Efficacy of Embedded Phishing Training

by

Brandon Geitman

An assignment submitted in partial fulfillment
of the requirements for the degree of
Masters of Science
in
Information Security and Intelligence

Graduate Program - College of Business
Ferris State University
ISIN 799 – Master's Thesis
Summer 2018
Professor: James Furstenberg.
Due: December 18, 2018

DEDICATION

This is dedicated to my father, Greg Geitman. There are very few people in this lifetime whom I will share so many great memories with. You have had such a positive impact on my life. You shaped me into the man I am today. Without your advice and unconditional support, I would not be where I am today. I love you Dad.

ACKNOWLEDGEMENTS

I would like to thank my mother, Sherrie Geitman, who has always supported any decisions I have made and pushed me to try my hardest. Secondly, I would like to thank all professors in the Information Security Intelligence program at Ferris State University. Their constant efforts to help students and improve the curriculum made for a great learning experience. Lastly, I would like to thank Professor Furstenberg for guiding me along my thesis process. His suggestions and help allowed me to complete this study.

Table of Contents

List of Tables

List of Figures

Abstract

Embedded phishing training is a training methodology where users are sent simulated phishing emails to test users' vulnerability to phishing attacks. Research studies seeking to evaluate the effectiveness of embedded phishing training at educating end-users have conflicting results. In this study, a phishing campaign with embedded phishing exercises is conducted to determine the effectiveness of embedded phishing exercises. The phishing campaign involved 924 participants from a single financial institution and utilized 1,848 embedded phishing emails. The first part of this study focuses on previous studies that have attempted to measure the efficacy of embedded phishing training at educating end-users. Based on previous studies, a methodology is developed to measure efficacy of the embedded phishing training. The first and last round of the phishing campaign is utilized to perform an analysis of the effectiveness of the embedded phishing training. Based on the results of the phishing campaign, a hypothesis can be made that the embedded phishing training was effective at educating end-users and reduced participants susceptibility to phishing attacks. Suggestions are given to identify how the design of embedded phishing training can be improved

Chapter 1: Introduction

Phishing attacks are one of the most dangerous information security threats present in the world today, with losses toping $5.9 billion in 2013 (Alam & El-Khatib, 2016). Phishing is a type of attack that communicates socially engineered messages to humans via electronic communication in order to persuade them to perform certain actions for the attacker's benefit (Cui, Jourdan, Couturier, & Onut, 2017). Phishing attacks aim to steal confidential information such as username, password, and online banking details (Arachchilage & Love, 2014). At the organizational level, information security is not solely responsible for specific personnel, but it is necessary to form an organizational culture that emphasizes the importance of information security and change of awareness (Sung & Kang, 2017).

Phishing awareness training is a crucial part of any information security program either at the personal or organizational level (Al-Daeef, Basir, & Saudi, 2017). The most common technique of changing end-user security behaviors is security education and training (Wash & Cooper, 2018). Phishing training delivery methods are varied and can include; web-based training materials, contextual training, or embedded training (Arachchilage & Love, 2014). Web-based training materials can include; email broadcasting, blogging, animation, multimedia, or any online media (Abawajy, 2014). Contextual training is a type of presentation done by security experts used to raise phishing awareness (Abawajy, 2014). Contextual training typically has a top-down approach, aimed at having an impact on the individual level through an expert (Abawajy, 2014). An effective education and training experiment should help trainees to learn new knowledge, practice learned knowledge for a long time period, and apply this knowledge into other related activities (Al-Daeef et al., 2017). The benefit of embedded training over other traditional training methods is that, it can help trainees to retain acquired knowledge for a long time and transfer this knowledge into other related fields (Al-Daeef et al., 2017).

Embedded training is a methodology in which training materials are integrated into the primary tasks that users perform in their day-to-day lives (Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor, & Hong, 2007). Embedded training is different than conventional training methods as it provides training at the time of the user making an error (Wash & Cooper, 2018). A key factor in embedded training is timing of the training, it provides users real time feedback that can be perused at the user's leisure (Wash & Cooper, 2018). An example of embedded training is running a phishing campaign; where purposely crafted fictious emails are sent out to unsuspecting end users.

Organizations conduct embedded phishing exercises as a security training strategy to promote security awareness in the defense of phishing threats (Siadati, Palka, Siegel, & Mccoy, 2017). Siadati et al. (2017), research stated that embedded phishing exercises followed by phishing awareness training reduces an employee's susceptibility to legitimate phishing attacks. This research investigated the efficacy of embedded phishing training at educating end-users.

Embedded training is a method where users are sent simulated phishing emails to test users' vulnerability to phishing attacks (Abawajy, 2014). Determining the effectiveness of these types of training exercises can be difficult (Siadati et al., 2017). Abawajy (2014), stated although there has been past research on efficacy of information security training delivery methods, the empirical research on which phishing training method is most effective is conflicting. Despite the efforts to train end-users, a large number are still vulnerable to phishing attacks (Wash & Cooper, 2018). The challenge becomes the fact that there is conflicting evidence on whether embedded phishing training is effective at educating end-users (Siadati et al., 2017) (Karumbaiah, Wright, Durcikova, & Jensen, 2016). This research will empirically investigate existing studies and use click rate results from the phishing campaign to measure if embedded phishing training is effective at educating end-users.

Background

Wash and Cooper (2018), research demonstrated embedded training where users were sent multiple phishing emails with randomly assigned embedded training. 2000 staff members at a university were set to receive these phishing emails (Wash & Cooper, 2018). If and when a user clicked on the link in any of the phishing emails, they were prompted to complete the training (Wash & Cooper, 2018). According to Wash and Cooper's (2018) findings, embedded phishing training is significantly more effective at educating users than similar training methods. Embedded training allows the user to learn about their mistake of clicking on an inappropriate link as soon as it happens (Wash & Cooper, 2018). Wash and Cooper (2018), found that overall percentage of clicks on the phishing emails declined about 45% from the beginning of the study. These results suggested the embedded training was effective at educating users, based on the click rate reductions from the first to last round of the phishing campaign.

Karumbaiah et al. (2016), research observes the impact of the different training techniques to increase the likelihood of participants identifying phishing messages. Karumbaiah et al. (2016), assigned users to three different training types; video/quiz training, embedded training, and leaderboard/game training. A group of 30 participants was randomly assigned to a training session (Karumbaiah et al., 2016). Karumbaiah et al. (2016), embedded training research included a link in the phishing email, which directed participants to a webpage and demonstrated a 3-step procedure that could have helped identify the email as phishing (Karumbaiah et al., 2016). Participants only received training if they clicked on the link in the phishing email (Karumbaiah et al., 2016). Karumbaiah et al. (2016), found no difference in the number of correct phishing emails that were reported by the subject, suggesting that the embedded training was not effective. Reducing end-user susceptibility to phishing attacks is crucial to an organization to defend assets (Abawajy, 2014). The conflicting results of the effectiveness of embedded phishing training at educating end-users leads to confusion about whether it is the ideal training method.

The research problem that this study will address is the efficacy of embedded phishing training methods on end-user awareness and their discernment of malicious phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016). According to the FBI (2016), from the last quarter of 2015 to the first quarter of 2016 the number of phishing attacks increased by 250%. The FBI (2016), estimated damage from phishing attacks exceeds $2.3 billion USD annually. It becomes apparent that ineffective embedded phishing training may leave end-users vulnerable to phishing attacks. It is difficult for end-users to identify phishing attacks without phishing training (Kumaraguru et al., 2007).

There is a lack of agreement about efficacy of embedded phishing training methods (Siadati et al., 2017) (Karumbaiah et al., 2016). While some research has a lack of agreement, Siadati et al. (2017) and Wash and Cooper (2018), research found embedded phishing training to be effective at educating end-users. Al-Daeef et al. (2017), claim that by using embedded training, users can acquire more knowledge, retain this knowledge for longer time, and can transfer this knowledge into other security fields. However, Karumbaiah et al. (2016), tested embedded phishing training and found no evidence that embedded training reduced the likelihood to click on a phishing email. According to Siadati et al. (2017), research has suggested that embedded phishing exercises might mitigate end-users from engaging with malicious phishing emails because they provide a “teachable moment”. Information about efficacy of embedded phishing training is needed to inform and support end-users in making better trust decisions that will help them avoid falling for phishing attacks (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). The specific problem that prompts this research is conflicting research on embedded phishing training methods on end-user awareness and discernment of malicious phishing emails which is needed before a conclusion can be made on whether embedded phishing training is effective at educating end-users.

Purpose

The purpose of this study is to empirically investigate the efficacy of embedded phishing training on end-user awareness via click rates of fraudulent emails. Security education and training is typically done using webpages, flyers, and posters, along with basic computer training (Wash & Cooper, 2018). Wash and Cooper (2018) believe training with webpages, flyers, and posters leaves many people vulnerable to phishing attacks. This research leverages Wombat Security phishing training tools to determine the efficacy of the embedded phishing training. The objective of this study is to empirically validate the effectiveness of embedded phishing training on reducing end-user susceptibility via reduced click rates.

Siadati et al. (2017), research suggested that embedded training can have a significant effect on decreasing the susceptibility of end-users to phishing attacks. There are many methods of phishing training, but the research appears to be conflicted about which method is the best at reducing end-users click rates of fraudulent emails (Al-Daeef et al., 2017) (Karumbaiah et al., 2016). Embedded training has become the industry standard of protecting an organization from phishing attacks, but there is still much work to be done to maximize the effectiveness of the training (Wash & Cooper, 2018).

Embedded training provides a strong motivation to learn and provides fast and effective feedback to users at the time they are most receptive to it (Wash & Cooper, 2018). Siadati et al. (2017), found that embedded training is likely not useful in providing protection for vulnerable users who are easily deceived by unpersuasive phishing emails. These conflicting results warrant for additional research on the efficacy of embedded phishing training. By researching embedded phishing training and testing its effectiveness, this study will allow an organization or user to review their options for phishing training and determine if embedded training will be effective at educating their end-users.

Research Questions

The research will answer the following questions:

1. What is the initial click rate of end-users on Phish A?
2. How did click rates of end-users change from Phish A to Phish B?
3. What percentage of end-users clicked neither Phish A nor B?
4. What percentage of end-users clicked on both Phish A and B?

Nature of the Study

This exploratory study will use a case study approach. The design of this study is a phishing campaign utilizing embedded phishing exercises. PhishSim by Wombat Security will be used to conduct the phishing campaign. Siadati et al. (2017), research compared click rate changes to determine if their embedded training was effective at educating users. This same method will utilize click rate results of the phishing campaign to determine if the embedded phishing training was effective at educating end-users. Results of the study will be used to answer the research questions.

Significance of the Study

There are many different forms of phishing training methods available to help educate end-users. There is some research on the efficiency of phishing training methods, but research is limited regarding effectiveness of phishing training (Abawajy, 2014). With conflicting results on efficacy of embedded phishing training, it is understandable that organizations and users are unsure of whether embedded training will educate them effectively. This research intends to provide information on whether embedded phishing training is effective at educating users.

Definition of Terms

- Attacker – unauthorized user who attempts to or gains access to an information system (NIST, 2013).
- Awareness – Activities which seek to focus an individual's attention on an issue or set of issues (NIST, 2013).
- Education (Information Security) – Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce IT security specialists and professionals capable of vision and proactive response (NIST, 2013).
- Efficacy – The ability to produce a desired or intended result (Dictionary, 2018).
- Embedded training (Information Security) – The ability to train work activities and skills by using the associated operational system including software and machines that people normally use (Al-Daeef et al., 2017).
- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST, 2013).

- Phishing – A digital form of social engineering that uses authentic looking emails to request information from users to direct them to a fake website that requests information (NIST, 2013).
- Security breach – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST, 2013).
- Social engineering – An attempt to trick someone into revealing information (NIST, 2013).
- Spam – The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages (NIST, 2013).
- Spear-phishing – A more sophisticated phishing attack, where the attacker will go through an extra step of personalizing an email to their targets (Alam & El-Khatib, 2016).
- Spoof – Masquerading as the sending machine and sending a message to a destination (NIST, 2013).
- Training (Information Security) - Training strives to produce relevant and needed (information) security skills and competencies (NIST, 2013).
- Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (NIST, 2013).

Assumptions

- Adequate research will be found to support this study.
- Users will have basic knowledge on how to operate a computer.
- Users will complete the embedded training fully if prompted to do so.
- Users will attempt to retain knowledge from the embedded training.

Limitations

- Phishing campaign will have a limited timeframe of two weeks.
- Phishing campaign is limited to two emails.
- Phishing campaign is limited to quarter of the organization participating.
- Case study done on one company in the financial sector. Generalizability of a population may be limited.
- This is a study of efficacy of embedded phishing training, not comparing other phishing training delivery methods.
- Others testing efficacy of embedded phishing training may have differing results.
- Literature research is limited to articles available through the Ferris State University Library database and the Internet.

Chapter 2: Literature Review

The research problem that this study will address is the efficacy of embedded phishing training methods on end-user awareness and discernment of malicious phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016). There is conflicting research on embedded phishing training methods on end-user awareness and discernment of malicious phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016). While it may be impossible to eliminate the end-user from engaging in phishing emails, the best possible approach is to educate the end-user on phishing (Arachchilage & Love 2014). This literature review identifies previous studies that focus on efficacy of embedded phishing training at educating end-users. Although most research supports that embedded phishing training is effective at educating users, there is conflicting results on whether this is true. To provide context of the study, related work on embedded phishing training from academic literature will be examined.

Embedded phishing training is a simulation-based delivery method, where users are sent simulated phishing emails to test users' vulnerability to phishing attacks and then follow-up with training (Abawajy, 2014). If the user clicks on the embedded phishing training email they are given materials that inform them about phishing attacks and subsequent phishing emails were used to assess progress in phishing detection abilities of the users (Abawajy, 2014). Embedded phishing training is utilized by organizations to reduce the susceptibility of its employees to phishing emails (Siadati et al., 2017). Embedded training provides a strong motivation to learn and gives the user quick feedback at the time they are most receptive to it (Wash & Cooper, 2018). Embedded training has become an industry standard way of protecting an organization against phishing attacks, but much work needs to be done to maximize the effectiveness of the training messages (Wash & Cooper, 2018).

This research builds on efficacy of embedded phishing training. Previous research done by Siadati et al. (2017) and Wash and Cooper (2018), suggests that embedded phishing training is effective at educating end-users. In a study done by Siadati et al. (2017), they conducted embedded phishing exercises to determine how effective the embedded training was at educating users. Siadati et al.'s (2017), experiment involved 19,180 participants from an organization, utilizing 115,080 test phishing emails. Siadati et al. (2017), focused on eliminating sources of bias, enabling sounder evaluations of the efficacy of embedded phishing exercises. Little or no research has explored possible factors that might bias results, such as differing levels of persuasiveness of the phishing emails (Siadati et al., 2017). Effectiveness of phishing exercises is primarily evaluated on changes in the click rate of the first and last round of phishing exercises (Siadati et al., 2017). This study will use a similar method to determining effectiveness of embedded phishing training at educating users, by measuring click rates of each email in the phishing campaign.

Embedded phishing training is considered effective if the average click rate is significantly reduced (Siadati et al., 2017). In research conducted by Siadati et al. (2017), the average click rate of phishing emails decreased by over 40%. The differences in each phishing email may provide misleading results as each email has differing content (Siadati et al., 2017). Although click rates of phishing emails may not directly relate to effectiveness of the training, research shows embedded phishing training can have a significant effect on decreasing susceptibility of the users to phishing attacks (Siadati et al., 2017).

Wash and Cooper (2018), conducted a phishing experiment sending users multiple phishing emails with randomly assigned embedded training. When a user clicks on the link in any of the phishing emails, they receive a training message (Wash & Cooper, 2018). Wash and

Cooper (2018), randomly targeted 2000 staff members at a university with a series of four phishing emails that were sent over the period of two months. The first phishing email sent was clicked on by 11.7% of users (Wash & Cooper, 2018). The last phishing email sent was clicked on by 7.51% of users (Wash & Cooper, 2018). This is a decrease of click rate by 4.19%.

Wash and Cooper (2018), results suggested that the embedded training was effective at reducing click rates and reducing end-user susceptibility to phishing attacks. A challenge Wash and Cooper (2018), faced is getting all participants to engage in this study. Only users who clicked on a phishing link in the first three emails received embedded training (Wash & Cooper, 2018). This is because users who only clicked on the last email and received training did not have another opportunity to use the training (Wash & Cooper, 2018). Only 421 users clicked on one of the first three emails, limiting their sample size to about 20% of the original size (Wash & Cooper, 2018). This limited size of participants may have had an effect on results of how effective the embedded training was at educating users. According to Siadati et al. (2017), research, measuring the effect of phishing training can be limited by small sample size. To address the limitations of sample size, this study will have a higher number of participants than previous studies, such as the studies conducted by Wash and Cooper (2018) and Karumbaiah et al. (2016). Wash and Cooper (2018), research had 502 users complete their embedded phishing training. Karumbaiah et al. (2016), research used 30 participants in their embedded training exercises.

Research done by Karumbaiah et al. (2016) as well as, Caputo, Pfleeger, Freeman, and Johnson (2014), suggested that embedded phishing training is not effective at educating end-users. Karumbaiah et al. (2016), research took a preliminary look at the effects of different types of phishing training methods. This research was conducted to observe the impact of the different training techniques to increase the likelihood of participants identifying and reporting phishing messages (Karumbaiah et al., 2016). The three types of training examined by Karumbaiah et al. (2016), were video/quiz training, embedded (just-in-time) training, and a phishing leaderboard game. Karumbaiah et al. (2016), had a group of 30 participants randomly assigned to one of the training sessions. The study emulated a normal working day, where participants were expected to accomplish tasks and respond to work-related emails while watching for and reporting phishing emails (Karumbaiah et al., 2016).

In the video/quiz training, participants were introduced to a high-quality video describing how to identify phishing messages and given a follow-up quiz that reinforced the phishing training (Karumbaiah et al., 2016). In the embedded (just-in-time) training, participants received training if they clicked on a phishing message (Karumbaiah et al., 2016). The phishing leaderboard game tracks when participants identify phishing message correctly. Karumbaiah et al. (2016), measured efficacy of the embedded training by focusing on users who clicked on at least one phishing message. The preliminary results of the training done by Karumbaiah et al. (2016), indicated that the video/quiz and leaderboard training decreased the likelihood of a user clicking on a phishing message as measured by; the follow-up quiz results and number of phishing messages reported correctly. The embedded training did not reduce the likelihood of a user clicking on a phishing email as measured by the click rates of the phishing messages (Karumbaiah et al., 2016). The lack of participants, 30, in the study done by Karumbaiah et al. (2016), may provide misleading results, suggesting that embedded phishing training was not effective at reducing the likelihood of a user clicking on a phishing email. Siadati et al. (2017), research claimed that previous works are limited in measuring efficacy of phishing training due to small sample size. To avoid any issues with inaccurate results due to small sample size, a larger sample size of 924 users will be used to complete this study.

Caputo et al. (2014), explored the effectiveness of embedded training by conducting a spear-phishing experiment. Spear-phishing is a type of phishing attack that occurs when the attacker targets individuals with a phish that they are likely to expect or welcome (Alam & El-Khatib, 2016). The email is tailored to each specific recipient, using personal information available on social networking websites to appeal to the user's interests (Verma, Ensias, Mohamed, Abdellah, & Rabat, 2015). Caputo et al. (2014), hypothesized that if users are provided with embedded training immediately after clicking on a phishing link, they will be less likely to repeat the same error when presented with a similar situation. A lower rate of clicks on spear-phishing links and increased reporting of suspicious emails reflected an improved security culture at an organization (Caputo et al., 2014). Caputo et al. (2014), sample size consisted of 1,359 participants in one organization. The participants were all sent the same spear-phishing emails. The participants who clicked the link received embedded training and pointed out items that should have made the user suspicious (Caputo et al., 2014).

Caputo et al. (2014), research indicated that immediate feedback from embedded training does not reduce end-user click rates or increase reporting of phishing emails. However, Caputo et al. (2014), reported only the results of phishing training from one corporate organization. Caputo et al. (2014), claim their research needs to be replicated at other institutions in order to validate the generalizability of the results. Caputo et al. (2014), found that many participants did not read the training they were provided and either clicked on every embedded phishing link or none of them. Unfortunately, there is no practical way to confirm that a participant actually completed the embedded training (Caputo et al., 2014).

The research reviewed identified multiple embedded training exercises with conflicting results. A phishing campaign is considered effective if the click rate is reduced (Siadati et al., 2017). Siadati et al. (2017), research found embedded phishing training was effective at reducing click rates and reducing end-user susceptibility to phishing attacks. Karumbaiah et al. (2016), research claimed that embedded phishing training was ineffective at educating end-users and reducing click rates of fraudulent emails. The conflicting results from the studies done by Karumbaiah et al. (2016) and Siadati et al. (2017), demand for additional embedded phishing testing to be conducted to measure the efficacy at educating end-users via reduced click rates.

Chapter 3: Methodology

This is an experimental, exploratory study to determine the efficacy of embedded phishing training methods on end-user awareness and their discernment of malicious phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016). Existing literature provides one with conflicting results on whether embedded phishing training is actually effective at educating the end-user and reducing end-user susceptibility to phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016).

This study will have a quantitative approach. Quantitative information can be very useful for augmenting the summary of an event or for adding more context to a topic (Alonso, 2015). Alonso (2015), research stated extracting relevant quantitative information can be beneficial to a topic and useful in scenarios where numerical data can help with context or summaries. An example of this is using numerical data, click rate changes, from the embedded phishing exercises to give context to whether the embedded training was effective at educating end-users.

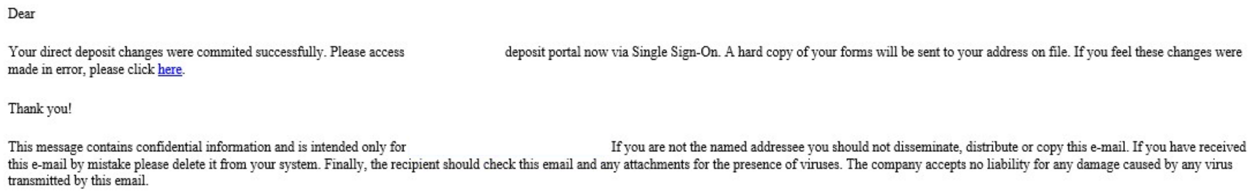
Design of Study

This study was designed to evaluate embedded phishing training to empirically investigate if the embedded training was effective at educating end-users via click rates of fraudulent emails. Effectiveness of phishing exercises is mainly evaluated on changes in click rate of the first and last round of the exercise (Siadati et al., 2017). A phishing campaign is considered effective if the average click rate is reduced (Siadati et al., 2017). To test embedded phishing training, a phishing campaign was conducted at an anonymous organization. Participants are expected to complete the phishing awareness training and attempt to retain the knowledge. 924 users have been randomly selected to participate in this study. The active directory from the participating organization was imported into Wombat’s phishing campaign tool to randomly select which of the 3000+ employees were going to receive the phishing emails. The available sample size for this study is a quarter of the organization participating in the study. The organization did not want all employees participating in this study, their user limit was a quarter of the company.

To conduct the embedded phishing training, a phishing campaign will be done using the PhishSim tool provided by Wombat Security. Wombat Security was selected as the phishing campaign tool because of the features it has to offer. Wombat offers an embedded phishing email service, which allows for the customization of each email for the phishing campaign and provides embedded training to users who fall for the phishing test. With the phishing campaign tool provided by Wombat, it tracks the clicks and other statistics, such as data entered, of each phishing email sent. The statistic tracking is done automatically by Wombat's phishing campaign tool.

In this study, participants were sent two phishing emails. The phishing emails are classified as 'Phish A' and 'Phish B'. Phish A and Phish B were sent over a two-week period. Phish A was sent to users on July 17th around 10:00am. Phish B was sent to each participant on July 24th around 10:00am. This day of the week and time were chosen as a time that people were likely to be using email, and also because it reflects a common time to receive real phishing emails (Wash & Cooper, 2018). Results of both Phish A and Phish B were recorded one week after the initial email was sent to give participants time to interact with the email. Phish A and Phish B contains a phishing link that tracks whether the user clicked on an email. Click rates for each phishing email will be recorded by Wombat Security automatically. The click rates on the phishing emails for each participant will be used to measure if the embedded phishing training was effective at educating users.

The first email, Phish A, was created to represent a legitimate change in the users' direct deposit information. The format of Phish A was chosen to trick users into thinking their direct deposit information has changed. Phish A was spoofed to appear to be coming from the organization the participants are employed for. This made for a believable phishing email, if a direct deposit information change email came from a random organization, the phishing email would not be as authentic. Below in *Figure 1.,* Phish A of the phishing campaign can be seen.



Dear

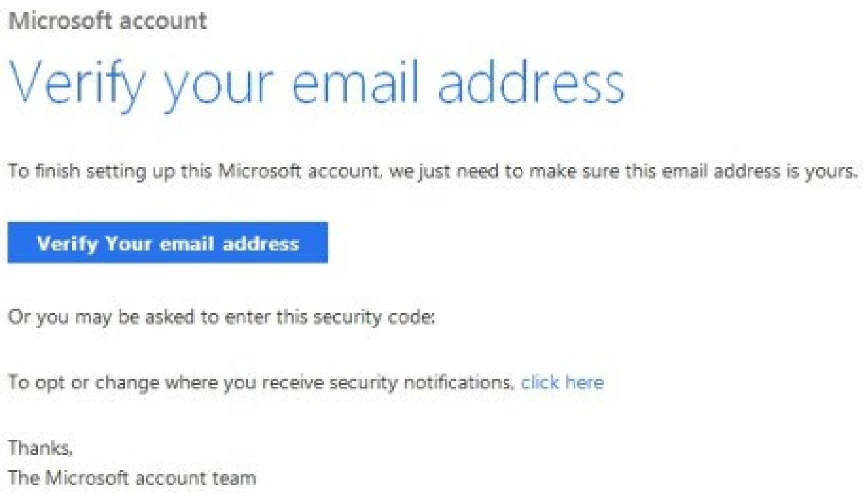
Your direct deposit changes were commited successfully. Please access deposit portal now via Single Sign-On. A hard copy of your forms will be sent to your address on file. If you feel these changes were made in error, please click here.

Thank you!

This message contains confidential information and is intended only for If you are not the named addressee you should not disseminate, distribute or copy this e-mail. If you have received this e-mail by mistake please delete it from your system. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.

Figure 1. Phish A

The second email, Phish B, was created to represent a legitimate Microsoft Outlook account verification. The format of Phish B was chosen to trick users into believing they need to verify their Microsoft Outlook account. End-users participating in this phishing campaign utilize Microsoft Outlook in their daily work. This made Phish B look more realistic to users. Below in *Figure 2.,* the last email of the phishing campaign can be seen.



Microsoft account

Verify your email address

To finish setting up this Microsoft account, we just need to make sure this email address is yours.

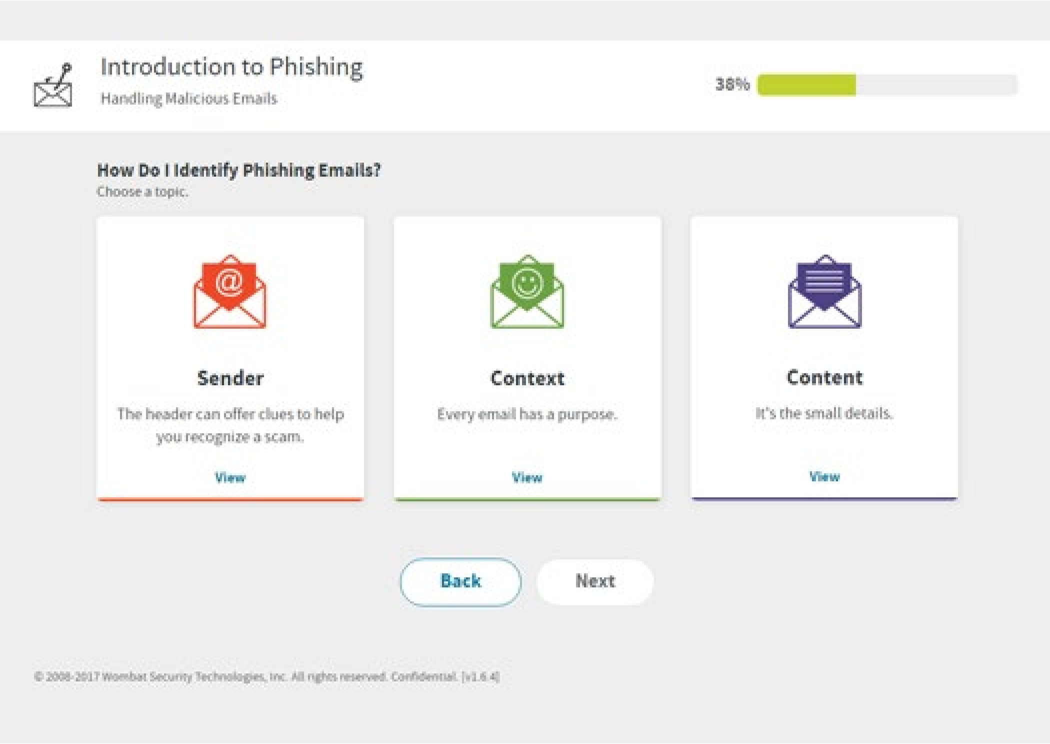
Or you may be asked to enter this security code:

To opt or change where you receive security notifications, click here

Thanks,
The Microsoft account team

Figure 2. Phish B

Both Phish A and Phish B contained embedded phishing training. When the user clicks the phishing link in either Phish A or Phish B, they will be redirected to a webpage where they are then provided with phishing awareness training. An example of the embedded phishing training can be seen in *Figure 3*. The embedded phishing training was designed around training users in a teachable moment, such as when the user makes a mistake by clicking on the embedded phishing link. The phishing awareness training will inform the user about the dangers of phishing and list suspicious indicators of Phish A and Phish B. Under the content option it provides information that can be used to identify that Phish A was fraudulent. For example, the phishing training informs the user about viewing the hyperlink before clicking. If the user hovered their mouse over the phishing link, they would have noticed the webpage being linked was not directing them to their organizations direct deposit page.



Introduction to Phishing

Handling Malicious Emails

38%

How Do I Identify Phishing Emails?

Choose a topic.

Sender

The header can offer clues to help you recognize a scam.

View

Context

Every email has a purpose.

View

Content

It's the small details.

View

© 2008-2017 Wombat Security Technologies, Inc. All rights reserved. Confidential. [v1.6.4]

Figure 3. Wombat Training Page

Data Analysis

After the phishing campaign is completed, click rate results will be added into an Excel spreadsheet. Wombat provides statistics about users who; received Phish A or B, opened Phish A or B, and clicked on the phishing link in Phish A or B. Phish A and Phish B click rates of the phishing campaign will be measured to compute the percentage of participants who clicked on a phishing link. To measure the end-user click rates of Phish A or B, the number of users who clicked on the phishing link will be divided by the total sample size of 924 participants. The click rate percentages from each round will be compared in the spreadsheet. The click rate results for each test email will determine if embedded training was successful at reducing user susceptibility to fraudulent emails. A potential limitation of the data collection process is users' who don't click on any of the phishing emails. To address this, non-clickers will be measured from the sample size as well as participants who clicked on the embedded phishing link in both Phish A and Phish B.

One ethical concern of this study is consenting to participate. If users are aware they are participating in a phishing campaign, they may be looking out for suspicious emails. This can reduce study validity due to changes in behavior (Wash & Cooper, 2018). Users might evaluate emails differently than normal if they know they are a part of a study (Wash & Cooper, 2018). To avoid this, users are not being informed of the study. No users will encounter any negative consequences by participating in this study, as users will be kept anonymous as well as click rates for Phish A and Phish B.

Another ethical concern of this study is approval from the participating organization. Conducting the phishing campaign without permission may lead to legal consequences, as the organization would have no idea their users are being phished. To gain approval, a proposal for the phishing campaign was sent to the Information Security Manager at the participating organization. The phishing campaign was done with permission of, and in coordination with, the Information Security team.

Summary

Existing literature about efficacy of embedded phishing training at educating end-users is conflicting (Siadati et al., 2017) (Karumbaiah et al., 2016). This study will have a quantitative approach, focusing specifically on the click rate changes from Phish A to Phish B. A quantitative approach is beneficial, as it will allow for the comparison of the differing click rates for both Phish A and Phish B. This study was designed to evaluate embedded phishing training to determine if the embedded training was effective at educating end-users via reduced click rates. A phishing campaign with embedded phishing training is being conducted with PhishSim, a tool provided by Wombat Security. Wombat Security automatically collects data on whether a user clicked either Phish A or Phish B. Participants will be sent two emails, Phish A and Phish B, over a two-week period. Phish A and Phish B each contain a phishing link that tracks whether the participant clicked on the email or link. Phish A was designed to imitate a change in the participants direct deposit information. Phish B was designed to imitate a Microsoft Outlook account verification. Phish A and Phish B were designed to trick users into believing the emails are legitimate. When the participant clicks on the embedded phishing link in either Phish A or Phish B, they will be redirected to a webpage where they are provided with phishing awareness training. Succeeding the phishing campaign, click rate results will be added into Excel and evaluated. Click rates of Phish A and Phish B will be measured to determine efficacy of the embedded phishing training. A major ethical concern of this study is not receiving consent from participants. If users are informed of the ongoing phishing campaign, there is a possibility that participants behavior toward emails will change. To ensure the validity of these results, participants are not being informed of the phishing campaign.

Chapter 4: Results

The research problem that this study will address is the efficacy of embedded phishing training methods on end-user awareness and their discernment of malicious phishing emails (Siadati et al., 2017) (Karumbaiah et al., 2016). The purpose of this study is to empirically investigate the efficacy of embedded phishing training on end-user awareness via click rates of fraudulent emails. Wash and Cooper (2018), research found that embedded training has become an industry standard way of protecting an organization against phishing attacks. It is critical to understand whether embedded phishing training is an effective method of education and can be used to improve phishing training messages in organizations, as it has become one of the most common methods of phishing training. Each research question is addressed in this chapter by using the phishing campaign results.

The goal of this research study was to determine if the embedded phishing training was effective at educating end-users via reduce click rates of fraudulent emails. According to Siadati et al. (2017), effectiveness of phishing exercises is primarily evaluated on changes in the click rate of the first and last round of phishing exercises. Reduction of overall click-through rates of the phishing campaign indicate the effectiveness of the embedded phishing training at reducing end-user susceptibility to fraudulent emails. Measuring click rates of the first and last round of the phishing campaign is used in this study to evaluate if the embedded phishing training was effective at educating end-users. If the average click rate in this study is reduced, the embedded phishing training was effective.

A phishing campaign with embedded phishing exercises was conducted to determine if embedded phishing training is effective at educating end-users. The phishing campaign was conducted with the PhishSim tool provided by Wombat Security. Statistics of the phishing campaign, such as click rate, is automatically recorded in Wombat. Wombat does this by tracking each email, in this case Phish A and Phish B, by using the embedded phishing link. Each time a user clicks on the embedded phishing link, Wombat stores the interaction. 924 participants of an organization were randomly selected to take part in the phishing campaign. This includes participants with varying job titles: everyone from high-level executives to entry-level positions. Participants were randomly selected to attempt to accurately represent the organization. No participant was informed of the phishing campaign, to ensure the legitimacy of the results. While all participants in this sample size work for the same organization, the wide range of job titles may allow for generalization beyond this organization. Limiting the phishing campaign to specific users may not provide accurate results.

Phish A was sent to 924 participants on Tuesday, July 17th around 10:00am. Phish B was sent to each participant on July 24th around 10:00am. This day of the week and time was chosen as a time that people were likely to be using email. Sending both Phish A and Phish B at the same time of day helps minimize any differences due to timing. Only two emails were sent in this study due to time constraints and organizational preference. The organization participating was undergoing an internal system conversion. It was requested by the organization that the phishing campaign only run for a short period of time.

To measure the effectiveness of the embedded phishing training, a table was created containing each email, number of emails sent, number of users who clicked on the phishing link, and percentage clicked. Results of the phishing campaign can be seen in Table 1. The first column, email, lists emails Phish A and Phish B which were sent during the phishing campaign. The second column, emails sent, lists the exact number of emails that were sent of Phish A and Phish B. In this phishing campaign, 924 emails were sent out in each round. Equaling 1,848 emails sent in total. The third column, emails opened, lists how many emails were opened in Microsoft Outlook by the participant. Wombat tracks if a user has opened an email. This does not necessarily mean the user clicked on the phishing link, just that the email was opened and viewed. If a user ignored or deleted the email from their inbox, the email will not be recorded as opened. The fourth column, number of users clicked, is the number of participants that clicked on the embedded phishing link in Phish A and Phish B. This statistic is recorded automatically by Wombat. When a participant clicks the embedded phishing link for the first time, Wombat records the interaction and provides phishing awareness training. The fifth column, percentage of users clicked, is the embedded phishing link click rate of Phish A and Phish B. This is calculated by dividing the number of participants who clicked on the embedded phishing link by number of emails sent.

Table 1

Phishing Campaign Results

Email	Emails Sent	Emails Opened	# of Users Clicked	% of Users Clicked
Phish A	924	489	383	41%
Phish B	924	449	258	28%

Research Question 1: What is the initial click rate of end-users on Phish A?

The first email of the phishing campaign is named Phish A. Phish A was sent out to all 924 participants. Out of the 924 participants who received this email in their inbox, 489 participants opened Phish A. Of the 489 participants who opened Phish A, 383 of the participants clicked on the embedded phishing link. To determine the click rate for Phish A, the number of participants who clicked on the embedded phishing link must be divided by the total number of emails sent. The click rate of all participants for Phish A is 41%. The click rate of the participants who opened Phish A is 78%. The results of Phish A can be found in *Figure 4*.

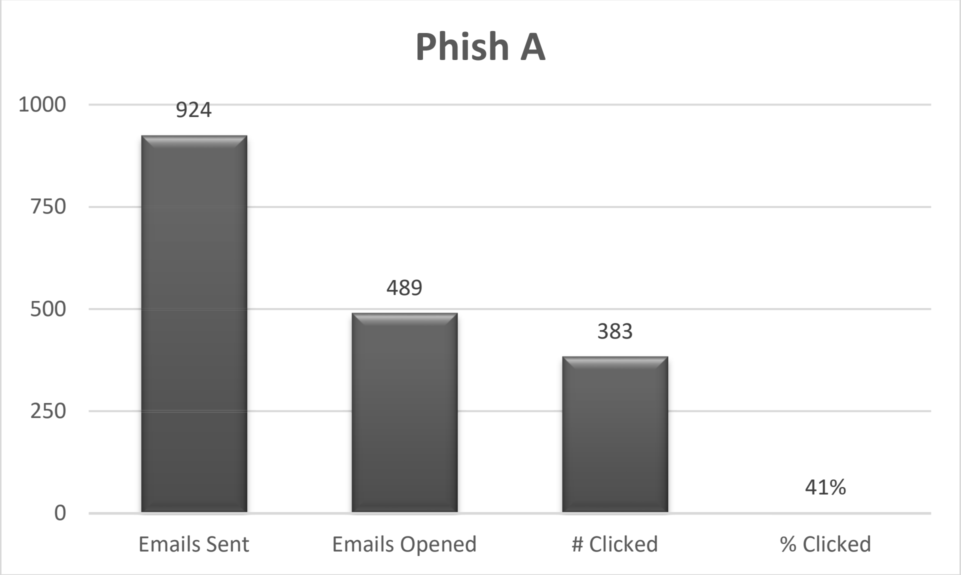


Figure 4. Phish A Results

The click rate of 41% on Phish A is extremely high. This was an unexpected result. Comparing the results to previous studies of embedded phishing training, this study had a much higher click rate percentage. Wash and Cooper (2018), embedded phishing training results had an 11.7% click rate for the first email sent, compared to the 41% click rate of Phish A in this study This may be due to the design of Phish A. Phish A was designed to represent a direct deposit information change coming from the organization that the participants are employed at.

The second email of the phishing campaign is named Phish B. Phish B was sent out to the same 924 participants as the first email. Of the 924 participants who received Phish B, 449 of them opened the email. Out of the 924 participants who received this email in their inbox, 258 of the participants clicked on the embedded phishing link. To determine the click rate for Phish B, the number of participants who clicked on the embedded phishing link must be divided by the total number of emails sent. The click rate of all participants for Phish B is 28%. The click rate of the participants who opened Phish B is 57%. The results of Phish B can be found in *Figure 5*.

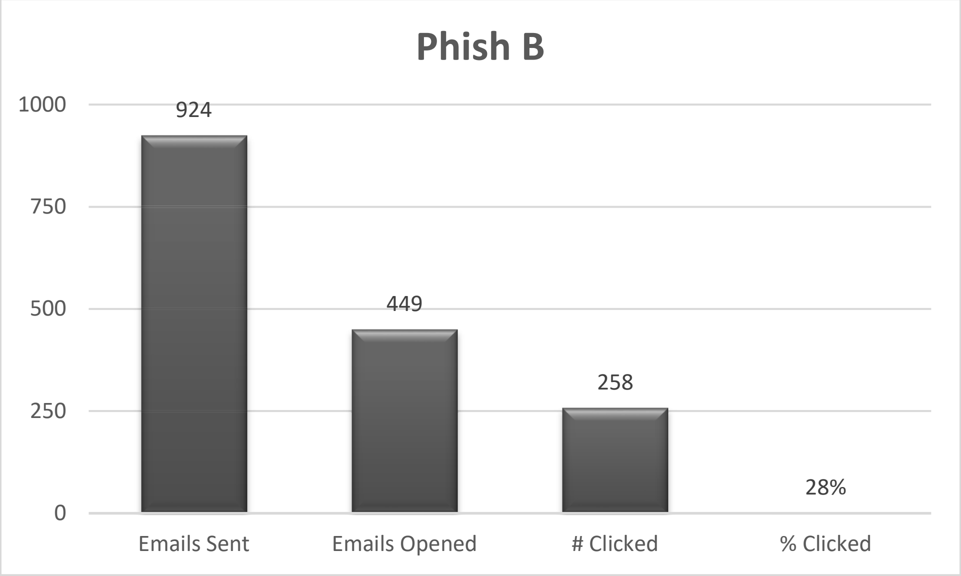


Figure 5. Phish B Results

While the click rate for Phish B is still somewhat high at 28%, compared to the 41% click rate of Phish A this is a considerable improvement. Phish B may have been less persuasive than Phish A. Phish A appeared to be coming from the organization the participants work for, while Phish B appeared to be coming from an outside source. It is difficult to determine if this is the case, as only two different types of emails were sent during this phishing campaign. Subsequent rounds of the phishing campaign with varying email types would provide a better understanding on whether click rates have a direct relationship with email types.

Research Question 2: How did click rates of end-users change from Phish A to Phish B?

To determine if the embedded phishing training was effective at educating end-users, the click rates of Phish A and Phish B of the phishing campaign will be measured and compared. Effectiveness of phishing exercises is primarily evaluated on changes in the click rate of the first and last round of phishing exercises (Siadati et al., 2017). Phish A was sent to 924 participants. Of the 924 participants, 383 clicked on the embedded phishing link. The click rate of participants for Phish A was 41%. Phish B was sent to the same 924 participants. Of the 924 participants, 258 clicked on the embedded phishing link. The click rate of end-users for Phish B was 28%. By subtracting the click rate of Phish B, 28%, from the click rate of Phish A, 41%, it provides the differences in click rate for Phish A and Phish B. This means the click rate of participants from Phish A to Phish B reduced by 13%. A hypothesis can be made that the embedded phishing training was effective at educating end-users and reducing their susceptibility of clicking on fraudulent emails. As participant click rates decline, their susceptibility to fraudulent emails reduces. This is due to the reduced click rates from Phish A to Phish B.

In *Figure 6.*, the result comparison of Phish A and Phish B can be seen. The bar with dots inside represents the number of emails, Phish A and Phish B, that were sent to participants. The bar with lines represents the number of participants that opened Phish A or Phish B. The grey bar represents the number of participants who clicked on Phish A or Phish B. The black line going across the figure represents the click rate percent changes from Phish A to Phish B.

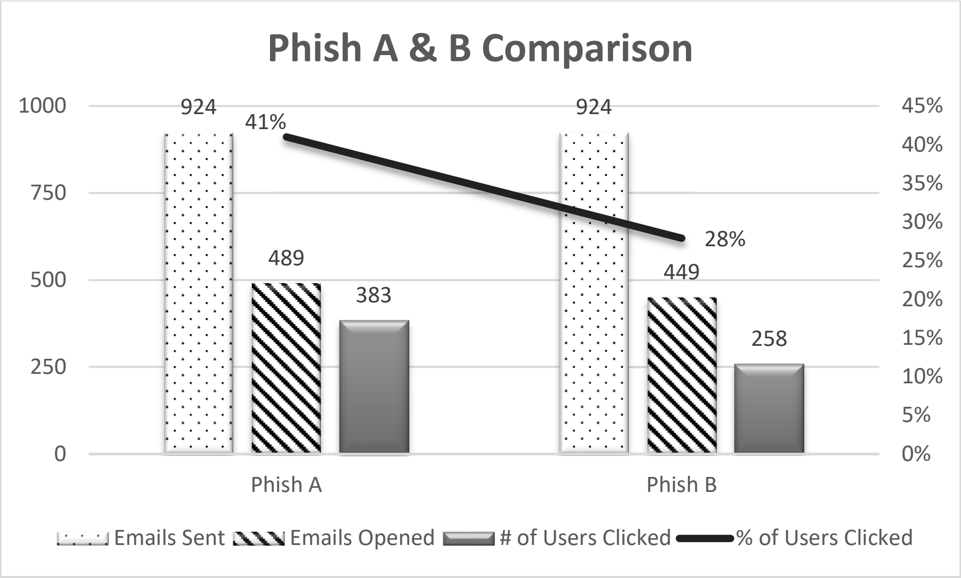


Figure 6. Phish A & B Comparison

Research Question 3: What percentage of end-users clicked neither Phish A nor B?

While the main purpose of Wombat is to determine what number of participants clicked on the embedded phishing link in either Phish A or Phish B, Wombat also provides statistics about how many users did not click on the embedded phishing link in either Phish A or Phish B. 320 participants were secure and did not click on an embedded phishing link in either Phish A or Phish B. To calculate the percentage of participants that clicked on neither Phish A or B, divide the number of participants who did not click on the embedded phishing link in both Phish A or Phish B by the total number of participants. This calculation means that 35% of the participants did not click on an embedded phishing link. These participants didn’t click on either phishing email, meaning these participants received no form of embedded phishing training. This may be due to two reasons; participants not opening the phishing email or participants recognized that the email was fraudulent and didn’t interact with the embedded phishing link.

Research Question 4: What percentage of end-users clicked on both Phish A and B?

Knowing the click rates for Phish A and Phish B, as well as those participants who did not click either embedded phishing link, allows for a calculation to be made about which participants clicked on the embedded phishing link in both Phish A and Phish B. To calculate the percentage of participants that clicked on the embedded phishing link in both Phish A and Phish B, add the number of participants who clicked on Phish A, the number of participants who clicked on Phish B, and the number of participants who clicked on neither Phish A or Phish B from the total number of participants. This calculation returns a number of 961. As stated previously, 924 participants were selected for this study. Subtracting the number of participants from 961 will provide the number of participants who clicked on both Phish A and Phish B. This calculates that 37 participants clicked on both Phish A and Phish B. To determine the percentage of participants that clicked on both Phish A and Phish B, divide the number of participants that clicked on both Phish A and Phish B by the total number of participants. The percentage of participants that clicked on both Phish A and B is 4%. These 37 participants received embedded training twice, each time they interacted with the embedded phishing link. Although only a small amount, 37, of participants clicked on both Phish A and Phish B, the embedded phishing training was ineffective for these participants as they were susceptible for both fraudulent emails. Table 2 contains the click results of the phishing campaign for all participants. Never clicked means the participant did not interact with either embedded phishing link in either Phish A or Phish B. Clicked once means the participant clicked on one embedded phishing link in either Phish A or Phish B. Always clicked means the participant clicked on the embedded phishing in both Phish A and Phish B.

Table 2

Percent of Participants Who Never Clicked, Clicked Once, or Always Clicked.

Type of User	Subjects	Percent
Never Clicked	320	35%
Clicked Once	567	61%
Always Clicked	37	4%

The effectiveness of the embedded phishing training at educating end-users is conspicuous. Overall click rate percentage declined from Phish A to Phish B by 13%. 604 users received phishing training as a part of this study, which is 65% of the people who were selected for this study. 65% of participants clicking on a phishing link is a tremendously high percentage. Wash and Cooper (2018), evaluated their own embedded training and resulted in only 25.8% of users receiving training. Although 65% of users clicked on either Phish A or Phish B, the reduced click rates indicate that the embedded phishing training is helping reduce user's susceptibility to fraudulent emails. The results from the phishing campaign supports that embedded phishing training is effective at educating end-users and reducing their susceptibility to fraudulent emails. While participants in this population work for a financial institution, the wide range of job titles exemplifies that this study can represent a selection of workers and is likely to generalize to another financial institution or similar organization.

Chapter 5: Conclusion

In this study, an empirical investigation has been done on embedded phishing training efficacy at educating end-users and their discernment of malicious phishing emails. The hypothesis for this study is embedded phishing training is effective at educating end-users and reducing susceptibility of phishing attacks. Phishing attacks are one of the most dangerous information security threats present in the world today (Alam & El-Khatib, 2016). Training users to recognize and avoid clicking on links in phishing emails is a large and important business today (Wash & Cooper, 2018). Embedded phishing training is a method where users are sent simulated phishing emails to test users' vulnerability to phishing attacks (Abawajy, 2014). Embedded training has become an industry standard way of protecting an organization against phishing attacks (Wash & Cooper, 2018).

A phishing campaign with embedded phishing training was conducted to determine if embedded phishing training was effective at educating end-users. The phishing campaign was conducted using PhishSim, a tool provided by Wombat Security. PhishSim is a phishing campaign tool, which integrates an embedded phishing link into the email to track when a participant has clicked on the phishing link. When a user clicks on the embedded phishing link, they are immediately provided with phishing awareness training. Although embedded training has become the industry standard, there are still conflicting results on whether embedded training is effective at training end-users.

One issue discovered in this study is regarding the conflicting results of embedded phishing training. Previous studies done by Siadati et al. (2017) and Karumbaiah et al. (2016), have conflicting results on whether embedded training is effective at training end-users. Siadati et al. (2017), research suggested embedded training is effective at educating end-user and reducing susceptibility to phishing emails, while Karumbaiah et al. (2016), research claims that embedded training had no effect on the end-users phishing awareness or susceptibility to fraudulent emails.

Results from the phishing campaign show a reduced click rate of 13% from Phish A (41% click rate) to Phish B (28% click rate). Phishing campaigns are considered effective if the average click rate is reduced (Siadati et al., 2017). The click rate results support the hypothesis that embedded phishing training is effective at educating end-users and reducing their susceptibility to fraudulent emails. Results from the phishing campaign implicate that the embedded phishing training was successful at educating end-users. This is determined via the reduced click rates from Phish A to Phish B. A reduction in click rates suggests that participants are less susceptible to fraudulent emails after receiving embedded phishing training. The significance of this study is to provide empirical data about embedded phishing training.

The method used to measure reduced end-user susceptibility to phishing attacks is done via reduced click rates. Comparing the click rates of the 924 users from Phish A to Phish B in the phishing campaign, results show that the embedded phishing training significantly reduced click rates of fraudulent emails. Overall, the embedded phishing training was a success. Click rates from Phish A to Phish B were reduced, meaning that the embedded phishing training was effective at educating end-users and reducing susceptibility to phishing attacks. Based on these findings, recommended improvements can be made in the design of embedded phishing training that will most likely increase their efficacy and generalizability.

Further Study

Improvements can be made to increase the efficacy and generalizability of embedded phishing training at educating end-users. In this case study, there were limitations in both sample size and phishing campaign run time. The sample in this study was limited to 924 users. Embedded phishing training with a larger number of participants may offer more accurate results that can be generalized to other financial institutions. The click rate results presented may not reflect other business sectors, as this study focused on an organization in the financial sector. Embedded phishing training involving users from multiple business sectors may provide more accurate results and allow for better generalization. Due to time constraints, the phishing campaign only provided two rounds of embedded phishing training to users. Adding extra rounds of embedded phishing training will allow for further measurements of the changing click rate percentages. This can be used to measure changes in end-user susceptibility to phishing attacks.

References

Abawajy, J. (2014). *User preference of cyber security awareness delivery methods*. Retrieved from https://doi.org/10.1080/0144929X.2012.708787

Alam, S., & El-Khatib, K. (2016). *Phishing Susceptibility Detection through Social Media Analytics*. Retrieved from https://doi.org/10.1145/2947626.2947637

Alonso, O. (2015). *Quantitative Information Extraction From Social Data*. Retrieved from https://doi.org/10.1145/3209978.3210133

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). *Security Awareness Training: A Review*. Retrieved from http://www.iaeng.org/publication/WCE2017/WCE2017_pp446-451.pdf

Arachchilage, N. A. G., & Love, S. (2014). *Security awareness of computer users: A phishing threat avoidance perspective*. Retrieved from https://doi.org/10.1016/j.chb.2014.05.046

Ariu, D., Frumento, E., & Fumera, G. (2017). *Social Engineering 2.0*. Retrieved from https://doi.org/10.1145/3075564.3076260

Dictionary. (2018). *Dictionary.com*. Retrieved from http://www.dictionary.com/

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). *Going spear phishing: Exploring embedded training and awareness*. Retrieved from https://doi.org/10.1109/MSP.2013.106

Cui, Q., Jourdan, G.-V., Couturier, R., & Onut, I.-V. (2017). *Tracking Phishing Attacks Over Time.* Retrieved from https://doi.org/10.1145/3038912.3052654

FBI. (2016). *FBI Warns of Dramatic Increase in Business E-Mail Scams.* Retrieved from https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

Jensen, M. L., Durcikova, A., & Wright, R. T. (2017). *Combating Phishing Attacks: A Knowledge Management Approach*. Retrieved from https://doi.org/10.24251/HICSS.2017.520

Karumbaiah, S., Wright, R. T., Durcikova, A., & Jensen, M. L. (2016). *Phishing Training: A Preliminary Look at the Effects of Different Types of Training*. Retrieved from http://aisel.aisnet.org/wisp2016

National Institute of Standards and Technology. (2013). *Glossary of Key Information Security Terms.* Retrieved from https://doi.org/10.6028/NIST.IR.7298r2

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). *School of Phish: A Real-Word Evaluation of Anti-Phishing Training* (CMU-CyLab-09-002).

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Protecting People from Phishing*. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1062&context=hcii

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). *Lessons from a real world evaluation of anti-phishing training*. Retrieved from https://doi.org/10.1109/ECRIME.2008.4696970

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*. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1045&context=isr

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). *Teaching Johnny not to fall for phish*. Retrieved from https://doi.org/10.1145/1754393.1754396

Siadati, H., Palka, S., Siegel, A., & Mccoy, D. (2017). *Measuring the Effectiveness of Embedded Phishing Exercises*. Retrieved from https://www.usenix.org/system/files/conference/cset17/cset17-paper-siadatti.pdf

Sung, W., & Kang, S. (2017). *An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness*. Retrieved from https://doi.org/10.1145/3085228.3085242

Verma, R., El, A., Ensias, A., Mohamed, A., Abdellah, B., & Rabat, R. (2015). *Comprehensive Method for Detecting Phishing Emails Using Correlation-based Analysis and User Participation*. Retrieved from https://doi.org/10.1145/3029806.3029842

Wash, R. & Cooper, M. M. (2018). *Who Provides Phishing Training? Facts, Stories, and People Like Me*. Retrieved from https://doi.org/10.1145/3173574.3174066

Wombat Security. (2018). *ThreatSim Phishing Simulations*. Retrieved from https://www.wombatsecurity.com/security-education/simulated-phishing-attacks

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). *One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails*. Retrieved from https://doi.org/10.1177/1541931214581306

FERRIS STATE
UNIVERSITY

College of Business – Masters of Information Security and Intelligence Program (MISI)

Certification of Authorship of MISI Course Assignment

Submitted to Professor Furstenberg

Student’s Name: Brandon Geitman

Date of Submission: December 18, 2018

Purpose and Title of Submission: Efficacy of Embedded Phishing Training

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature:__Brandon Geitman___________________________________