs will indicate what their preferred audio sound for each sign of phishing in email. 1, 2, or 3. • The SMEs will indicate what their preferred visual icon is for each sign of phishing in email. 1, 2, or 3. • The SMEs will indicate what their preferred haptic alert timing is for each sign of phishing in email. 1, 2, or 3.	Likert Scale Ranking Highest percentage of choice among the SMEs will be chosen for the PAWS Mobile App.
RQ3	What are the SMEs' validated tasks for the measures of: (a) *ability to notice*, and (b) *time to notice* signs of phishing in emails?	SME anonymous survey	Question: (Ability) A choice of selections for screen presentation for PAWS Mobile App. (Ability) What determines a recipient's ability to notice signs of phishing in emails? Time • Age • Gender	Likert Scale Ranking Highest percentage of choice among the SMEs will be chosen for the PAWS Mobile App.

			• Prior experience with phishing training • Attention Span (Time) How long should it take a recipient of a phishing email to notice signs of phishing? • 25 seconds • 30 seconds • 35 seconds (Tasks)What are some tasks that determine a recipient’s ability to detect signs of phishing in emails? • Clicking Phishing • Not clicking anything on the screen. • Clicking signs of phishing noticed • Clicking Phishing within a certain amount of time?	
RQ4	What is the SMEs’ validated maximum *time for users’ ability to notice* signs of phishing in emails?	SME anonymous survey	Question: What is the maximum amount of time to lapse before it is determined the recipient did not notice signs of phishing in emails? Choice 1, 2, or 3.	Likert Scale Ranking Highest percentage of choice among the SMEs will be chosen for the PAWS Mobile App.
RQ5	What validation and testing procedures should be considered in order to deliver a mobile app phishing alert and warning prototype?	PAWS Prototype	Evidence of completed prototype using SME responses User testing observation	Successful testing of mobile app functionality. Qualitative and quantitative user testing analysis
RQ6a	Are there any statistically significant mean differences among users’	PAWS Mobile App	User selection of signs of phishing noticed on PAWS Mobile App	ANOVA Analysis of correct signs of phishing identification using PAWS email

	ability to notice signs of phishing in emails with or without PAWS?			screens without AVH compared to screens with AV, H, or AVH.
RQ6b	Are there any statistically significant mean differences among users' *time to notice* signs of phishing in emails with or without PAWS?	PAWS Mobile App	Time it takes user to click Legitimate or Phishing on PAWS Mobile App	ANOVA Analysis of recorded time to click Legitimate or Phishing buttons time using PAWS email screens without AVH compared to screens with AV, H, or AVH.
RQ6c	Are there any statistically significant mean differences among users' *ability to notice signs* of phishing in emails with or without PAWS?	PAWS Mobile App	Participant clicks of "what sign of phishing did you notice" screen	ANOVA Analysis of "what sign of phishing did you notice" screen without AVH compared to screens with AV, H, or AVH.
RQ7a	Are there any statistically significant mean differences among users' *ability to notice* signs of phishing in emails using PAWS based on: (a) age, (b) gender, (c) prior phishing training, and	PAWS Mobile App	Analysis of user responses to demographic questions and attention span questions against PAWS user responses to PAWS AVH compared to screens with AV, H, or AVH.	ANCOVA Analysis of user responses to demographic questions and attention span questions against PAWS user responses to PAWS AVH compared to screens with AV, H, or AVH.

	(d) attention span.			
RQ7b	Are there any statistically significant mean differences among users *time to notice* of phishing in emails using PAWS based on: (a) age, (b) gender, (c) prior phishing training, as well as (d) attention span.	PAWS Mobile App	Analysis of user responses to demographic questions and attention span questions against PAWS user responses to PAWS AVH compared to screens with AV, H, or AVH.	ANCOVA Analysis of user responses to demographic questions and attention span questions against PAWS user responses to PAWS AVH compared to screens with AV, H, or AVH.s.
RQ7c	Are there any statistically significant mean differences among users' *ability to notice signs* of phishing in emails with or without PAWS?	PAWS Mobile App	Participant clicks of "what sign of phishing did you notice" screen	ANCOVA Analysis of user responses to demographic questions and attention span questions against PAWS user responses to PAWS AVH compared to screens with AV, H, or AVH.s.

IRB Exemption Letter

NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Molly Cooper**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **March 10, 2020**

Re: **IRB #: 2020-120; Title, "An Empirical Assessment of Audio, Visual, and Haptic Alerts and Warnings to Mitigate Risk of Phishing Susceptibility in Emails"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a
manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of

informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, lifethreatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

References

AAA (2020). *Digest of Motor Laws.* https://drivinglaws.aaa.com/tag/seat-belts/

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

Abrams, L. (2018). Beware of extortion scams stating they have video of you on adult sites. https://www.bleepingcomputer.com/news/security/beware-of-extortion-scams-stating-they-have-video-of-you-on-adult-sites/

ACAS Program Final Report. (1998). https://one.nhtsa.gov/people/injury/research/pub/acas/Ch3-4.htm

Alert. (2019). In *Merriam-Webster's online dictionary* (11th ed.). http://www.m-w.com/dictionary/alert

Alexandar, M. (2016). Methods for understanding and reducing social engineering attacks. SANS institute, InfoSec Reading Room.

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.

Anderson, B. B., Jenkins, J. L., Vance, A., Kirwan, C. B., & Eargle, D. (2016). Your memory is working against you: How eye tracking and memory explain habituation to security warnings? *Decision Support Systems*, *92*, 3–13.

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). How polymorphic warnings reduce habituation in the brain. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2883–2892.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364–390.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, *33*(3), 713–743.

Anti-Fraud and Anti-Phishing Protection. (2019). https://campus.barracuda.com/product/essentials/doc/49054072/anti-fraud-and-anti-phishing-protection/

Anti-Phishing Working Group (2018). Phishing Activity Trends Report. 1st Quarter 2018. 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

Axon, L., Nurse, J. R. C., Goldsmith, M., & Creese, S. (2017). A formalised approach to designing sonification systems for network-security monitoring. *International Journal on Advances in Security*, *10*(1 & 2), 26–47. https://www.cs.ox.ac.uk/files/9105/2017-advsec-angc-preprint.pdf

Berls, B. (2016). Security Tip: Hover over links before you click. https://www.brucebnews.com/2016/08/security-tip-hover-over-links-before-you-click/

Caputo D., Pfleeger S., Freeman J., & Johnson M. (2014) Going spear phishing: Exploringembedded training and awareness. *IEEE Security & Privacy, 12 (1),* 28-38. http://doi.org: 10.1109/MSP.2013.106

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, *5*(2), 16-28. http://www.iiakm.org/ojakm/articles/2017/volume5_2/OJAKM_Volume5_2pp16-28.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

Canfield, C. I. (2018). Setting priorities in behavioral interventions: An application to reducing phishing risk. *Risk Analysis*, *38*(4), 826–838.

Can Gmail Detect Phishing Scams? (2018). DSL Reports.com. http://www.dslreports.com/faq/11024

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection based on structural properties. *NYS cyber security conference* (3)2-8.

Chang, D. (2002). Haptics: Gaming's new sensation. *Entertainment Computing, 35(8), 84-86.* https://webpages.uncc.edu/~jmconrad/ECGR6185-2008-01/notes/haptics%20gamings%20new%20sensation.pdf

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

Cohen, J. (1988). Statistical power analysis for the social sciences.

Cooper, S. (2014). Research Explains the Importance of Ranking In The Top 10. *Forbes.* https://www.forbes.com/sites/stevecooper/2014/01/29/research-explains-the-importance-of-ranking-in-the-top-10/#2de9864421f4

Continuous Wireless Pressure Monitoring and Mapping With Ultra-Small Passive Sensors For Health Monitoring and Critical Care. (2019). https://advanceseng.com/continuous-wireless-pressure-monitoring-mapping-ultra-small-passive-sensors-health-monitoring-critical-care/

Corsica Technologies. (2017). 15 Examples of phishing emails from 2016-2017. https://www.corsicatech.com/15-examples-of-phishing-emails-from-2016-2017/

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

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

Darwish, A., El Zarka, A., & Aloul, F. (2012, December). Towards understanding phishing victims' profile. In *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1-5). IEEE.

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

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

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

Evans, R., Burnett, D., Kendrick, O., Macrina, D., Snyder, S., Roy, J., & Stephens, B. (2009). Developing valid and reliable online survey instruments using commercial software programs. *Journal of Consumer Health on the Internet*, *13*(1), 42–52.

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

Findling, R. D., & Mayrhofer, R. (2015). Towards Device-to-user Authentication: Protecting Against Phishing Hardware by Ensuring Mobile Device Authenticity Using Vibration Patterns. *ACM International Conference on Mobile and Ubiquitous*

Multimedia (MUM), 131-135.

Freedman, M., Levi, S., Zador P., Lopdell J., & Bergeron E. (2007). *The effectiveness of enhanced seat belt reminder systems – Observational field data collection Methodology and findings*. (DOT HS 810 844). National Highway Traffic Safety Administration.

Frauenstein, E. D. (2019). An investigation into students responses to various phishing emails and other phishing-related behaviours. *17th Internaltional Information Security South Africa Conference*, 44–59. http://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

Greene, N. (2016). The meanings behind 15 symbols on your car's dashboard. *Mentalfloss.com* http://mentalfloss.com/article/63747/meanings-behind-these-15-symbols-your-cars-dashboard

Hacquebord, F. (2017). Pawn storm abuses open authentication in advanced social engineering attacks. *Trendmicro.com.* https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks/

Hale, M. L., Gamble, R. F., & Gamble, P. (2015). CyberPhishing: A game-based platform for phishing awareness testing. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015-March*(March), 5260–5269. https://doi.org/10.1109/HICSS.2015.670

Hegde, S. (2019, June 14). 11 easy ways to identify phishing emails- Marketers edition [web log post]. https://aritic.com/blog/aritic-pinpoint/identify-phishing-emails/

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

Hoggan, E., Raisamo, R., & Brewster, S. A. (2009). Mapping information to audio and tactile icons, 327. https://doi.org/10.1145/1647314.1647382

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

Isaac, M. S., & Schindler, R. M. (2014). The top-ten effect: Consumers' subjective categorization of ranked lists. *Journal of Consumer Research*, *40*(6), 1181-1202.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods*, *18*(1), 3–20.

Jagatic, T., N. Johnson, M. Jakobson & F. Menczer (2007) Social phishing. *Communications of the ACM* , 50(10), 94-100. http://doi.org/10.1145/1290958.129068

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. https://doi.org/10.1080/07421222.2017.1334499

Jensen, M. J., Tolbert, A. M., Wagner, J. R., Switzer, F. S., & Finn, J. W. (2011). A customizable automotive steering system with a haptic feedback control strategy for obstacle avoidance notification. *IEEE Transactions on Vehicular Technology*, *60*(9), 4208–4216. https://doi.org/10.1109/TVT.2011.2172472

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.

Krisher, T. (2016). Those chirps and chimes in your car have a science behind them. *The San Diego Union-Tribune.* https://www.sandiegouniontribune.com/sdut-those-chirps-and-chimes-in-your-car-have-science-2016sep06-story.html

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A real-world evaluation of anti-phishing training. *Symposium on Usable Privacy and Security (SOUPS), 1-12.*

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *APWG eCrime Researchers Summit*, 70–81.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31.

Levy, Y. (2006). Assessing the value of e-learning systems. IGI Global.

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

Libicki, M. C., Senty, D., & Pollak, J. (2014). H4cker5 wanted: An examination of the 25 cybersecurity labor market. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_R27R430.pdf

Lohr, T. (1974). *United States Patent No. 3,840,849* https://patentimages.storage.googleapis.com/b8/67/29/0bd5bb4784e4c4/US384084.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. http://doi.org/10.1016/j.ijinfomgt.2013.01.011

Mason, C. H., & Perreault Jr, W. D. (1991). Collinearity, power, and interpretation of multiple regression analysis. Journal of marketing research, 268-280.

McAlaney, J., & Benson, V. (2020). Cybersecurity as a social phenomenon. In *Cyber Influence and Cognitive Threats* (pp. 1-8). Academic Press.

McLeod, B. (2018). Mobile marketing statistics. https://www.bluecorona.com/blog/mobile-marketing-statistics

Mertler, C. A., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (Fifth edition.). Pyrczak Publishing.

Miranda, M. J. A. (2018). Enhancing Cybersecurity Awareness Training : A Comprehensive Phishing Exercise Approach, *14*(2), 5–10.

Molinaro, K., & Bolton, M. L. (2018). Evaluating the applicability of the double system lens model to the analysis of phishing email judgments. *Computers and Security*, *77*, 128–137. https://doi.org/10.1016/j.cose.2018.03.012

Mouton, F., Leenen, L. and 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. (2017). Majority of emails read on mobile devices. https://www.mediapost.com/publications/article/304735/majority-of-emails-read-on-mobile-devices.html

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

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

Oliveira H., Rocha H., Uang, H., Ellis D., Dommaraju S., Muradoglu M., Weir D., Soliman A.,Lin T., & Ebner N. (2017) *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/ 10.1145/10.1145/3025453.302583

Palarchio, J. (2016). Office 365 – Providing your users visual cues about email safety. https://blogs.perficient.com/2016/04/04/office-365providingyour-users-visual-cues-about-email-safety/

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/

Phishing Examples. (2019). https://www.knowbe4.com/phishing

Phishing Examples. (2018). http://www.phishing.org/phishing-examples

Phishing Scam: McGill Incoming Email on Hold. (2017). https://www.mcgill.ca/it/channels/news/phishing-scam-mcgill-incoming-mail-hold-274974

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

ProofPoint. (2019). PhishAlarm and PhishAlarm Analyzer features and benefits. https://www.proofpoint.com/us/products/phishalarm-email-reporting-analysis

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., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber- 6 attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, *8*(4), 24-34.

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

Real, D. (2013). Cyber threats: Trends in phishing and spear phishing -infographic. *Media and Tech Network*, 2.

Rubin, J., & Chisnell, D. (2008). Handbook of usability testing. How to plan, design, and conduct effective tests. Wiley.

Sauro, J., Lewis, J., (2012). Quantifying the User Experience, Practical statistics for user research. Elsevier Publishing.

Salkind, N. J., & Rainwater, T. (2003). *Exploring research*. Prentice Hall.

Sirull, E., (2017). How to avoid phishing scams [web log post]. https://www.experian.com/blogs/ask-experian/white-house-phishing-scam-a-warning-to-all-americans-heres-how-to-avoid-getting-hooked/

Scott, J., & Gray, R. (2008) A comparison of tactile, visual, and auditory warnings for rear-end collision prevention in simulated driving. *Human Factors, The Journal of the Human Factors and Ergonomics Society*. 50, 264-75. http://doi.org/10.1518/001872008X250674.

Sekaran, U., & Bougie, R. (2013). *Research methods for business*: *A skill-building 17 approach (6th Ed.)*. John Wiley & Sons Ltd.

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

Sheng, S., & Magnien, B. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *In Proceedings of SOUPS 2007*, 88–99. https://doi.org/10.1145/1280680.1280692

Should your new car have blind spot monitoring? (2019). https://www.cartelligent.com/blog/should-your-new-car-have-blind-spot-monitoring

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. *SpaceOps 2016 Conference*, 1–12. http://doi.org/10.2514/6.2016-2616

Sternlund, S., Strandroth, J., Rizzi, M., Lie, A., Tingvall, C., (2017). The effectiveness of lane departure warning systems — A reduction in real-world passenger car injury crashes passenger car injury crashes. *Traffic Injury Prevention*, *18*(2), 225–229. http://doi.org/10.1080/15389588.2016.1230672

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13(2),* 35 147-169.

TechTarget. (2014). *How to hone an effective vulnerability management program.* https://searchsecurity.techtarget.com/essentialguide/How-to-hone-an-effective-vulnerability-management-program

The anatomy of a phishing email. (2019). https://www.varonis.com/blog/spot-phishing-scam/

The inbox report: Consumer perceptions of email. (2018). https://www.fluentco.com/resources/the-inbox-report/

Tracey, M. W., & Richey, R. C. (2007). ID model construction and validation: A multiple 18 intelligences case. *Educational Technology, Research and Development*, *55*(4), 19, 369-390.

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 der Heiden, R. M. A., Janssen, C. P., Donker, S. F., & Merkx, C. L. (2018). Visual in-car warnings: How fast do drivers respond? *Transportation Research Part F: Traffic Psychology and Behaviour*. https://doi.org/10.1016/j.trf.2018.02.024

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.

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

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Warning. (2019). In *Merriam-Webster's online dictionary* (11th ed.). http://www.mw.com/dictionary/warning

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*. 1-12. http://doi.org/10.1145/3173574.3174066

Watch your inbox for fake postal service emails. (2017). https://www.spamstopshere.com/blog/watch-your-inbox-fake-postal-service-emails

What is phishing? (2019). *PhishTank.com.* https://www.phishtank.com/what_is_phishing.php

What motivates people to click: Phishing examples and techniques used. (2018). https://www.vircom.com/blog/phishing-examples-techniques-motivations/

Whigham, N. (2018). This is the device the tech industry wants to replace your smartphone with, but will we be ready? *News.com AU.*

Wombat Security. (2015). *The cost of phishing and value of employee training.* https://www.wombatsecurity.com/cost-of-phishing

Wombat Security. (2018). *The 2018 state of the phish.* https://www.wombatsecurity.com/state-of-the-phish

Wyro, B. (2019). Not today, scammer! Today's phishing attempt. http://blogs.mdaemon.com/index.php/tag/phishing/

Yates, D., & Harris A. (2015). Phishing attacks over time: A longitudinal study. *The 21st Americas Conference on Information Systems, Puerto Rico.*

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.