Heads-up! An alert and warning system for phishing emails

Molly Cooper
Information Security and Intelligence, Ferris State University, Big Rapids, Michigan, USA, and
Yair Levy, Ling Wang and Laurie Dringus
College of Computing and Engineering, Nova Southeastern University, Fort Lauderdale, Florida, USA

Received 9 March 2021
Revised 4 June 2021
16 June 2021
Accepted 17 June 2021

Abstract

Purpose – This study introduces the concept of audiovisual alerts and warnings as a way to reduce phishing susceptibility on mobile devices.

Design/methodology/approach – This study has three phases. The first phase included 32 subject matter experts that provided feedback toward a phishing alert and warning system. The second phase included development and a pilot study to validate a phishing alert and warning system prototype. The third phase included delivery of the Phishing Alert and Warning System (PAWS^{TM} mobile app) to 205 participants. This study designed, developed, as well as empirically tested the PAWS^{TM} mobile app that alerted and warned participants to the signs of phishing in emails on mobile devices.

Findings – The results of this study indicated audio alerts and visual warnings potentially lower phishing susceptibility in emails. Audiovisual warnings appeared to assist study participants in noticing phishing emails more easily and in less time than without audiovisual warnings.

Practical implications – This study's implications to mitigation of phishing emails are key, as it appears that alerts and warnings added to email applications may play a significant role in the reduction of phishing susceptibility.

Originality/value – This study extends the existing information security body of knowledge on phishing prevention and awareness by using audiovisual alerts and warnings to email recipients tested in real-life applications.

Keywords Organizational cybersecurity, Phishing susceptibility, Social engineering, Cyber threat mitigation, Human factor in cybersecurity, Cyber alerts and warnings

Paper type Research paper

1. Introduction

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 still fall for phishing in emails (Wash and 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 cost organizations an average of US$3.7m annually (Abass, 2018). Phishing and social engineering encompass approximately 93% of information security incidents (Anti-Phishing Working Group, 2018). Phishing emails continue to present a significant threat to both personal and corporate data loss, even after phishing awareness training (Allodi *et al.*, 2019; Almomani *et al.*, 2013;

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 1 No. 1, 2021
pp. 47-68
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-03-2021-0006

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.

The overarching research problem this study addresses 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; ElAassal *et al.*, 2020). Dakpa and Augustine (2017) define 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, a sense of urgency in the message, incorrect sender address and requests for personal information. Other signs of phishing in emails include an incorrect uniform resource locator (URL) in the email message, an unfamiliar or inaccurate logo for a company, unfamiliar fonts, incorrect language translations, inconsistent greetings 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).

Termed as “System 2 Thinking Mode” (S2), Kahneman (2011) describes an individual in a more aware state that he/she can utilize when making important decisions. Users have a tendency to be more deliberate with their choices in S2, as opposed to “System 1 Thinking Mode” (S1). S1 is more routine and not as deliberate or thoughtful (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” (Warning, 2019, p. 30). Alerts and warnings can be used to trigger S2 (Kahneman, 2011).

Alerts and warnings are 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 by 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 to prompt the driver to a potentially dangerous situation. 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. Social engineering and phishing are still problems that need 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. Subject matter expert (SME) opinion was gathered toward validation of the most important signs of phishing users should be warned about. This step included collecting SME opinions via survey to rank simulated phishing examples. SME feedback was also used to pair alerts and warnings with emails. SME 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 Phishing Alert and Warning System (PAWS) mobile application prototype. Thus, the main goal of this research study was to design, develop and empirically test the effectiveness (via the measures of (1) *ability to identify (ATI)*, (2) *ability to notice signs (ATNS) of phishing* and (3) *time to notice signs (TTNS) of phishing*) of an audio, visual and haptic warning system that alerts users to the signs of phishing in emails on mobile devices. Additionally, this study addressed the following three research questions:

RQ1. What validation and testing procedures should be considered to deliver a mobile app phishing alert and warning prototype?

RQ2. Does the use of PAWS aid users' *ATI, ATNS of and TTNS of* phishing in emails?

RQ3. What is the relationship of users' demographics to their *ATI, ATNS and TTNS of* phishing in emails with or without the use of PAWS?

2. Literature review

According to Hadnagy (2018), 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. 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. 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. 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).

There are several signs of phishing in emails (Wash and 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 and Cooper, 2018; Yates and Harris, 2015). 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. Many signs of phishing exist today and are still tricking recipients into clicking links and/or divulging personal information, despite user training methods.

2.1 User phishing training

User training toward 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 a 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 includes Kumaraguru *et al.* (2009), who tested an embedded antiphishing 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 antiphishing training appear to be less vulnerable to phishing attempts against them as compared to participants who did not receive antiphishing 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.

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, 2019).

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 they help 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 toward predicting user's susceptibility. Age appears to be a strong predictor of user susceptibility toward 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 toward demographic analysis toward 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.*, 2010). Other studies show conflicting information. For example, Sheng and Magnien (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 toward the ATNS of phishing in emails. More research in this specific area could benefit the field of demographics as it relates to phishing attempts and, thus, reduce the gap in the literature.

2.2 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 emergencies. 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 seatbelt reminder systems utilizing sound, icon and text increased front occupant seatbelt use.

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 the 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).

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's (2011) theory of thinking fast and slow related to 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.

2.3 User use of smartphones

Poushter and Stewart (2016) indicated that the volume of smartphone ownership and use has increased in Europe, the USA and emerging economies around the world. Their research concluded that at least 89% of Americans own a smartphone (Poushter and 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 past five years. McLeod (2018) indicated that consumers now spend more than 5 h a day on their smartphones.

2.4 Hypotheses

The following are the six hypotheses examined, where H1 to H3 address RQ2 and H4 to H6 addressed RQ3:

H1. Users' *ATI* phishing emails will differ with or without PAWS.

H2. Users' *ATNS of* phishing emails will differ with or without PAWS.

H3. Users' *TTNS of* phishing in emails will differ with or without PAWS.

H4. Users' *ATI phishing emails* will differ with or without PAWS *when controlling for differences in: (a) age, (b) gender, (c) experience with phishing training and (d) attention span.*

H5. Users' *ATNS of phishing emails* will differ with or without PAWS *when controlling for differences in: (a) age, (b) gender, (c) experience with phishing training and (d) attention span.*

H6. Users' *TTNS of phishing emails* will differ with or without PAWS *when controlling for differences in: (a) age, (b) gender, (c) experience with phishing training and (d) attention span.*

3. Methodology

This research methodology includes three phases. 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" in the context of developmental research, the PAWS prototype addressed a problem (Levy and Ellis, 2006). 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 a sequential exploratory research design (Creswell, 2017). According to Ivankova *et al.* (2006), a sequential exploratory research design is a valid methodology for developmental research, especially when conducting applied research. The research methodology used is illustrated in Figure 1. The first phase of this research study included collecting SME opinion on the initial list of simulated phishing examples, the study measures to be operationalized by the app, along with a set of audio/visual/haptic alerting should be paired with matching signs of phishing in emails for presentation in the PAWS mobile app prototype. The second phase 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 phase also included qualitative and quantitative data collection with the PAWS mobile app participants (Straub, 1989).

3.1 Phase I – measure design and expert panel validations

Phase I of this research study utilized initial qualitative data collection phrase using SMEs (Straub, 1989). A group of 32 experts validated the initial signs of phishing in emails in ranked order along with determining the tasks for measures of *(1) ATI phishing emails*, *(2) ATNS of phishing* and *(3) TTNS* of phishing in emails by the users. Then, the SMEs panel assisted in identifying the matched audio and visual warnings for each sign of phishing in emails that (in the SMEs opinion) reflected the severity of the sign of phishing.

3.2 Phase II – PAWS mobile app prototype development and pilot testing

Phase II included the development of the PAWS mobile app prototype. SME feedback on the top signs of phishing in emails was paired with the SME feedback on audio, visual and haptic signs that were used to alert the user of phishing. 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," as illustrated in Figure 2. The data collected from this screen were analyzed to determine *ATNS* of phishing in emails by the participants. Pilot testing of the prototype was conducted in this phase. Testing the functionality of applications is an important part of application design (Rubin and Chisnell, 2008). The pilot testing included five participants, and data were verified to ensure proper capture of all data points was considered and recorded. Observations, scoring and manual measurements of time were conducted to ensure the assessment by the PAWS mobile app prototype is accurate.

3.3 Phase III – experiments and data collection

Phase III encompassed the main research study with 205 participants. The participants answered a short demographic survey, and then completed an attention span test.

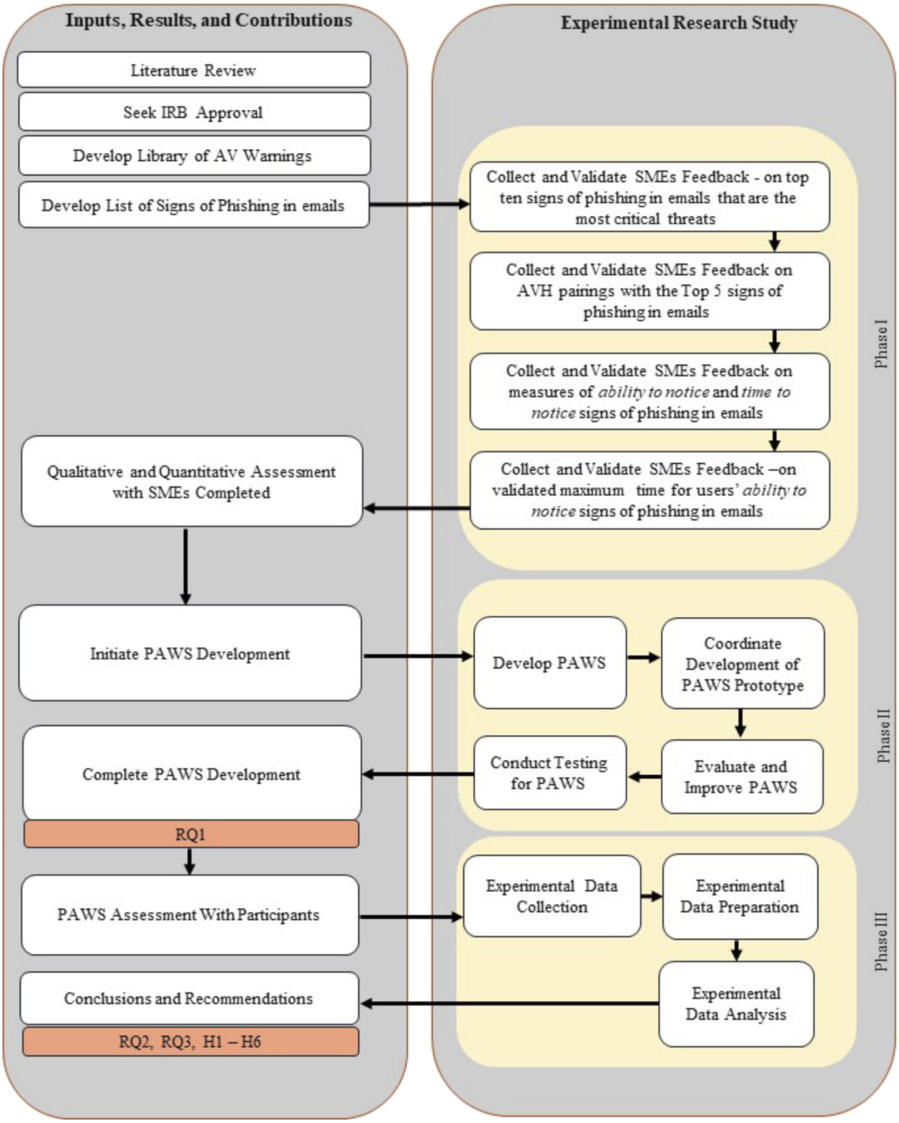
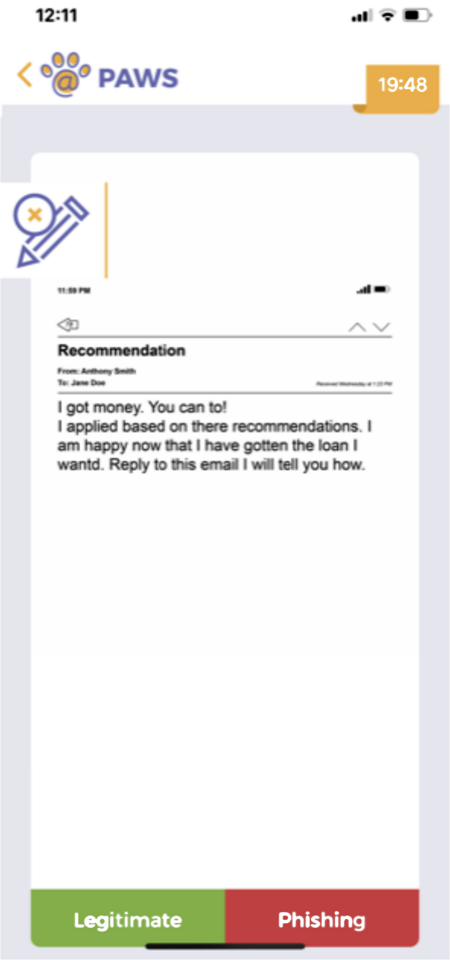

Inputs, Results, and Contributions
Literature Review
Seek IRB Approval
Develop Library of AV Warnings
Develop List of Signs of Phishing in emails
Qualitative and Quantitative Assessment with SMEs Completed
Initiate PAWS Development
Complete PAWS Development
RQ1
PAWS Assessment With Participants
Conclusions and Recommendations
RQ2, RQ3, H1 – H6
Experimental Research Study
Collect and Validate SMEs Feedback - on top ten signs of phishing in emails that are the most critical threats
Collect and Validate SMEs Feedback on AVH pairings with the Top 5 signs of phishing in emails
Collect and Validate SMEs Feedback on measures of ability to notice and time to notice signs of phishing in emails
Collect and Validate SMEs Feedback –on validated maximum time for users' ability to notice signs of phishing in emails
Phase I
Develop PAWS
Coordinate Development of PAWS Prototype
Conduct Testing for PAWS
Evaluate and Improve PAWS
Phase II
Experimental Data Collection
Experimental Data Preparation
Experimental Data Analysis
Phase III

Figure 1.
Research methodology flowchart

The participants then entered the PAWS mobile app. Each participant saw several simulated emails verified from the Phase 1 SME survey as the top signs of phishing in emails. Alerts and warnings accompanied the simulated emails as decided by the SMEs in Phase I. Demographic questions for each participant were asked in the PAWS mobile app. 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, there should be no direct relationship between the individuals who



11:59 PM

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.

Figure 2.
PAWS mobile app example

participated. 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 six attention span questions. Answers were ranked on a five-point scale with values from quite often to almost never. Participants were assigned a unique number to ensure confidentiality. Each number was used to uniquely identify participants and PAWS mobile app data, however, without a direct relationship between the individuals who participated.

The PAWS mobile app was delivered to the participants in two process flows, totaling four experiment groups. Process 1 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. Process 2 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 s 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.

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 email examples were designed, utilizing the literature review to validate signs of phishing contained in the email example. All designs were of varying length and randomized per experiment group. Randomization of experiment groups (AV, H and AVH) was addressed by randomizing alert and warning examples, as shown in Table 1. 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 1, 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 1.

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) *A TNS* of phishing in emails. Pilot testing of the PAWS mobile app was completed prior to PAWS participant study with five testers to ensure all measures were valid and any data or performance issues were resolved.

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

Table 1.
PAWS experimental groups and randomization table

Multiple specific testing was completed to ensure the PAWS mobile app 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.

4. Findings

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 not to fall for phishing emails (Abass, 2018). PAWS mobile app development and testing add to the body of research in this area.

4.1 Findings – Phase I

A group of 32 cybersecurity SMEs participated in the study, the majority of them (18) with ten years or more practicing cybersecurity. The SME pairing of visual icons for the top signs of phishing in emails (Figure 3) 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 a 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 3 illustrates the outcome of Phase I, final icons paired with the top five signs of phishing in emails that were used in the PAWS mobile app.

SMEs ranking of the audio and haptic pairings resulted in the consensus that the audio alerts would be most effective as a female voiceover 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

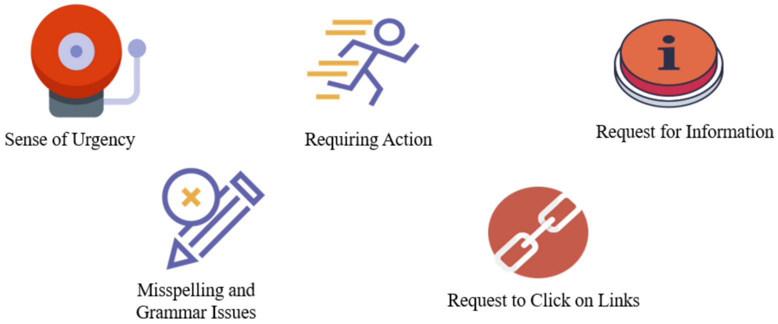


Figure 3.
SME visual icon matching to top signs of phishing in emails

recipient seeing the simulated email on the mobile screen, with SME consensus at 38.71%. Other haptic presentation choices included 1 s after the simulated email appears (29.03%), 2 s after the simulated email appears (16.13%) and 3 s after the simulated email appears (16.13%). Female voiceover audible warnings, as well as haptic/vibration upon participants viewing simulated emails were used for the PAWS mobile app. The results from this phase indicated strong support for RQ1 in the validation and testing procedures, which were validated by the 32 SMEs to deliver a mobile app prototype for phishing alert and warning.

4.2 Findings – Phase II

Phase II included the development of PAWS, the mobile prototype and study application. SME consensus on audio, visual, haptic feedback, top signs of phishing, ATNS of phishing measures, time to notice measures, ATNS of phishing in email measures, and order of appearance of simulated emails were used. Development of the application involved (as previously shown) randomization of emails by alert group as well as email length while coding and programming the PAWS mobile app prototype. All participants saw the same randomized order of PAWS mobile app 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 and 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.

4.3 Findings – Phase III

Data collection occurred from June 1, 2020 through June 24, 2020. 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 and Vannatta, 2013) determined one multivariate outlier, with a value of 130.78. This outlier was removed from further analysis. The final sample size for this study was 205. The 205 participants included several demographic areas. 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 who chose not to answer the gender demographic question. Experience with phishing training was also asked in the demographic question set. Participants who 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 not to answer the question. To answer if any statistically significant mean differences exist among users' *ATI, ATNS* and *TTNS* of 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 H1 – ATI [$F(3,816) = 7.53, p < 0.001$], H2 – TTNS [$F(3,816) = 6.39,$

$p < 0.001$], and H3 – ATNS [$F(3,816) = 115.7$, $p < 0.001$]. The p-values of the F-test were less than 0.05 level of significance. The results are shown in Table 2 and Figures 4–6.

This section represents the results of descriptive statistics between groups for ATI, ATNS and TTNS among all 205 participants for Group 1 (NAVH), Group 2 (AV), Group 3 (H) and Group 4 (AVH). Based on mean comparisons 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. Group 2 (AV) was also the best performing group for *time to notice* and *ATNS* among all of the PAWS groups.

Statistically significant mean differences among users' *ATI, TTNS* and *ATNS of* 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 corresponding to H4–H6. The results indicated there were significant differences among age groups (18–20, 21–29, 30–39, 40–49, 50–59, 60+) for ATI (ability to identify) – H4a – [$F(5,814) = 7.72$, $p < 0.000$], significant differences for ATNS (ability to notice signs) – H5a – [$F(5,814) = 2.20$, $p = 0.052$] and significant differences among age groups for TTNS (time to notice signs) – H6a – [$F(5,814) = 8.10 = 2.20$, $p = 0.052$]. When it comes to gender, the results indicated there were no significant differences among gender groups (female, male and

Table 2.
ANOVA results of difference in PAWS groups ($N = 205$)

Measure	Sum of squares	df	Mean square	*F*	Sig.
ATI	11.72	3	3.90	7.53	*0.000****
ATNS	456.51	3	1.31	115.7	*0.000****
TTNS	59,064.31	3	19,688.10	6.39	*0.000****

Note(s): ***$p < 0.001$

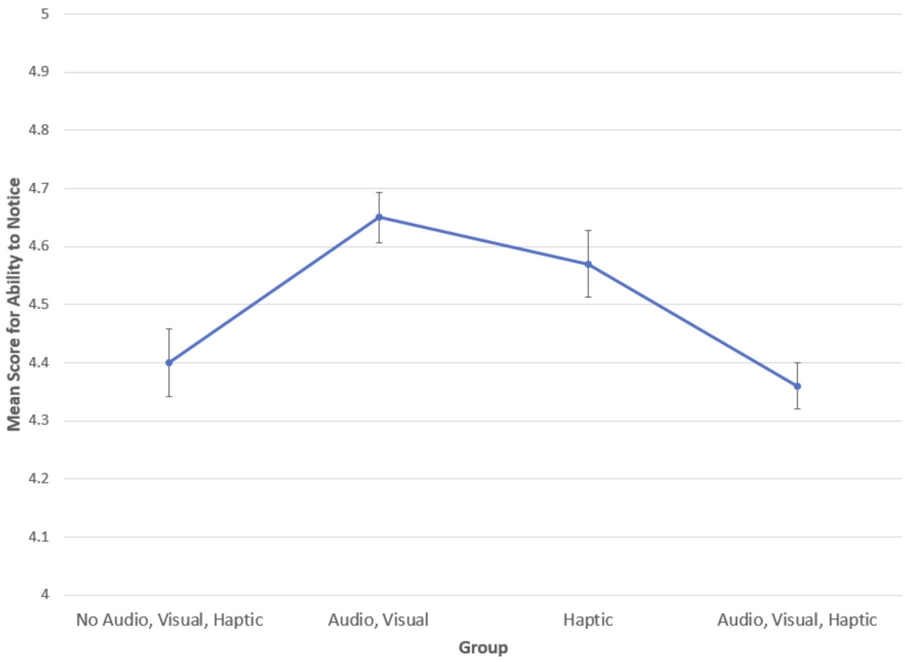


Figure 4.
Mean score for ATI phishing emails by NAVH, AV, H and AVH

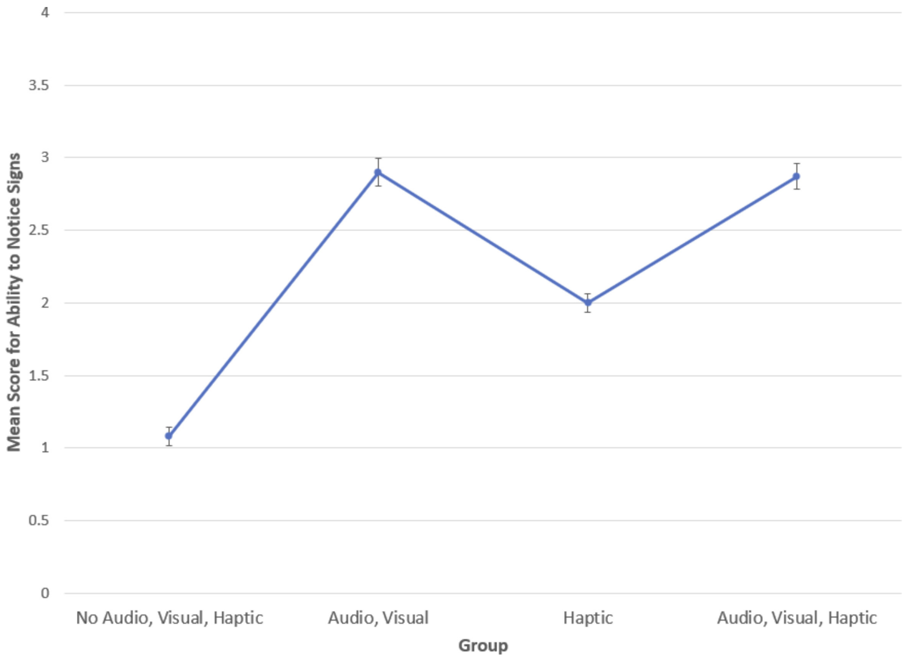


Figure 5.
Mean score for ATNS of phishing in emails by NAVH, AV, H and AVH

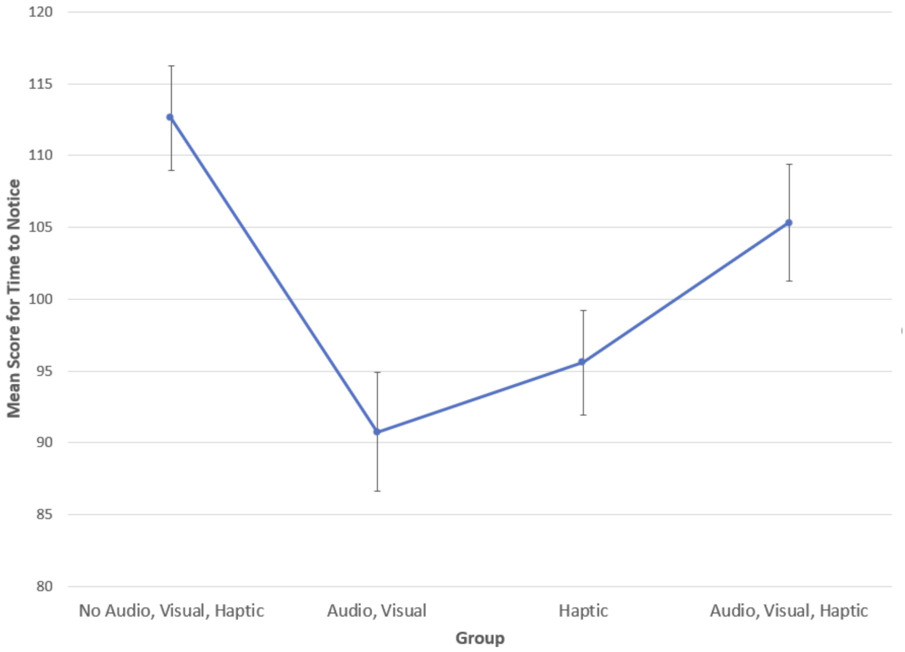


Figure 6.
Mean score for TTNS of phishing in emails by NAVH, AV, H and AVH

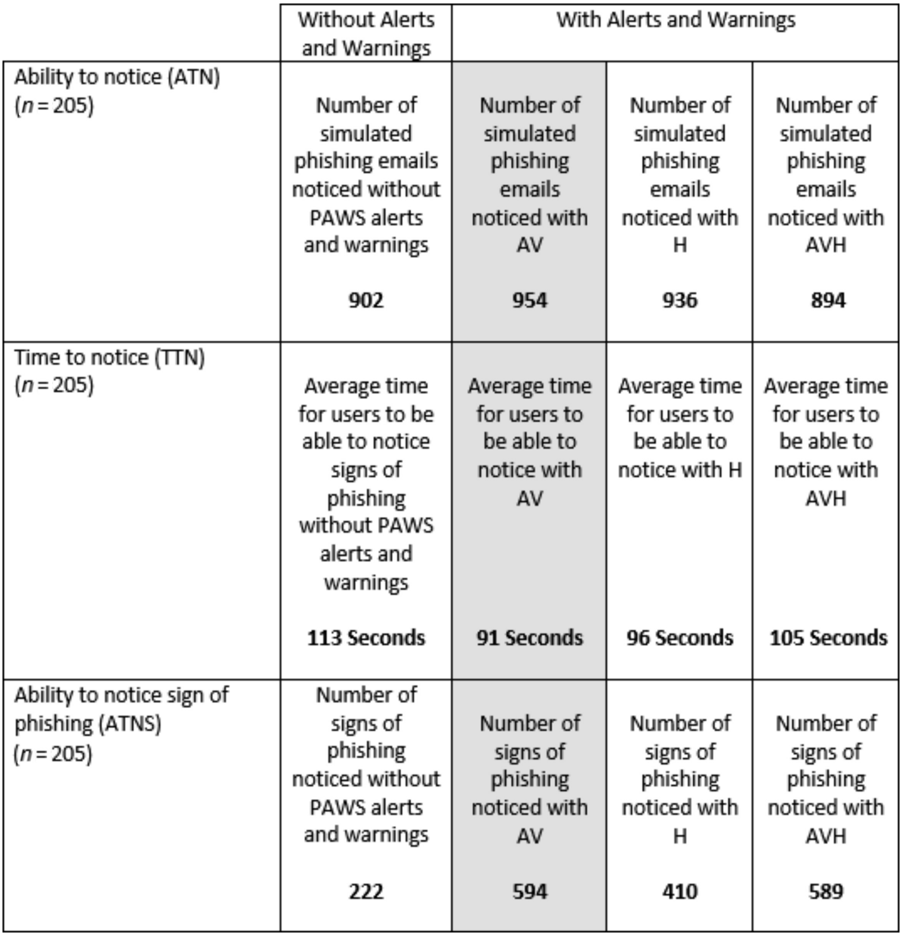
choose to not answer) for ATI (*ability to identify*) – H4b [F(2,817) = 1.957, p = 0.142], no significant differences for ATNS (*ability to notice signs*) by gender – H5b – [F(2,817) = 1.597, p = 0.203] and significant differences were shown for TTNS (*time to notice signs*) – H6b – [F(2,817) = 3.970, p = 0.019]. Among phishing training groups (prior training, no prior training, not sure if training was received and choose to not answer), the results indicated there were significant differences for ATI (*ability to identify*) – H4c – [F(3,816) = 8.319, p < 0.001], significant differences for ATNS (*ability to notice signs*) – H5c – [F(3,816) = 4.925, p = 0.002] and no significant differences for TTNS *(time to notice signs*), H6c – [F(3,816) = 1.517, p = 0.209]. 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 in 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. 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 and 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 *ATNS* of phishing in emails (clicking what sign of phishing the participant saw) for each of the 20 simulated email screens. Figure 7 illustrates the indication that the AV (audio and visual alerting) group was the best-performing group of the PAWS groups for *ability to notice*, *time to notice* and *ATNS* of phishing in emails. The number of simulated email 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 s, with NAVH averaging 113 s, H averaging 96 s and AVH at 105 s. ATNS of phishing in emails were 594 for the AV group, 222 for NAVH, 410 for H and 589 for AVH groups.

When it comes to the attention span scores among the participants, the results showed there were significant differences for ATI (*ability to identify*) – H4d – [F(19,800) = 2.038, p < 0.006], no significant differences for ATNS (*ability to notice signs*) – H5d – [F(19,800) = 0.714, p = 0.807] and significant differences for TTNS (*time to notice signs*) – H4–H6d – [F(19,800) = 3.456, p < 0.0001].

Table 3 itemizes each PAWS-simulated email screen by correct clicks by the participant, number of TTNS below the SME agreed time of 25 s for maximum time to notice phishing in emails and correct clicks by the participant toward identification of signs of phishing in the specified simulated email screen.

4.4 Summary of findings

Answers from the Phase I – SME survey validated the constructs set by our study to measure the effectiveness (via the measures of (a) *ATI*, (b) *ATNS of phishing* and (c) *TTNS of phishing*) for the PAWS mobile app in using audio, visual and haptic warning to alert users to the signs of phishing in emails on mobile devices. Phase II developed, designed and tested the PAWS mobile app prototype. Phase III included the PAWS mobile app study with a group of 205 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. The findings from the SMEs survey also included visual icon matching for each sign of phishing, and a voiceover 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 by combining



	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**

Figure 7.
Sums and averages for ATI, TTNS and ATNS for all participants

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 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 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

Table 3.
Sums and averages for PAWS-simulated email screens by participant ($N = 205$)

PAWS screen	Version	Group	ATI clicks	TTNS ≤ 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

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.

5. Conclusion

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 s 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. 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.

5.1 Study limitations

Some limitations of the study indicated some 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 voiceover 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 voiceover to be a “novel” and “unexpected” alert or warning. Analyzing 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 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. There are potential issues of confusion regarding 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.

5.2 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. 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 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 ATNS 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.

6. Discussion

The focus of the experiments was to assess if alerting for email will work the same way seatbelt alerts work for drivers. The premise of the relationship within the auto industry to create the association of the audio sound of the seatbelt to the realization of the driver that the seatbelt needs to be "clicked" took years to develop in the drivers' mindset. Our goal of this research is to begin that association for individuals reading email and being alerted that there is a potential malicious aspect in the email.

6.1 Recommendations and future research

A deeper analysis of separated audio, visual and 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, personal security experience, security self-efficacy and other potential phishing email noticing behaviors in mind. Additional emails for PAWS should also be studied, including legitimate email examples to consider false alerts. Email filtering with alerts and warnings could be helpful toward 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, and different structure and message tones that may alter effectiveness. 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 who 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.

6.2 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 voiceover combined with a visual alert is the best combination of alert and warning. Overall, this study developed a phishing alert and warning system utilizing constructs determined by SMEs. 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.

References

Aaron, G. (2010), "The state of phishing", *Computer Fraud and Security*, Vol. 2010 No. 6, pp. 5-8.

Abass, I. (2018), "Social engineering threat and defense: a literature survey", *Journal of Information Security*, Vol. 9 No. 4, pp. 257-264, doi: 10.4236/jis.2018.94018 (accessed 5 March 2021).

Allodi, L., Chotza, T., Panina, E. and Zannone, N. (2019), "The need for new antiphishing measures against spear-phishing attacks", *IEEE Security and Privacy*, Vol. 18 No. 2, pp. 23-34.

Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A. and Almomani, E. (2013), "A survey of phishing email filtering techniques", *IEEE Communications Surveys and Tutorials*, Vol. 15 No. 4, pp. 2070-2090.

Anti-Phishing Working Group (2018), "Phishing activity trends report", 1st Quarter 2018, available at: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf (accessed 5 March 2021).

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

Caputo, D., Pfleeger, S., Freeman, J. and Johnson, M. (2014), “Going spear phishing: exploring embedded training and awareness”, *IEEE Security and Privacy*, Vol. 12 No. 1, pp. 28-38, available at: https://ieeexplore.ieee.org/document/6585241 (accessed 5 March 2021).

Carlton, M., Levy, Y. and Ramim, M.M. (2018), “Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool”, *Online Journal of Applied Knowledge Management*, Vol. 6 No. 1, pp. 107-118, doi: 10.36965/OJAKM.2018.6(1)107-118 (accessed 5 March 2021).

Chandrasekaran, M., Narayanan, K. and Upadhyaya, S. (2006), “Phishing email detection based on structural properties”, *NYS Cyber Security Conference* No. 3, pp. 2-8.

Clement, J. (2018), “Email usage in the United States – statistics and facts”, *Statista.com*, available at: https://www.statista.com/topics/4295/e-mail-usage-in-the-united-states (accessed 5 March 2021).

Creswell, J.W. and Creswell, J.D. (2017), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Los Angeles, CA.

Dakpa, T. and Augustine, P. (2017), “Study of phishing attacks and preventions”, *International Journal of Computer Applications*, Vol. 163 No. 2, pp. 5-8.

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

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

Dublin, J. (2019), “Email filtering tools and techniques”, available at: https://searchsecurity.techtarget.com/tip/Email-filtering-tools-and-techniques (accessed 5 March 2021).

El Aassal, A., Baki, S., Das, A. and Verma, R.M. (2020), “An in-depth benchmarking and evaluation of phishing detection research for security needs”, *IEEE Access*, Vol. 8, pp. 22170-22192.

Findling, R.D. and 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)*, pp. 131-135.

Greene, N. (2016), “The meanings behind 15 symbols on your car’s dashboard”, *Mentalfloss.com*, available at: http://mentalfloss.com/article/63747/meanings-behind-these-15-symbols-your-cars-dashboard (accessed 5 March 2021).

Hadnagy, C. (2018), *Social Engineering: The Science of Human Hacking*, John Wiley & Sons.

Hoggan, E., Raisamo, R. and Brewster, S.A. (2009), “Mapping information to audio and tactile icons”, Vol. 327, doi: 10.1145/1647314.1647382 (accessed 5 March 2021).

Hong, J. (2012), “The state of phishing attacks”, *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81.

Ivankova, N.V., Creswell, J.W. and Stick, S.L. (2006), “Using mixed-methods sequential explanatory design: from theory to practice”, *Field Methods*, Vol. 18 No. 1, pp. 3-20.

Jagatic, T., Johnson, N., Jakobson, M. and Menczer, F. (2007), “Social phishing”, *Communications of the ACM*, Vol. 50 No. 10, pp. 94-100, doi: 10.1145/1290958.129068.

Kahneman, D. (2011), *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York, NY.

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

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L.F. and Hong, J. (2007), “Getting users to pay attention to antiphishing education: evaluation of retention and transfer”, *APWG eCrime Researchers Summit*, pp. 70-81.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T. (2009), “School of Phish: a real-world evaluation of antiphishing training”, *Symposium on Useable Privacy and Security (SOUPS)*, pp. 1-12.

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

Lohr, T. (1974), "United States patent No. 3,840,849", available at: https://patentimages.storage.googleapis.com/b8/67/29/0bd5bb4784e4c4/US384084.pdf.

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

Mertler, C.A. and Vannatta, R.A. (2013), *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*, 5th ed., Pyrczak Publishing, Los Angeles, CA.

Miranda, M.J.A. (2018), "Enhancing cybersecurity awareness Training ", *A Comprehensive Phishing Exercise Approach*, Vol. 14 No. 2, pp. 5-10.

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

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

Nelson, J. (2017), "Majority of emails read on mobile devices", available at: https://www.mediapost.com/publications/article/304735/majority-of-emails-read-on-mobile-devices.html.

Oliveira, H., Rocha, H., Uang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T. and Ebner, N. (2017), "Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. doi: 10.1145/10.1145/3025453.302583.

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

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

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

Poushter, J. and Stewart, R. (2016), "MobilePhone", Vol. 22, available at: www.pewresearch.org.

Rubin, J. and Chisnell, D. (2008), *Handbook of Usability Testing. How to Plan, Design, and Conduct Effective Tests*, Wiley, Hoboken, NJ.

Sauro, J. and Lewis, J. (2012), *Quantifying the User Experience, Practical Statistics for User Research*, Elsevier Publishing, Cambridge, MA.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and 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, pp. 373-382, doi: 10.1145/1753326.1753383 (accessed 5 March 2021).

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

Straub, D.W. (1989), "Validating instruments in MIS research", *MIS Quarterly*, Vol. 13 No. 2, 35, pp. 147-169.

van Rijn (2019), "The ultimate mobile email stats overview", available at: https://www.emailmonday.com/mobile-email-usage-statistics/ (accessed 5 March 2021).

Warning (2019), *Merriam-Webster's Online Dictionary*, 11th ed., available at: http://www.mw.com/dictionary/warning.

Wash, R. and 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*, pp. 1-12, doi: 10.1145/3173574.3174066 (accessed 5 March 2021).

Yates, D. and 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. and Fei-Yue Wang, G. (2004), "Toward intelligent driver-assistance and safety warning systems", *Intelligent Systems*, Vol. 19 No. 2, pp. 8-11.

Further reading

Alert (2019), *In Merriam-Webster's Online Dictionary*, 11th ed., Springfield, MA, available at: http://www.m-w.com/dictionary/alert.

Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D. and Jenkins, J.L. (2016a), "How users perceive and respond to security messages: a NeuroIS research agenda and empirical study", *European Journal of Information Systems*, Vol. 25 No. 4, pp. 364-390.

Anderson, B.B., Vance, A., Kirwan, C.B., Jenkins, J.L. and Eargle, D. (2016b), "From warning to wallpaper: why the brain habituates to security warnings and what can be done about it", *Journal of Management Information Systems*, Vol. 33 No. 3, pp. 713-743.

Carlton, M. and Levy, Y. (2017), "Cybersecurity skills: the cornerstone of advanced persistent threats (APTs) mitigation", *Online Journal of Applied Knowledge Management*, Vol. 5 No. 2, pp. 16-28, available at: http://www.iiakm.org/ojakm/articles/2017/volume5_2/OJAKM_Volume5_2, pp16-28.pdf (accessed 5 March 2021).

Event Alert System (2019), available at: https://www.rrca.org/resources/event-directors/guidelines-for-safe-events/eas (accessed 5 March 2021).

Hernandez, W., Levy, Y. and Ramim, M. (2016), "An empirical assessment of employee cyberslacking in the public sector: the social engineering threat", *Online Journal of Applied Knowledge Management*, Vol. 4 No. 2, pp. 93-109, doi: 10.36965/OJAKM.2016.4(2)93-109 (accessed 5 March 2021).

Jensen, M.J., Tolbert, A.M., Wagner, J.R., Switzer, F.S. and Finn, J.W. (2011), "A customizable automotive steering system with a haptic feedback control strategy for obstacle avoidance notification", *IEEE Transactions on Vehicular Technology*, Vol. 60 No. 9, pp. 4208-4216, doi: 10.1109/TVT.2011.2172472.

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

Kane, S. (2012), "Pay attention to that buzz below: Cadillac's new safety alert seat", available at: 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. and Sheikh, A. (2011), "Clinical decision support systems could be modified to reduce 'alert fatigue' while still minimizing the risk of litigation", *Health Affairs*, Vol. 30 No. 12, pp. 2310-2317.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J. (2010), "Teaching Johnny not to fall for phish", *ACM Transactions on Internet Technology*, Vol. 10 No. 2, pp. 1-31.

Levy, Y. (2006), *Assessing the Value of e-Learning Systems*, IGI Global, Hershey, PA.

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

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

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

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

Ramim, M. and 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*, Vol. 8 No. 4, pp. 24-34.

Ramim, M. and Lichvar, B. (2014), "Eliciting expert panel perspective on effective collaboration in system development projects", *Online Journal of Applied Knowledge Management*, Vol. 2 No. 1, pp. 122-126, available at: http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp122-136.pdf (accessed 5 March 2021).

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

Corresponding author
Yair Levy can be contacted at: levyy@nova.edu