COMPARING SOCIAL ENGINEERING TRAINING IN THE CONTEXT OF HEALTHCARE

by

Giovanni Ordonez

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Interdisciplinary Program in Information Security

West Lafayette, Indiana

May 2022

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Ida Busiime Ngambeki, Chair

Department of Computer and Information Technology

Dr. Marcus K. Rogers

Department of Computer and Information Technology

Dr. Baijian Yang

Department of Computer and Information Technology

Dr. Dawn Laux

Department of Computer and Information Technology

Approved by:

Dr. Eugene H. Spafford

Dedicated to my family, that has supported me throughout my studies and never stopped motivating me to finish my studies.

ACKNOWLEDGMENTS

I would like to first thank my family and friends for their support throughout my graduate studies. Especially to my parents for their love and constant prayers during rough times. I am extremely grateful to have such a supportive family that has encouraged me to continue my studies in a field that I am interested in. Without your help, I do not think I would have been able to complete this thesis or even get to where I am today. Likewise, I want to thank my friends for always keeping me company, even if it was through a phone call. Those random conversations really helped me during my rough times.

I would like to give my gratitude to my advisor Dr. Ida Ngambeki. Without her help, I would have been extremely lost as to the process of doing a master's thesis. The constant support and guidance really helped me in being able to complete this thesis. I have learned a lot about what researchers do, and I respect the amount of work that is put into doing research.

I would like to also thank my committee members, Dr. Baijian Yang, Dr. Marcus Rogers, and Dr. Dawn Laux who gave me a lot of feedback on how to better this thesis. Your feedback really helped me evolve my research from what it was, so I thank you all for that.

Finally, I would like to thank my academic advisor, Dr. Eugene H. Spafford, who helped me understand the steps I needed to take to start my thesis research and graduate. I would have not been able to get to the thesis writing without your guidance. I really appreciate all your help.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Social Engineering – "The use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network" (Hatfield, 2018).

Phishing Attacks – "Phishing is an attempt to gain personal and sensitive information from individuals through online deception" (Harrison et al., 2016). "Phishers typically utilize an e-mail with a hyperlink embedded in it and a message with a warning of account closure or suggesting some unclaimed reward to entice the potential victim to click on the link" (Harrison et al., 2016).

Spear Phishing – "These attacks are more targeted than phishing emails and use personal information about their intended victims in an attempt to seen authentic and improve the likelihood that the target responds to the attacks" (Halevi et al., 2015).

Impersonation Attack – "Where the social engineer impersonates the target in order to gain access to something which the target has access to" (Mouton et al., 2014).

ABSTRACT

Social Engineering attacks have been a rising issue in recent years, affecting a multitude of industries. One industry that has been of great interest to hackers is the Healthcare industry due to the high value of patient information. Social Engineering attacks are mainly common because of the ease of execution and the high probability of victimization. A popular way of combatting Social Engineering attacks is by increasing the user's ability to detect indicators of attack, which requires a level of cybersecurity education. While the number of cybersecurity training programs is increasing, Social Engineering attacks are still very successful. Therefore, education programs need to be improved to effectively increase the ability of users to notice indicators of attack. This research aimed to answer the question - what teaching method results in the greatest learning gains for understanding Social Engineering concepts? This was done by investigating text-based, gamification, and adversarial thinking teaching methods. These three teaching methods were used to deliver lessons on an online platform to a sample of Purdue students. After conducting analysis, both text-based and adversarial thinking showed significant improvement in the understanding of Social Engineering concepts within the student sample. After conducting a follow-up test, a single teaching method was not found to be better among the three teaching methods. However, this study did find two teaching methods that can be used to develop training programs to help decrease the total number of successful Social Engineering attacks across industries.

CHAPTER 1. INTRODUCTION

1.1 Statement of the Problem

Cyber-attacks have been prevalent for many decades, but specifically, one of the more popular attacks for hackers is Social Engineering attacks, such as phishing attacks. This is because these attacks are easier to perform (Dunham, 2004) and tend to be more successful than other cyber-attacks. Social Engineering attacks target people by attempting to gain their trust to manipulate them into doing beneficial actions for the attacker. Unlike other cyber-attacks that target vulnerabilities found within a machine or some program, the vulnerability targeted is a human who cannot be fixed in the same manner as a bug within software. However, research suggests that “training can assist people [with] knowing what to look for” to determine if there is a Social Engineering attack happening or not (Workman, 2007).

According to Internet Crime Complaints published by the FBI (2021), in the past year, there were about six million complaints of cyber-related crimes. There was an increase of about 70% from 2019 to 2020, and the top three reported crimes in 2020 were "phishing scams, non-payment/non-delivery scams, and extortion" (IC3 Logs 6 Million Complaints, 2021). Within these phishing scams, the FBI defines these as Spoofing and Phishing attacks, which fall within the category of Social Engineering attacks. In another report made by Proof Point (2021), it was reported that there had been an increase in the number of successful phishing attacks. It was said that from a survey conducted on various organizations, 57% of organizations in the survey were affected by successful phishing attacks in 2020 when in 2019, it was 55%. Even with studies showing that the likelihood of being susceptible to an attack can be reduced by educating people, Social Engineering attacks are still increasing. Its effectiveness does not seem to be decreasing, as seen from these reports. Given that there are various Social Engineering training programs, one would reasonably expect that the number of successful attacks would be decreasing, but that is not the case. This brings to question - if current training programs are not that effective, what can be done to improve the teaching of Social Engineering concepts to people, to then ultimately lessen the number of victims that fall for such attacks? Specifically, what teaching method can further improve the understanding of Social Engineering concepts to change people's underlying behaviors to stop attacks from successfully happening?

The need for the improvement in teaching methods is not only because of Social Engineering attacks but also because avenues for other attacks such as malware and ransomware attacks tend to begin with Social Engineering attacks. Attackers can leverage Social Engineering attacks to compromise a machine or a network and conduct even more sophisticated attacks. One such example of a big attack beginning from a Social Engineering attack is the Petya Ransomware attack. In 2007, the Petya attack spread around the world. It targeted machines with a Windows vulnerability in the Server Message Block protocol, allowing attackers to encrypt a portion of the hard drive and other files within a system. This ransomware attack spread through phishing emails where victims would open an email and were tricked into clicking on something that started the process for Petya to get onto the victim's machine (Imarc, 2017). Although Social Engineering attacks can be used to do more sophisticated attacks like Petya, Social Engineering attacks by themselves can also cause a lot of damage. One of the most extensive phishing campaigns was Operation Phish Phry which targeted bank customers by sending them emails that looked to be from a bank or a credit card vendor. Within these emails, the customers were directed to go to some fake website and enter their credit card or bank account numbers, passwords, and other personal information (Singer, 2012). While this is only one out of many phishing attacks that have happened in the past, this shows just how devastating a single case of a Social Engineering attack can be.

While various industries are affected by multiple Social Engineering attacks, one of the more attractive industries for hackers is the Healthcare industry. It is attractive because of the patient information value, since it can be sold in black markets for a considerable price. People want to buy patient information to do things such as commit fake medical claims or other fraudulent activity (JA, 2015). A report from Check Point (2021) showed a 45% increase in cyber-attacks in Healthcare, which was "more than double the overall increase in cyber-attacks across all industry sectors worldwide" during November 2020. Most of these attacks were reported to be from ransomware and phishing emails which shows how Social Engineering attacks are very prevalent within the context of Healthcare (Check Point, 2021). Hospitals need to be well equipped to combat Social Engineering attacks to ensure that they can keep patient information private. Doing so can aid in stopping more sophisticated attacks, such as ransomware attacks, which can lead to critical situations. For example, in a case where there is a ransomware attack in a hospital, it could stop hospitals from accessing necessary medical information for physicians to treat

patients. In cases where patients are in critical condition, time is not something that many patients have, making the situation more serious.

The previously mentioned issues are not only occurring in Healthcare. Other industries also face devastating outcomes from being successfully attacked by Social Engineering attacks. This further supports the need for better teaching methods to increase knowledge retention, and ultimately decrease the number of successful Social Engineering attacks.

1.2 Scope

This research focused on looking at some online teaching methods that could be used to teach about Social Engineering attacks. A comparative analysis of teaching methods was done to determine which methods would be better for knowledge understanding. Specifically, this research looked at text-based, gamification, and adversarial thinking as the teaching methods to teach about Social Engineering attacks and determined which of these showed the greatest learning gains for the understanding of Social Engineering concepts. Since one of the most targeted industries is Healthcare, the content within the teaching included Social Engineering attacks within the context of Healthcare to give examples of actual attacks that can occur and relate it to one industry increasingly being targeted.

1.3 Significance

The significance of this research is that it has an immediate impact on current cyber-attacks that are threatening industries today. This research tackled the issue of Social Engineering through the analysis of teaching methods. This was done to improve the effectiveness of teaching certain concepts that need to be noticed when there is a Social Engineering attack occurring. This research can be translated to Healthcare, as done for this research, and other industries since other industries are also being affected by Social Engineering attacks. Hence, based on the results from this research, the more effective teaching method can be used to teach about Social Engineering concepts in various industries to ultimately help people identify indicators of attack and lessen the overall number of susceptible victims across various industries.

1.4 Research Question & Hypothesis

Which teaching method results in the greatest learning gains to help people recognize Social Engineering attack indicators and ultimately to help lower the number of successful Social Engineering attacks?

Hypothesis: Adversarial thinking is a better method by which Social Engineering concepts can be taught.

1.5 Limitations

Limitations with doing this research:

1. Given the circumstances brought by COVID-19, it is not feasible to test the teaching methods on medical staff to truly see their impact in Healthcare.
2. This research used a convenience sample of Purdue students, which posed a generalizability limitation.
3. Only a small sample of Purdue students was obtained for this research which posed a power limitation in the results.

1.6 Delimitations

Delimitations with doing this research:

1. While there are many other teaching methods, this research focused on only three teaching methods that can be applied for Social Engineering.
2. Teaching methods are focused on e-learning methods since many Social Engineering programs are now using online platforms. As well as given the COVID-19 circumstances, it is more feasible to test teaching methods that can be done on an online platform.

1.7 Assumptions

Assumptions with doing this research:

1. Users can navigate the online platform effectively
2. Users will take the lessons without simply skipping the content and going onto the assessment portion

1.8 Summary

This chapter has provided the background for this research and has explained why this research has significance within the current state of cyber attacks in various industries. This chapter also explained the Scope, Limitations, Delimitations, and Assumptions within this research. The next chapter will explore the current literature that exists within Social Engineering and teaching methods used to teach about Social Engineering concepts. The next chapter will also describe the teaching methods used within this study: text-based teaching, gamification, and adversarial thinking.

CHAPTER 2. LITERATURE REVIEW

2.1 Social Engineering

When thinking about Social Engineering attacks, it is common to associate this form of hacking with attacks such as phishing emails or scam calls. However, within Social Engineering, other various attacks are sometimes not considered or associated with Social Engineering. Historically, one of the first known misuses of technology that used Social Engineering techniques was phone phreaking which refers to the exploration of how phones work. Specifically with early phone phreakers such as John Draper in the 1970s. Draper had discovered how to bypass telephones systems by using a whistle found in a Captain Crunch cereal box which had the same frequency as the sound used by telephone companies to allow for foreign calls to be made. During some interviews with John Draper, it was found that he would use his phone phreaking knowledge of hijacking telephone systems with Social Engineering techniques to gain "information from unsuspecting Bell Telephone employees" (Hatfield, 2018). While this attack was not solely focused on Social Engineering, this is one of the earliest cases of Social Engineering techniques applied in the context of phones.

Since then, there has been an increase in the types of Social Engineering attacks that exist. There has been some taxonomy research done to organize the different forms of Social Engineering attacks. One manner by which it has been done is to separate them into two distinct groups: human-based and technical-based Social Engineering Attacks. These groups refer to how "Social engineering attacks can be done, respectively, by manipulating human psychology and by using computer technology such as pop-up windows, mail attachments, online, and vishing" (Foozy et al., 2011). Within the group of human-based attacks, you have attacks such as impersonating a user, dumpster diving, shoulder surfing, creating a sense of urgency, persuasion, and even reverse social engineering (Foozy et al., 2011). In contrast to the technical-based attacks, which include attacks such as trojan horses, pop-up windows, websites, phishing, denial of service, and Vishing (Foozy et al., 2011). There are other attacks of these two groups, but with just these, we can begin to see the vast number of different attacks that fall within Social Engineering attacks.

While some of the attacks mentioned, like phishing, are more obvious to understand why they are Social Engineering attacks, there are other attacks that are not as easily recognizable to be

associated with Social Engineering attacks. This includes attacks such as denial of service and trojan horses. For attacks like denial of service, which uses infected computers to flood a target with requests to render some services unavailable, the infection process of the machines can be achieved via Social Engineering techniques (Cloudflare, n.d.). One example of this is attackers using instant messaging to send messages to people with a malicious link and, if clicked, would install some software that the attacker would then use to control the machine. A trojan horse is some software that seems to be normal software but has some malicious code within it, and hence once installed, would infect the victim machine. Like the denial of service, a trojan horse attack can be spread through a malicious link inside a message (Householder, 2001). From these examples, we can begin to see just how Social Engineering creates more opportunities for hackers to distribute a diverse number of cyber attacks.

The increase in the number of attacks caused by Social Engineering has pushed for the development of defense methods that can be used to combat Social Engineering attacks. The different methods to defend against Social Engineering attacks can be divided into two groups which are "human-based detection and technical-based detection"(Uways Zulkurnain et al., 2015). This can be further divided into policy and auditing or education, training, and awareness within human-based detection. The policy manner can be applied to set certain rules that employees need to follow. With auditing, employees are tested on their level of awareness of Social Engineering. However, when looking at education, training, and awareness, you are approaching mitigation through the employee's education which is needed to "ensure policies, procedures and standard that have been developed in the organization [are] able to be deployed effectively" (Uways Zulkurnain et al., 2015) . Furthermore, education can allow employees to identify when there is a Social Engineering attack occurring "and know how to handle the attacks they have encountered" (Uways Zulkurnain et al., 2015).

2.2 Social Engineering in Healthcare

Some of the most common forms of Social Engineering attacks in Healthcare are phishing, Vishing, spear phishing, and impersonation (Choo at. el, 2021). An example of some of these Social Engineering attacks was in 2020 when a phishing attack was used to conduct a ransomware attack on Magellan Health, resulting in hackers getting access to about 365,000 patient and private employee information (Brownley, 2020). Another example of these commonly used Social

Engineering attacks is a recent malware attack in 2021 called TrickBot. This malware was spread through a spear-phishing campaign that targeted healthcare administrators. However, even before then, TrickBot was being used in a ransomware attack against Universal Healthcare Services in 2020, which was able to "cost the health system about $67 million in lost revenue and recovery efforts" (Davis, 2021).

Recently from 2019 to 2020, due to the uprise of the COVID-19 pandemic, there was an increase in Social Engineering attacks. During this time of fear and anxiousness due to the unknown harm of the COVID-19 virus, many attackers took advantage of these emotions to trick people into giving them personal information. In 2020, when the COVID vaccine was being developed, there were a lot of Social Engineering attacks where attackers would offer "early access to vaccines upon a deposit or monetary fee" (Davis, 2020). Various other fraud schemes were being used, and many were very successful because the general public wanted a cure due to the fear of the virus's effects. That fear made many people rather vulnerable to these scams. A study was conducted to see if health-related concerns that people had and their motivation to seek help online would result in a higher chance of them falling victim to phishing attacks related to health. It was found that their "results suggested that health concerns lead to higher phishing susceptibility" (Abdelhamid, 2020), which shows that fear about health issues raises susceptibility of falling victim to attacks. This theory is also supported by the increase in the number of victims to COVID-19 related Social Engineering attacks because fear influenced them to want to get help, and scams stating that they could aid them against the virus resulted in people being lured.

Given the multiple examples of Social Engineering in Healthcare, which contained different approaches to using Social Engineering attacks, education of Social Engineering on both employees and the public is needed to allow people to identify signs of attacks across the different sophistication of attacks. Some studies have been done within Healthcare to see the effectiveness of education and what it can do to increase the employees' awareness of Social Engineering attacks. In a study conducted on US health care institutions that use simulated phishing emails to train their employees, phishing emails were being sent to a group of employees to see if their training was beneficial in lessening the employees' susceptibility to phishing emails (Gordon et al., 2019). The results from the study indicated that "repeated phishing campaigns were associated with decreased odds of clicking on a subsequent phishing email" (Gordon et al., 2019). Hence, in the context of Healthcare, education on Social Engineering attacks has been shown to decrease falling victim to

attacks. However, the teaching methods can vary per vendor, which is where some variability can exist as to the training's effectiveness in learning about Social Engineering concepts.

2.3 Current Teaching Methods Used for Training

Efforts for Social Engineering training have been made within various organizations, and there have been various developed programs for online and in-person teaching formats. Current education methods used in industry to combat Social Engineering are serious games, virtual labs, simulations, gamification, apps, and tournaments (Aldawood & Skinner, 2019). These methods have some similarities and are often used together, but they have some distinct attributes that make them different.

Firstly, when looking at serious games and gamification, it can be quite hard to see where their difference lies. While similar to gamification, serious games are different because, within gamification, you are extracting certain gaming elements for use in a non-game application. In contrast, a serious game uses all game elements within a traditional game (Landers, 2014). According to research done on the use of Serious Games within cyber security, Serious Games is a method that is popular because it can "allow people to practice in a safe and playful way and therefore developing cyber security Serious Games may be a cost-effective solution to educate people and reduce cybercrimes" (Hendrix et al., 2016).

Virtual labs and Simulations are two other methods that share some things in common but have distinct characteristics. Simulations are "models of a real system conducting experiments for the purpose of either understanding the behavior of the system or evaluating various strategies" (Aldawood & Skinner2019). Within virtual labs, you can implement some simulations to create some phenomena or scenarios. In a sense, a virtual lab can be a platform by which we can use computers to create simulations. There are various uses of each, but one example of using a virtual lab for cybersecurity is giving students some hands-on practice with cybersecurity skills. One such example is NETLAB which has been used to teach people about cybersecurity concepts by emulating a full-scale system that includes virtual networks, routers, and firewalls, and more, as seen within different companies (Crichigno, 2019). By using NETLAB, students can have an easier transition from studying IT concepts in school to getting some real hands-on experience, which they can use when they work in industry. A common example of simulations used in cybersecurity is phishing campaigns. It is one of the more common methods used within industry

to help employees understand what to look out for when encountering malicious-looking emails. A study conducted at a high education institution in Australia did a phishing campaign where students would be sent emails that contained fake links, and if they would click on them, then they would be sent to a site containing an educational phishing video created by a cybersecurity team. After conducting the study, it was found that "if individuals landed on the training page immediately after making a mistake, they would not behave similarly in the future" (Yeoh et al., 2021). This indicates that simulation-based training can be quite effective in teaching about phishing attacks.

Applications are also a means by which educational content can be spread and sometimes used within Social Engineering. "Training apps methods rely on the usage of software application training and learning modules to assess different types of social engineering threats," which is helpful given that people often use mobile devices. Lastly is the use of tournaments or competitions for training employees from companies. Within the context of cybersecurity, a typical application of tournaments is through Capture the Flag competitions to teach people how hackers use certain techniques and gain access to certain information. Specifically for Social Engineering, there is a special type of Capture the Flag competition called Social Engineering Capture the Flag (SECTF) (Social-Engineer, 2016). Within SECTF, participants of the competitions are given a target company that they will try to get information from through the use of Social Engineering techniques. This included using tools like Open Source Intelligence to enumerate the target. Within the competition, the participants were given a time slot from which they could do calls to the company and use Social Engineering techniques to get information from the employees that would answer the phone (Social-Engineer, 2016). In this manner, the participants are able to get an understanding of how Social Engineering attacks work from an attacker's perspective, and the receiving employees from the companies can get practice for how some Social Engineering tactics are used over the phone.

2.4 Methods used within this Research

Within the scope of this research, the types of teaching methods that were studied were text-based, gamification, and adversarial thinking. This was done to evaluate their effectiveness in teaching Social Engineering concepts. As mentioned in the previous section, gamification is one of the popular options for teaching concepts of Social Engineering. However, methods such as

text-based are one of the more basic options for spreading information on an online platform. While in comparison to Adversarial Thinking, which is a relatively newer concept used within teaching.

2.4.1 Text-Based

Text-Based information is seen everywhere on the internet as it is one of the primary forms of delivering information. However, when using text-based as a form of education, there are some concerns that can come up when the goal of using such a method is to increase the understanding of a person. For example, in online learning, information is just displayed on a screen that is not interactive with the users, which can cause a lack of interest in the content being taught. In a study conducted at Deakin University to compare teaching methods preferences for text-based, game-based, and video-based teaching methods on teaching security awareness concepts, it was found that participants preferred to use video-based learning over text-based because the delivery of content in text-based potentially caused the users to have a "lack of interest when presented with a document to read" (Abawajy, 2014) which is an issue because this does not guarantee that the content is actually retained. However, this same study also indicated that text-based learning was preferred over game-based learning because of how "clear, concise and easier to follow" the information was (Abawajy, 2014).

The preference results from the study done in Deakin University indicates that text-based teaching methods are preferred over other popular forms, and other studies support this. In an evaluation experiment conducted in Germany, computer-based training delivered over asynchronously on an Android device, text-based training, and instructor-based training were compared to see their overall effectiveness (Stockhardt et al., 2016). The effectiveness was measured by looking at the participant's ability to determine whether or not there were phishing URLs or legitimate URLs within post and pre-tests. The participant's understanding of phishing was based on these scores. Then once the participants were given the teaching portion of the experiment, the post-test helped to see how it improved the participants understanding of phishing concepts. "Interestingly, text-based training performs better than computer-based training" (Stockhardt et al., 2016).

Current research done with text-based teaching seems to have different results when using text-based, which can be a result of how the content is being conveyed. However, because text-

based seems to have some benefits with its simplicity and is used widely on the internet as a form of communicating information, it was included within this research to have as a baseline to compare with other methods.

2.4.2 Gamification

Generally, gamification can be defined as a "process of enhancing services with (motivational) affordance in order to invoke gameful experiences and further behavioral outcomes" (Hamari et al., 2014). However, when applied within the context of cyber security, it can be used as an interactive experience to teach concepts that can allow for behavioral change or more secure behavior from users. Gamification has been proposed as a newer method for learning concepts in cybersecurity because current training programs seem to be lacking from "engaging and authentic InfoSec training activities" (Nguyen & Pham, 2020). Hence, gamification is seen to be a good method to use in education because "Game approaches lead to a higher level of commitment and motivation of users to activities and process in which they are involved" (Angelova et al., 2014). In the context of cyber security, gamification can increase motivation for wanting to continue to learn more about the security concepts being taught and potentially allow the increased interaction with the material to cause a better understanding of the material.

Various studies have been done to test the performance and benefits of using game elements for education versus the traditional teacher or text-based approaches within the context of Social Engineering. One example is a study done at Iowa State University that compared the usage of gamification versus text-based to teach about identify theft which can occur through Social Engineering techniques (Helser, 2016). Students were randomly placed into an educational track in which students would be exposed to information about identity theft. The track determined whether the students received the content in either a text-based form or in a gamified form. The students were given a pre and post-survey to assess their knowledge of identity theft concepts. The results from the study showed that while text-based exposure did increase the student's knowledge, it was not as effective as gamification. Also, "it appears that the game-based delivery method engaged the students and held their interest in the topic more than text-based material" (Helser, 2016).

Another application of gamification is with one study conducted at North Carolina A&T State University. During this course, there were two groups used within this experiment. Within

one group, it contained students taught about cybersecurity concepts using a gamification platform called OneUp. In the control group, these students were not taught via a gamified platform. For those students using the OneUp platform, the students would have quizzes or challenges that they could take. The gamification elements came from adding features such as avatars, leaderboards, and progress bars (Demmese et al., 2020) onto the OneUp platform. Based on the number of challenges the students would do, they would receive certain badges within their profile to show their achievements. The results showed that those students using the gamification platform had "improved the median grade of students from B+ to A-" (Demmese et al., 2020) compared to those other students in the control group.

Various studies have been done on gamification and its effect on performance in learning. These studies have shown that using gamification can increase their motivation and immersion within the content to learn. Due to these factors, gamification was included in this research to evaluate its performance against the other methods.

2.4.3 Adversarial Thinking

Adversarial thinking can be defined as "thinking like a hacker" (Hamman & Hopkinson, 2016) but more specifically, "adversarial thinking is the ability to embody the technological capabilities, the unconventional perspectives, and the strategic reasoning of hackers" (Hamman & Hopkinson, 2016). This is often seen as an important skill to have within the context of cybersecurity. The reason is that if you can understand what an attacker might do, it can help you combat what you can anticipate will happen or at least know could potentially happen.

Very often, Adversarial Thinking is partnered with the ideas of game theory because it can be used to improve people's strategic ability. Strategic ability in the context of Adversarial Thinking refers to "the ability to anticipate the strategic actions of hackers, including where, when, and how they might attack, and their tactics for evading detection" (Hamman et al., 2017). Specifically, one study that used game theory in conjunction with adversarial thinking was that of a study done at Midwestern University where two groups of students were experimented on where one group acted as the defender and another group acted as the attacking group. The defense students were split into a group that was taught concepts about cybersecurity and game theory, while the control group did not. Afterward, the attack group would attack the defense group to determine if the lectures on game theory and adversarial thinking would help them combat against

the attacker group. The study showed that "the intervention subjects were able to more accurately predict the days the attackers chose after receiving the game theory instruction" (Hamman et al., 2017). This study indicates that through adversarial thinking it allowed for anticipation of attacks, which can be very impactful if used within industry because it can result in the stopping of various attacks.

One example of a tool created to assess how it can help adversarial thinking on students in cybersecurity is CyberAIMs. CyberAIMs is a simulation tool in which students can see actions that can be taken from both an attacker and a defender perspective in certain attack events (Zoto et al., 2018). The students are able to give certain values to indicate who the attacker could be, such as a script kiddy or a state actor. Similarly, the defense can also be chosen based on certain values representing defenders, such as a multinational corporation or a state agent. This simulation essentially allows the students to be able to decide whether or not they should attack a target or not and this is based on their adversarial thinking. From having an attackers perspective they can decide if it seems possible to successfully attack a defender based on their level of defense (Zoto et al., 2018). Based on post-surveys, it was found that the students felt that their understanding of adversarial thinking was improved. While this was only a pilot study, it shows some of the progress that has been made within the area of adversarial thinking used for cybersecurity education.

Since adversarial thinking has been shown to improve thinking like a hacker to better predict attacks, it was included within this research to further the research within this area since it shows promising results. Furthermore, suppose it can be used properly within education. In that case, it could lead to a better workforce prepared for anticipating attacks and aid in lessening the susceptibility to Social Engineering attacks since they will be able to think like a hacker and better understand what indicators of attacks they need to look out for.

2.5 Learning Theories

Within this research the three methods that were used to test effectiveness in teaching about Social Engineering were text based, gamification, and adversarial thinking. However, since these are teaching methods, they can also be connected to that of learning theories which can help us understand why these methods are actually usable as teaching methods. Each of these three teaching methods can be further understood under three different learning theories which are mastery learning, discovery learning, and experiential learning.

2.5.1 Mastery learning

Mastery learning is “a philosophically based approach” (Block & Burns, 1976) to learning and teaching where it is said that students are all able to learn well and can even master some subject under the appropriate conditions. This philosophy of learning can be connected to that of text based learning as a means to which people can achieve mastery of a subject. Mastery learning can be described as giving students a chance to show mastery of some content where in this case would be through the teaching material on Social Engineering concepts (Block & Burns, 1976). In online based learning, text-based learning follows this idea with online courses were information can be given to people in text form, they take their time to learn the material, and then their mastery level can be assessed through assessments. This understanding of the material, while can be measured by the scores of the assessments, it is really based on how much of the information that each person is able to understand and hence ‘master’. Hence text based learning is simply a form by which people can then approach the material in a learn for mastery manner.

2.5.2 Discovery Learning

Discovery learning is inquiry based and users can use the information given to them to try and solve problems (answering questions) and hence can get a better grasp of the material. Discovery learning has four main characteristics which are that the learning has “(1) motivation; stimulating interest and curiosity in learning; (2) structure; a knowledge structure and level that learners can best assimilate knowledge; (3) organization; find the best possible ways to present the material; and (4) consolidation; to make the best use of rewards and punishments for motivation” (Ozdem-Yilmaz & Bilican, 2020). Gamification can be used as a manner to provide a discovery learning approach to teach about a subject. Within gamification, the idea is to use elements of a serious game and adopt those elements into a non-game environment such as in teaching. The reason we want to use such serious game elements is that it gives the student a motivating manner by which they can learn a material without it being boring for them. Other elements that are used in gamification that follows discovery learning is that of the use of rewards which can be seen through the use of scoring or points upon being able to get something correct. This reward for learning also creates a motivating environment for which students would want to keep learning about a subject.

2.5.3 Experiential Learning

Experiential Learning concerns the idea that within learning each student has their own manner or experience for when they learn things. The components of experiential learning are that of “doing and having an experience, … concluding and learning from experience, … reviewing/reflecting on the experience, … planning and trying out what is learned” (Ozdem-Yilmaz & Bilican, 2020). Adversarial Thinking draws ideas from these components of experiential learning. Specifically, it draws on the reflection aspect of experiential learning, where individuals can develop their perspective about an experience and in this case, this would be learning to think as a hacker and then apply abstract thinking to reach conclusions about why it is that hackers do these sorts of attacks and why they are effective. Hence within this type of learning through adversarial thinking, people are not only learning about Social Engineering concepts but rather they are approaching it within a very different perspective where they can imagine themselves being the attacker.

2.6 Summary

As a general overview of all of the teaching methods used within this research, each method has its benefits for using them, but there are also some disadvantages that can arise from using such a teaching method. Firstly let's look at some of the previously mentioned advantages of using these methods for teaching. Studies showed that some prefer text-based learning because of its simplicity in conveying information. However, an issue with text-based is that its lack of interactive form of sharing information can cause people to want to skim or skip sections to finish the lessons. Hence, methods such as using gamification were created to enhance the interaction to learn new material and enable people to further immerse themselves in the material being taught. However, as seen from the previous studies mentioned for gamification, some individuals sometimes do not prefer it as the instructions of the material being conveyed are sometimes not clear. Lastly, adversarial thinking is a newer method applied within cybersecurity training programs to allow people to think like a hacker to anticipate attacks and better see attack indicators. Adversarial thinking seems to be one of the methods that could allow for a deeper understanding of combating cyberattacks and ultimately result in better defense against Social Engineering attacks.

Since these methods have been shown to have benefits for teaching cybersecurity concepts, they were used in this research to evaluate their effectiveness against one another. The importance of doing so is that in current times due to the increases in Social Engineering attacks, change is needed in Social Engineering education to decrease the total number of successful attacks. Ultimately, through this evaluation, we can better understand which methods are more effective than others for using in Social Engineering education.

CHAPTER 3. METHODS

This chapter will address the approach used to conduct the research and measure the effectiveness of different teaching methods in their application for Social Engineering teaching. The data collection will be described, and also the teaching method comparative methodology will be mentioned to address how the effectiveness of the teaching methods will be assessed.

3.1 Study Approach

This research focused on the three teaching methods of text-based, gamification, and adversarial thinking and their use in teaching Social Engineering concepts. To assess the effectiveness of the teaching methods, lessons were created to teach Social Engineering concepts within the context of Healthcare. As stated in the previous chapters, the context of this research is Healthcare as it is heavily targeted by hackers due to the value of patient information. Hence it was also included as a topic within the teaching materials created for this research.

The lessons themselves were created using the three teaching methods so that they contain the same teaching material but were expressed within their respective method. A detailed description of all the teaching materials created is in Appendix B. A pre and post assessment was also created based solely on the material that was taught within the teaching material created in this research, more of which is described in Appendix A. An additional section was also created with the consent form, purpose of the study, and IRB Protocol approval (#2021-1693) which is seen in Appendix C.

Qualtrics, which is an online survey software tool that can be used to host surveys online, was used to host the teaching materials, the pre and post assessments, consent form, and IRB Protocol approval in the form of a survey. This was made available to the participants using a link. Furthermore, Qualtrics has a functionality that allows you to create randomized assignments called the Randomizer, which was used to randomly assign participants to one of the three different teaching materials. In this manner, we can avoid systematic bias in favoring the outcome of one teaching method over the others by having more participants go into one teaching method group than the rest. Furthermore, Qualtrics has a functionality within the Randomizer that allows for the random assignments to be evenly presented to the participants, which was used. This means that

it can be used to try to mitigate an unbalanced design from occurring to try and get as close to an equal number of participants across all three of the teaching methods as possible.

For each of the treatment groups, the participants first read the consent form, which contained the IRB approval. If they agreed, they would answer some demographic questions followed by a pre assessment to determine their prior level of understanding of Social Engineering. Afterward, each participant completed lessons via one of the teaching methods depending on their specific random assignment to a treatment group. Once completing the lesson, the participants then took a post-assessment to see the effects of the lessons and determine whether the lessons were able to improve their scores from the pre to the post-assessment. Ultimately then to determine which teaching method had an overall better improvement on the scores of the participants. From the results, it was then possible to create a general conclusion about the effectiveness of each teaching method used for teaching Social Engineering concepts and hence determine which can be used in practice to lessen the susceptibility of people from falling victim to Social Engineering attacks.

3.2 Teaching Methods Assessment

Both a pre-test and post-test assessments were given to the participants to determine their prior and subsequent level of understanding of Social Engineering concepts. The questions of the assessment are described in detail in Appendix A.

The purpose of having a pre and post-assessment is to get an accurate understanding of what was the previous level of knowledge that participants had in Social Engineering. In this manner, we can then perform an individual comparison of the before and after results to get a more accurate representation of the changes caused by the teaching methods. In doing so, we can limit some bias from people who have any previous experience, knowledge in Social Engineering, or other individual lurking variables.

The pre and post test assessment questions were created using the content that was included within the teaching materials. The reason for doing this is that by ensuring that the content of the questions is solely from the teaching material, we can mitigate having some lurking variables present from having questions that are outside of the scope of the teaching material. In this manner, the participants will have the teaching material needed to be able to answer the questions asked. While the same content was used to create the pre and post test questions, the questions themselves

were not the same to ensure that there was no influence from participants memorizing the questions from the pre to post test. Hence we can avoid some lurking variables that could potentially cause for the true effect of the teaching methods to not be seen in the results.

As stated before, the teaching material was used to create the sets of questions used within the pre and the post test; more details on the actual teaching material will be explained in section 3.3. This was done by going through each of the main topics within the teaching material and picking out topics that pertained to issues such as indicators of attack, Social Engineering attacks, and what are some actions to take in case a user falls victim to an attack. Topics that were believed to be essential to identify attacks better and limit the effects of successful attacks were used to create the questions. This also added emphasis to these topics so that the participants could better remember them during and after having taken the lesson.

An additional two questions were also added to the pre and post assessment. These two added questions were added for the purpose of attention checks. These questions included the answer within itself. This was done so that students who answered these questions incorrectly could be removed from the study. This is important because answering these questions incorrectly means that they were most likely skimming through the teaching material and the questions to finish the survey. If these attention checks were not used and data from these students who were not paying close attention were included, this could cause the results to misrepresent the true effects of the teaching methods. Hence the attention checks helped with not having influences from lurking variables pertaining to attention.

3.3 Teaching Material Content

The three teaching methods explored in this research were text-based, gamification, and adversarial thinking. However, the content of the teaching material used within these teaching methods was the same to ensure that all teaching methods could be evaluated fairly by keeping the content consistent. This was done to ensure that differences in content would not inadvertently change the outcomes of post test scores of all teaching methods respectively. Since Healthcare is one of the most attractive industries for hackers, the content of the lessons and the assessments included examples of Social Engineering attacks within the context of Healthcare. Hackers utilize various attacks to get information about their target, but some of these often utilized attacks are “phishing, vishing, whaling, spear phishing, and impersonation” (Nguyen et al., 2021). Hence for

the purpose of this research, phishing, spear phishing, and impersonation attacks were used within the lessons as these are one of the most common attacks used in Healthcare.

When constructing these topics, a lot of time was taken to develop teaching material that could be presented to the public so that it could be understood by those who did not have any technical expertise. This was done through cybersecurity knowledge gained from coursework on the subject and on the insights from the literature review to develop the learning materials. For example, in section three on, 'What are some of the common attacks,' after having read that phishing, spear phishing, and impersonation attacks were common within the Healthcare industry (Choo at. el, 2021), they were added into that section. Pertinent insights about phishing reports were also used to inform the development of the teaching materials. This included reports from the FBI (2021) and Proof Point (2021) that reported that phishing attacks were commonly used, which further influenced the use of these attacks in the teaching material. In a similar manner, such tactics were used to develop the other sections of the teaching material to create the content that it has now.

The components of the teaching content are:

1. What is Social Engineering?
2. Why do hackers use Social Engineering attacks?
3. What are some of the common attacks?
    a. Phishing
    b. Spear Phishing
    c. Impersonation
4. Indicators of Attack.
5. What to do in the event that you are a victim of a Social Engineering attack.

More details of the material are located in Appendix B.

After having constructed the teaching materials, the materials were then expressed in the three teaching methods, respectively. Text based learning was expressed exactly the same as is seen in Appendix B. The differences in the methods can be seen at face value comparison between gamification and the adversarial thinking methods. For gamification, the same teaching material

was used as with text based, but with the addition of a gamification portion which was in the form of a Q&A style game created as a website. Screenshots of the website created can be found in Appendix B in the gamification section. The website itself contained gamification elements such as having a leaderboard section for all participants to enter a username of their choosing after having received a score from answering some or all of the Q&A questions correctly. These questions introduced within the website were also only from topics seen in the teaching material to ensure that the information being explained was consistent, and would have no effect on the participant's scores in the post test due to the scope of the teaching material. Other elements in gamification included a scoreboard to show their current score while playing, a progress bar to entail the participant how far they are in the questions, interactive user experience through having responsive buttons that would let the participants know if they answered a question correctly or not, and pop up messages. All of these elements categorized this website under gamification by adding game elements in a non-game context. Lastly, while the adversarial thinking section was presented in a text-based manner, the manner in which the topics were described were from the perspective of an attacker. For example, in the teaching material section about indicators of attack, in the text based section, this was explained as indicators of attack to look out for. However, in the adversarial thinking section, this same content was expressed by explaining the need for minimizing the number of obvious indicators of attack to ensure a higher chance of success, thereby providing the point of view of the attacker.

3.4 Sampling

For this research, a random sample was taken from Purdue Students at the West Lafayette campus from the College of Liberal Arts and from the College of Health and Human Sciences. The emails of students who were eighteen years and older were collected from these two colleges, and emails with the Qualtrics survey link were sent to all of these students so that they could participate in the study. A total of 3000 emails were sent, but at the end of the study, only 157 students participated in the study. From those students who did participate in the study, Qualtrics was only able to randomly assign those students who finished the pre test into the three treatment groups based on the three teaching methods. After data screening was conducted, there were only 80 students who remained in the dataset, with text based having 28 students, gamification having 22 students, and adversarial thinking having 30 students. While their sample sizes are not balanced,

they are relatively close to each other, which is preferred to have better interpretations of the individual group results since the power is not decreased too much from having an unbalanced design.

3.5 Validity & Reliability

To ensure face validity, the pre and post-assessment needed to be an obvious or logical way of evaluating understanding of Social Engineering concepts. In education, when assessments for some topic are done, this is conducted through some form of testing to quantify the knowledge that is understood. Similarly, for this research, this same approach was used. After taking a lesson on Social Engineering concepts using some teaching method, the participants took a post-test to measure their understanding improvement of Social Engineering concepts from the pre-test to the post-test. Hence in this manner, face validity was assessed. Furthermore, within the context of training programs, assessments within a study are commonly used to assess the effectiveness of training programs. This was also seen in some of the studies in the literature review that also used pre and post tests (Stockhardt et al., 2016).

Other considerations for threats to internal validity were also taken into account to ensure that the cause and effect relationship was valid and that inferences from the results would provide a better representation of the population. Firstly, random assignment was used in this research to combat systematic bias, which could occur in the assignment of participants into treatments groups. Secondly, testing, the pre-test, and the post-test were altered slightly so that the material asked was the same, but the tests were not identical. This was done to prevent the participants from memorizing the questions. In this manner, we can eliminate influences that the pre-test could have had on the post-test results.

Within the actual assessments created, validity checks were ensured by asking questions that contained attention checks. As mentioned before, these questions included the answers within them. In doing so, we could check whether the participant was paying attention when taking the assessments or was merely going through the material to finish the survey quickly. This is important because this could result in results that are not representative of the actual effects that the teaching methods can have on teaching Social Engineering concepts.

Regarding testing for reliability, given that the assessments were given to subjects, a practice run was needed to ensure that the assessments could provide reliable results. Hence, prior

to the actual test, a pilot study was conducted to ensure that the data collection instruments, which was Qualtrics, would work properly and give us consistent results. The pilot study worked well, and the results were as expected based on insights from the literature.

CHAPTER 4. DATA ANALYSIS & RESULTS

This chapter provides an overview of the data screening procedures, the descriptive statistics of the sample, the statistical methods used, and the results of the data analysis. A summary of all the results is provided at the end of the chapter.

4.1 Data Screening

From the sample of Purdue Students, a total of 157 responses were initially collected before data screening. During data screening, a total of 37 responses were deleted because they contained empty responses from participants who had never started or partially started but never finished. Afterward, an additional 39 responses were removed from participants who did not answer the attention check questions correctly. The purpose of having these attention checks was to ensure that there were no lurking variables from a lack of attention that would cause results that were not indicative of the true effects of the teaching methods. One low outlier was also removed, which was found to be in the adversarial thinking group post scores. Prior to removing it, the One Way ANOVA was run with the outlier, and the results stayed the same with or without it; hence, it was removed to better the normality assumption. As a result, this left only 80 responses to be used to perform analysis.

4.2 Validity and Reliability of Questions

To further check the validity of the questions being asked within the assessments, a principal components analysis was done using all the items from both the pre and post test across the data collected from the sample to ensure that the questions were in fact, good questions to use to measure the knowledge of Social Engineering that individuals have. With the sample, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy resulted in a value of 0.69, which is an acceptable value as the recommended value is 0.50. This tells us that the questions were good questions to measure the knowledge of Social Engineering Concepts.

Furthermore, internal consistency for the questions of the assessments was done using the Cronbach's Alpha to ensure that we would be receiving consistent responses when using the questions from the assessments. Similarly, to that for validity, after data was collected, the test was

done to check that reliability was ensured with the questions in the assessments. The student sample had a Cronbach's Alpha value of 0.73, which is an acceptable value as a range of 0.70-0.80 gives us an acceptable reliability value. Hence this tells us that the questions used had good reliability.

4.3 Descriptive Statistics

For the Purdue Student sample, at the beginning of the Qualtrics survey, there were some demographic questions that were asked. These included questions regarding age, college, major, and school year for each of the students. The students were composed mainly of ages ranging from 18 to 23 years old (n = 79, 98.9%). Most of the students were also from the Health and Human Sciences College (n = 62, 77.5%). The major with the most students were from the Psychology major (n = 12, 15%). The students were also composed mainly of Freshmen students (n = 24, 30.0%). A detailed breakdown of the sample based on the demographic questions can be found in Table 4.1.

Table 4.1 Purdue Student Demographics Based on Teaching Methods

Variable	Text-Based (*n* = 28)	Gamification (*n* = 22)	Adv. Thinking (n = 30)	Total (*N = 80*)
Age (yrs)				
18-19	12 (42.9)	8 (36.4)	13 (43.3)	33 (41.3)
20-21	10 (35.8)	11 (50)	11 (36.6)	32 (40.0)
22-23	6 (21.4)	2 (9.1)	6 (20)	14 (17.6)
24 and above	0	1 (4.5)	0	1 (1.3)
College				
Liberal Arts	7 (25.0)	6 (37.3)	5 (16.7)	18 (22.5)
Health and Human Sciences	21 (75.0)	16 (72.7)	25 (83.3)	62 (77.5)
Major				
Biomedical Health Sciences	2 (7.1)	1 (4.5)	1 (3.3)	4 (5.0)
Brain and Behavioral Science	2 (7.1)	1 (4.5)	3 (10.0)	6 (7.5)
Business Communication	1 (3.6)	0	0	1 (1.3)
Developmental & Family Studies	0	1 (4.5)	0	1 (1.3)
English	1 (3.6)	0	1 (3.3)	2 (2.5)
Film	2 (7.1)	0	1 (3.3)	3 (3.8)
Graphic Design	0	1 (4.5)	0	1 (1.3)
Health Sciences	0	0	2 (6.7)	2 (2.5)

Table 4.1 continued

History	1 (3.6)	2 (9.1)	1 (3.3)	4 (5.0)
Hospitality & Tourism	0	1 (4.5)	1 (3.3)	2 (2.5)
Human Services	1 (3.6)	0	1 (3.3)	2 (2.5)
Interior Design	0	1 (4.5)	0	1 (1.3)
Kinesiology	6 (21.4)	3 (13.6)	2 (6.7)	11 (13.8)
Mass Communication	0	0	1 (3.3)	1 (1.3)
Medical Laboratory	1 (3.6)	0	3 (10.0)	4 (5.0)
Nursing	0	2 (9.1)	4 (13.3)	6 (7.5)
Nutrition	0	1 (4.5)	0	1 (1.3)
Political Science	1 (3.6)	1 (4.5)	0	2 (2.5)
Professional Writing	1 (3.6)	0	0	1 (1.3)
Psychology	5 (17.9)	1 (4.5)	6 (20.0)	12 (15.0)
Public Health	0	1 (4.5)	1 (3.3)	2 (2.5)
Radiological Health	1 (3.6)	0	0	1 (1.3)
Retail Management	0	1 (4.5)	0	1 (1.3)
Selling & Sales	1 (3.6)	2 (9.1)	0	3 (3.8)
Sociology	0	1 (4.5)	0	1 (1.3)
Speech, Language, & Hearing	2 (7.1)	1 (4.5)	1 (3.3)	4 (5.0)
Visual Communication Design	0	0	1 (3.3)	1 (1.3)
School Year				
Freshman	9 (32.1)	6 (27.3)	9 (30.0)	24 (30.0)
Sophomore	8 (28.6)	8 (36.4)	6 (20.0)	22 (27.5)
Junior	5 (17.9)	4 (18.2)	7 (23.3)	16 (20.0)
Senior	6 (21.4)	4 (18.2)	7 (23.3)	17 (21.3)
Does Not Apply	0	0	1 (3.3)	1 (1.3)

Note. Values represent frequencies with percentages in parentheses. Valid *N = 80*

4.4 Analytical Strategies

When constructing the experiment, the design of the experiment was created as a Matched Pair Design (MPD) with the added randomization so that each participant would be randomly assigned to a certain training method. Hence there would be three different groups that follow the Matched Pair Design, so that we could test the before and after of having taken a lesson based on the difference in the pre and post test scores across the different teaching methods. Since the participants took a pre and post test, these are two measures from the same individual, and this

follows the idea of a Matched Pair Design which tells us that this is an appropriate statistical design to use for analysis. To be able to then look at their improvement, one way would be to analyze their improvement by using a paired t test as we are looking at the improvement in the individual's scores from the pre to the post test for that same subject. Hence, a one-tailed paired t test was used across all the teaching method groups to detect which teaching method resulted in the most significant improvement in scores from before to after having taken a certain lesson based on a specific teaching method. A One Way ANOVA with a follow up Tukey test was also conducted on the post scores to make a comparison across the scores to determine which would be significantly better at teaching Social Engineering concepts. The reason for using the Tukey test as the post-up test is because it is the better method when needing to conduct all pairwise comparisons, which we are doing here by comparing all the teaching methods against each other. Another benefit of using this follow-up test is that it controls the Type I error rate or the rate in having a false-positive.

4.5 Analysis Results

Before beginning the actual paired t tests across all the samples, some tests were conducted to ensure that the assumptions for the paired t tests were passed. For the paired t test, the assumptions that needed to be passed were the normality of the difference distribution from the pre to the post test, the independence of data, and no outliers in the difference distribution of the post and pre tests. Also prior to conducting the paired t test analysis of the pre and post scores, the statistical description of the scores from both tests was investigated. It was found that the mean pre scores were 7.25 for text based (M = 7.25), 7.27 for gamification (M = 7.27), and 7.27 for adversarial thinking (M = 7.27). In comparison, the means of the post scores were 8.04 for text based (M = 8.04), 7.68 for gamification (M = 7.68), and 8.87 for adversarial thinking (M = 8.87). By looking at these means, we can begin to see that adversarial thinking had a much higher mean score than the rest of the teaching methods for the post scores. Also, the initial mean values from the pre test were not that different from each other, which indicates that, on average, they all had a similar level of Social Engineering understanding. A clustered boxplot for both pre test and post test was created to visualize the distributions of scores for each teaching method. This can be found in Figure 4.1; The values that are indicated as outliers in the clustered boxplots were still within

the acceptable range of values for pre and post test scores, and are not outliers within their respective test scores distribution.

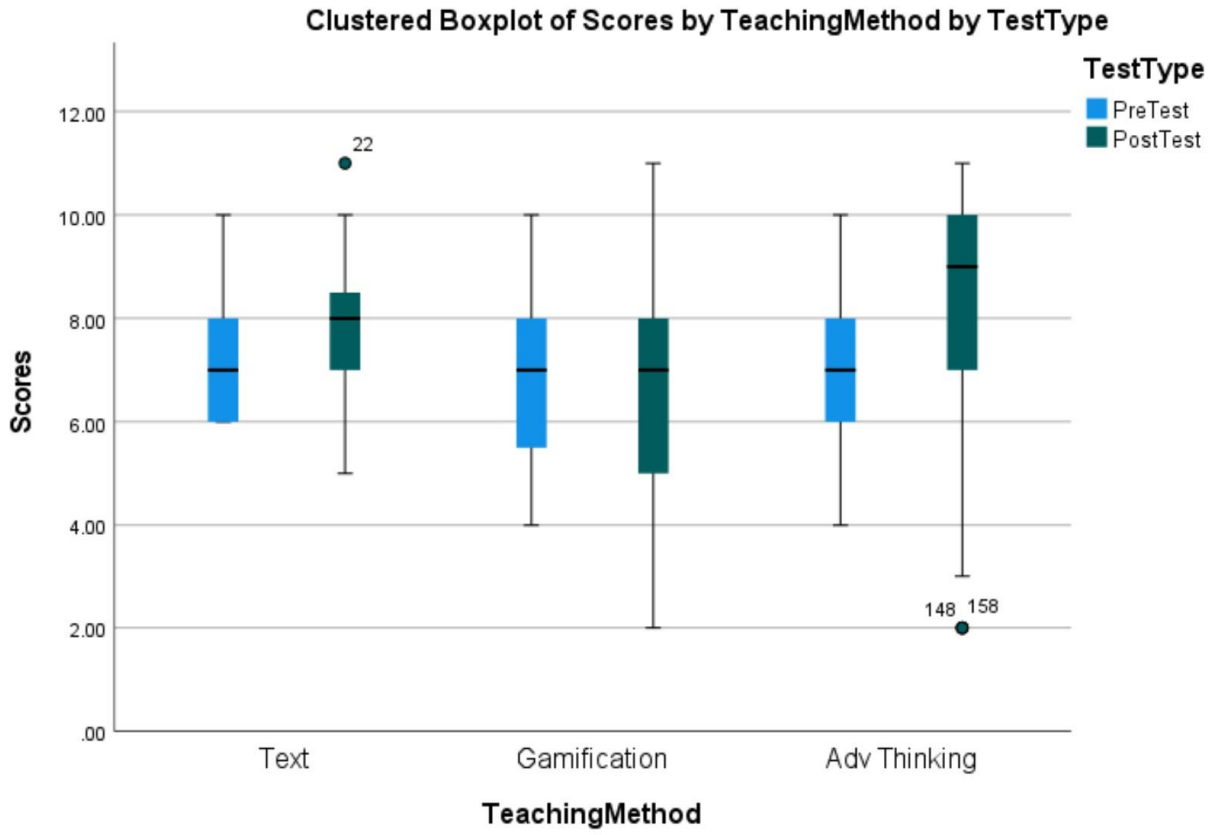


Figure 4.1: Comparison of Pre and Post Test Scores

The differences were computed by calculating the post test minus the pre test scores for the Purdue students sample. (*Difference = post test – pre test*) The reason for doing this is that by making this the difference, we can see if there is an improvement in the scores by seeing if the difference mean is a positive number or a negative number which will tell us the effect of the teaching methods. Now when looking at their difference distribution across all the teaching method samples, it was found that based on the QQplots from each of the samples, they were all normally distributed as they followed a linear pattern. The QQplots for the three different teaching method's difference distributions can be seen in Figure 4.2, Figure 4.3, and Figure 4.4, respectively below.

Normal Q-Q Plots

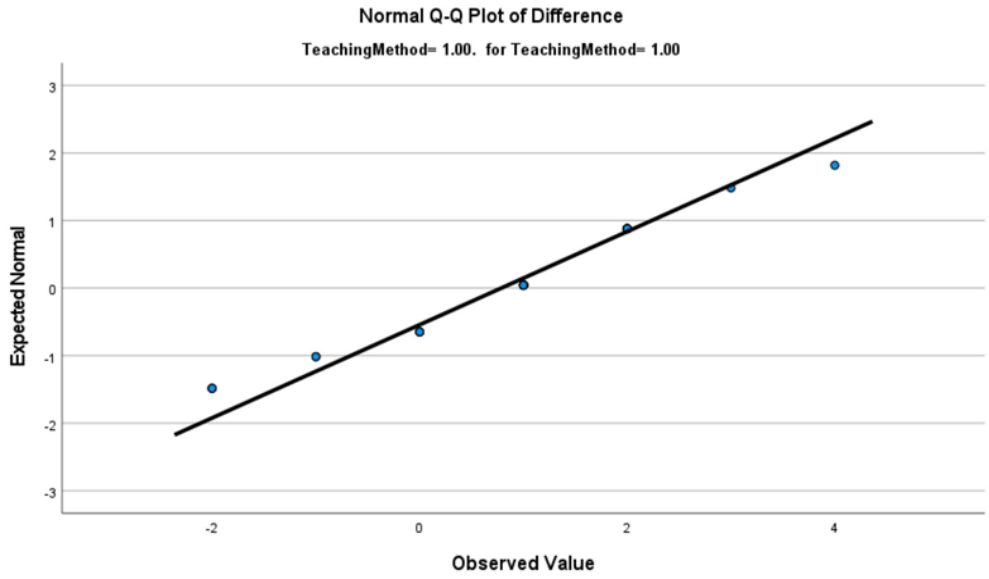


Figure 4.2: Text Based Difference Distribution QQplot

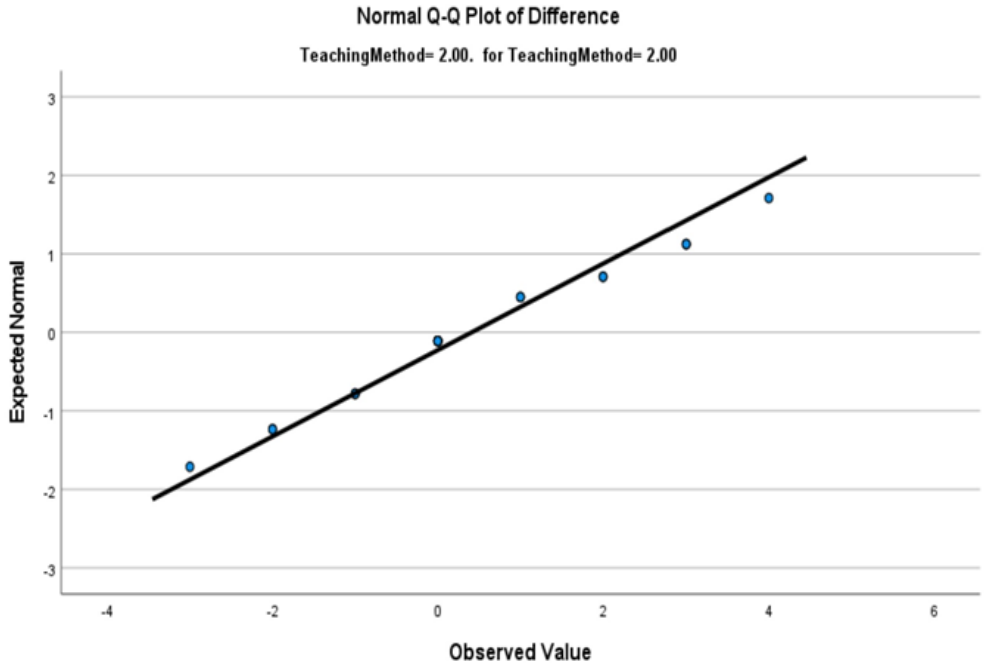


Figure 4.3: Gamification Difference Distribution QQplot

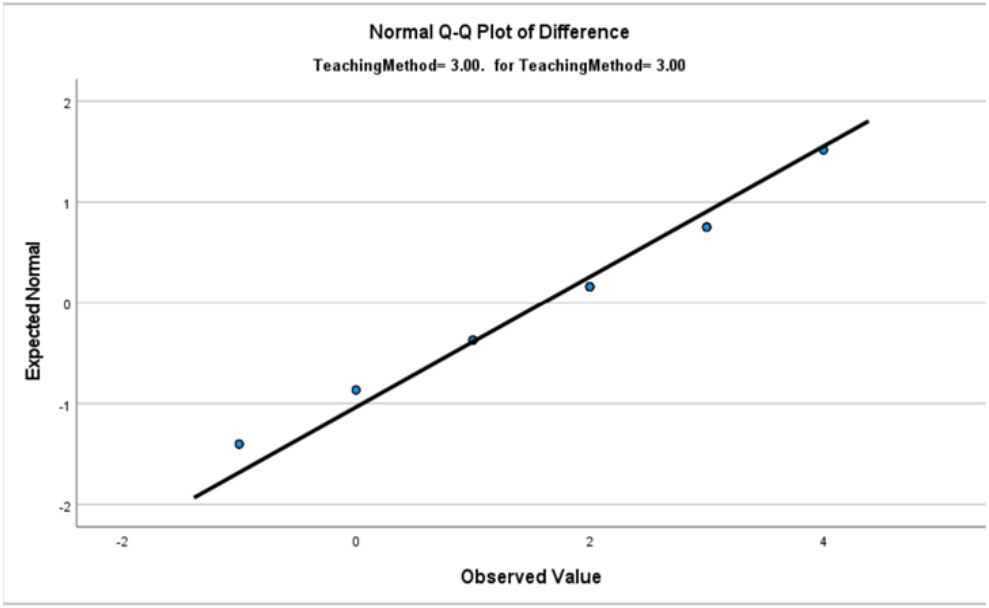


Figure 4.4: Adversarial Thinking Difference Distribution QQplot

Secondly, it was found that in the difference distributions, there were no outliers. Lastly, for the independence assumption, since the participants were randomly assigned to a teaching method, then we can pass this assumption as each participant is independent of the other participants. Now that the assumptions have been addressed for the one-tailed paired t test, we can continue doing the test across all teaching methods. For each of the one-tailed paired t tests, an alpha level of 0.05 was used to determine the significance of the results. If the p-value found was less than the alpha level, and the mean difference was positive, we would say there was a significant improvement in the scores, which indicates there was learning gain from the pre to the post test.

Alternative Hypothesis for the paired t test: There is a significant improvement in the scores from the pre to the post test after having taken one of the lessons using one of the three teaching methods ($\boldsymbol{H_A}$: $\boldsymbol{\mu_d > 0}$ where diff=post-pre)

Null Hypothesis for the paired t test: There is no significant improvement in the scores from the pre to the post test after having taken one of the lessons using one of three teaching methods ($\boldsymbol{H_0}$: $\boldsymbol{\mu_d = 0}$ where diff=post-pre).

The one-tailed paired sample t test revealed that on average, participants who were in the text based group showed improvement (M = .79, SD = 1.45) from the pre to post test scores. The results of this test were found to be statistically significant (t = 2.87, p = .004). This tells us that text based was able to significantly improve the understanding of Social Engineering concepts in the participants from that group.

The results also revealed that on average, participants who took the gamification lesson showed no significant improvement (M = .41, SD = 1.82) in the scores from the pre test to the post test (t = 1.06, p = .15). This tells us that there was no significant effect of gamification in aiding people in learning about the Social Engineering concepts.

Lastly, the test revealed that on average, participants showed significant improvement (M = 1.60, SD = 1.54) from the pre to post scores from those that took the adversarial thinking lesson. The results of this test were found to be statistically significant (t = 5.67, p < .001). This tells us that adversarial thinking was able to significantly improve the understanding of Social Engineering concepts in the participants. The results are summarized in Table 4.2.

Table 4.2 Paired T test for Purdue Students

	Teaching Method	*M*	*SD*	*t*
Pair 1	Text Based	.79	1.45	2.87*
Pair 2	Gamification	.41	1.82	1.06
Pair 3	Adversarial Thinking	1.60	1.54	5.67**

* p < .05, ** p < .001, one-tailed

Note. Difference = Post Test - Pre Test

To further compare the difference among the teaching methods to determine if there is one that is significantly different from the rest, a One Way ANOVA using the Tukey method was also used to assess the differences in the post scores. Before conducting the One Way ANOVA, the assumptions for this test were checked. These assumptions include a normal distribution in the post scores, an equal variance, and independence. After having checked the normality of the post score data using a QQplot, it was found to be approximately normal as it followed a linear pattern. This can be seen in Figure 4.5 below.

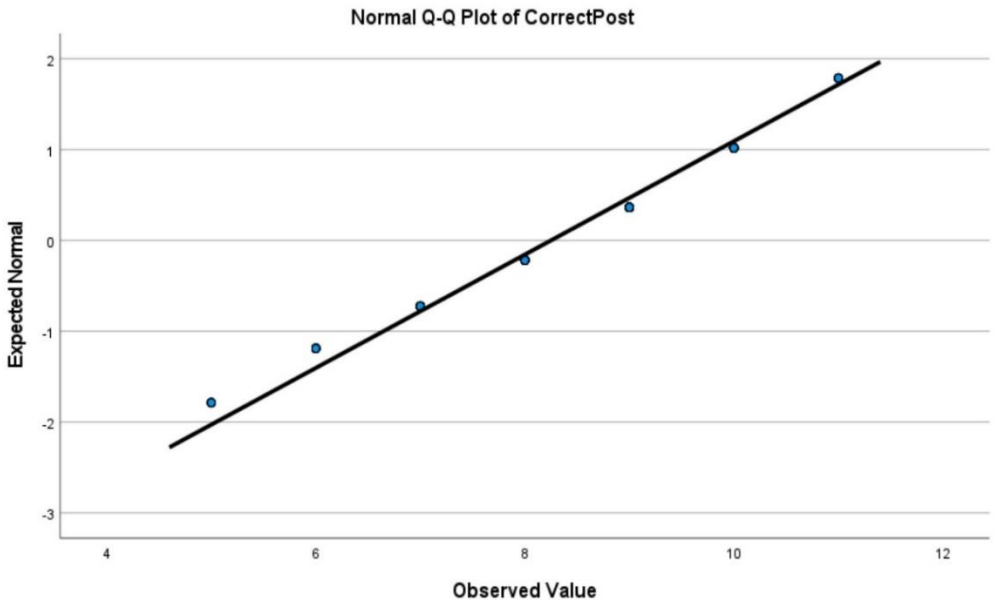


Figure 4.5: Post Scores QQplot

To address the assumption of equal variance, a Lavene's test was conducted. The test resulted in a significant value of 0.64 which is greater than 0.05 which tells us that the sample has an equal variance. Lastly, for the independence assumption, since the participants were randomly assigned to a teaching method, we pass this assumption as each participant is independent of the other participants. Hence we can continue with the One Way ANOVA test.

After running the One Way ANOVA, we find that there is significant evidence that at least one of the group means is significantly different from the other $F(2, 77) = 4.16$, $p = .02$. The post Tukey test showed a significant difference between Adversarial Thinking and Gamification *CI* 95% [0.15, 2.22]. This indicates that Adversarial Thinking ($M = 8.87$, $SE = 0.28$) had a much higher mean score than Gamification ($M = 7.68$, $SE = 0.33$), as seen from the mean values where the mean post score of Adversarial Thinking is larger. It also showed that there was no significant difference between Text Based and Gamification *CI* 95% [-0.70, 1.40] and that there was not a significant difference between Text-Based and Adversarial Thinking *CI* 95% [-1.80, 0.14]. The results from the ANOVA are summarized in Table 4.3 and for the Tukey in Table 4.4.

Table 4.3 One Way ANOVA

Results of One Way ANOVA

Factors	*df*	MS	*F*	*p*
Treatments	2	9.90	4.16	0.02
Error	77	2.38		
Corrected Total	79			

Table 4.4: Tukey Results

Results of One Way ANOVA Follow Up Tukey

Group Comparison	*Difference Between Means*	95% Confidence Limits		
3 - 1	0.83	-0.14	1.80	
3 - 2	1.19	0.15	2.22	***
1 - 3	-0.83	-1.80	0.14	
1 - 2	0.35	-0.70	1.40	
2 - 3	-1.19	-2.22	-0.15	***
2 - 1	-0.35	-1.40	0.70	

Note: Text Based = 1 , Gamification = 2 , Adversarial Thinking = 3

4.6 Summary Results

Hypothesis: Adversarial thinking is a better method by which Social Engineering concepts can be taught as it gives people an understanding of how to think like an attacker.

The initial hypothesis when first starting this study was that Adversarial Thinking would be the most effective teaching method because of how you are able to think like the attacker and have a good understanding of why it is that certain techniques are used to do certain Social Engineering attacks. However, with the tests used in this study, it was not found that Adversarial Thinking was the better method. The results of the paired t tests showed that Adversarial Thinking and Text Based learning significantly improved the learning gains of the students. The results from the One Way ANOVA indicated that there was a significant difference among the means of the post scores for all the treatments. From the post hoc Tukey test, we find a significant difference between Adversarial Thinking and Gamification based on looking at the means for each group. It

was also found that there was no significant difference between Text based and Gamification and no significant difference between Adversarial Thinking and Text based learning.

Interestingly, the results from the paired t test and the results from the One Way ANOVA were slightly different from each other. In the paired t test we find that Adversarial Thinking and Text Based showed significant improvement while Gamification did not. In the One Way ANOVA we find that Text Based is both grouped with Adversarial Thinking and Gamification. While it makes sense that Text Based and Adversarial Thinking would be grouped since they both showed significant improvement in the scores, Text Based and Gamification initially were not so clear as to why they were grouped together. One thing to consider is that when conducting the paired t test, we can control for a lot of the individual variability that can be present from things such as past experience or prior knowledge. In contrast, in the use of the One Way ANOVA, we are only looking at the post scores and not considering the initial base level understanding that each student had in Social Engineering concepts. Hence this can be one speculation for why these results were slightly different. Another thing to consider is that while the methods used were appropriate methods to conduct analysis, the power was not that large since the sample size for the students was small. Hence, another reason for these differences in both methods could be because of a power issue, and if we were to have had more power, perhaps the results would not have been different from each other.

Hence based on these results, we fail to find enough evidence to say that Adversarial Thinking is the better method. That being said, that does not mean that Adversarial Thinking is not a good method since, based on the paired t test results, Adversarial Thinking did show significant improvement in the students' scores from the pre to the post test. This tells us that it is a method that can be used to show improvement in understanding Social Engineering concepts.

CHAPTER 5. CONCLUSION AND FUTURE WORK

This chapter provides an overview of the limitations of this study, the conclusion, and the direction for future research.

5.1 Initial Hypothesis

After analyzing the student data, it was found that the initial hypothesis of this study was not proven to be true. However, there was enough evidence to support that while adversarial thinking was not the best method, it was an effective method as it showed improvement in the student's scores from the pre to the post-test.

5.2 Limitations

At the beginning of this study, the aim was to be able to test these teaching methods in person. Given that Healthcare is the most attractive industry for attackers, the initial intention was to be able to test these training methods with medical staff. However, given the circumstances of COVID-19, that was not feasible. Instead, a convenience sample was taken from Purdue students to conduct an online study. The Purdue students sampled for this study came from the Colleges of Liberal Arts and Health and Human Sciences. While they were not people working in industries such as Healthcare, they are representative of the target population because they are people who work with technology. Another limitation of using this convenience sample is that we must rely on the generalizability of these tests to determine whether these results will be truly effective across various industries. However, the population of interest is that of adults who use technology such as computers as they are all susceptible to Social Engineering attacks and hence the Purdue students can still be used to generalize the results and make some inferences for how the teaching methods would be able to affect people within the industry. This, of course, is by ensuring that the statistical methods can give good results, which we ensured by checking the assumptions for the methods used. Lastly, another limitation is that of having a small sample size. While the sample size was not as large as initially wanted, given that assumptions checks were met prior to analysis, those results can be used to interpret the effects of the teaching methods.

5.3 Discussion

Once all of the results were found, some of the findings were rather unexpected, compared to the hypothesis made from literature review insights. From the findings, only two methods were found to be effective, which were text based and adversarial thinking. What was rather unexpected was the fact that gamification was not a method that showed significant improvement in the scores for understanding Social Engineering concepts. This was found to be unexpected because, based on some of the studies mentioned within the literature review, gamification was a method that was found to help improve scores among students. Furthermore, one study actually did a very similar gamification program in the form of a Q&A style similar to that of the one used within this study (Helser, 2016). One difference was that their gamification component seemed to be more interactive based on screenshots that were seen. This then brings to question how two programs that fall under gamification can show significant differences in improvement. One speculation for the gamification results in this study is that while the classification of gamification can be met by simply having gaming elements in a non-game context, the manner in which the elements are used can cause differences in the program's effectiveness. Essentially, there are many variables to consider within the creation of a gamification program. Furthermore, there are a number of considerations that need to be accounted for when creating a truly effective gamification component, such as player knowledge, attention, aesthetics, and human-computer interaction elements. This is where more research needs to be done within gamification to identify or establish a set of criteria to indicate when a certain gamification program can be effective based on meeting said criteria.

After having found that two methods were effective within the paired t test results, the One Way ANOVA was used to determine if a single method could be found to be the better one based on the post scores of the students. However, a single best method was not found based on the results. This was also unexpected, given that within adversarial thinking, the student can think like an attacker and hence allows them to better understand what tactics are used within an attack. In this manner, they know what an attacker will do and hence be able to detect those tactics better to ultimately not fall victim to an attack. From this line of reasoning, and supported by insights from the literature review, it was expected to perform very well compared to the other learning methods. However, while it was effective in showing improvement, adversarial thinking was not significantly different from text-based. This was interesting because text based is the most

common manner of sending information on the web. Since it is so commonly used, it was not initially believed to be that effective. However, some insights from literature showed that text based was preferred over other teaching methods such as gamification, due to its simplistic nature (Abawajy, 2014). Hence text based was believed to be more helpful in understanding Social Engineering concepts due to familiarity with this teaching style. These results from the cited study also follow the results found in this study as text based was able to perform better than gamification did.

These two methods have their own benefits in explaining information and hence both resulted in showing significant improvement in the understanding of Social Engineering concepts. Ultimately based on aspects of adversarial thinking such as making someone think like an attacker and aspects of text based such as being simplistic, it made sense why these methods were effective. This could also be why there was no significant difference found within these methods, as they both help understanding in their own ways.

5.4 Conclusion and Future Work

Based on the results from all of the paired t tests conducted, we find that text based and adversarial thinking showed significant improvement in learning about Social Engineering concepts in the Purdue student sample. This is very insightful because not only did this research showcase that adversarial thinking can be an effective method, but that adversarial thinking can be an effective method to use to help people recognize Social Engineering attack indicators and ultimately help to lower the number of successful Social Engineering attacks across various industries. Regarding academia, this study demonstrates that adversarial thinking is an effective method to use to teach about Social Engineering concepts and this is important because adversarial thinking as a method still does not have a lot of research to back up its effectiveness. Since it is still very new as a teaching method this is another study that can now be used to show that adversarial thinking is in fact a good teaching method and should be studied more.

Another finding that was made was that text-based learning is still effective as a teaching method and is still better than gamification, as seen in this study. Now similar research was done and also found similar results which was mentioned in the previous section. However, as previously discussed, other research found that gamification was an effective teaching method. It was also discussed previously that further research needs to be done on finding a set of criteria

that, if met, would be a good indicator if a program would more likely be effective or not. If such criteria could be found, then it could improve the effectiveness of gamification programs so that as more gamification programs are created, they will more likely be able to show improvement in the understanding of Social Engineering concepts.

Based on the results founds, both adversarial thinking and text based learning also have implications for how they can be used within industries such as Healthcare. As stated earlier within this study, all industries face problems from Social Engineering attacks, but the more popular industry for attackers is the Healthcare industry. After finding that both text based and adversarial thinking can be used to teach Social Engineering concepts, these can also be used to create training programs for industries so that employees are not so susceptible to attacks. This matters because by being able to teach people within industries Social Engineering concepts, they become less susceptible to attacks and hence reduce the total number of successful Social Engineering attacks. The overall benefits of these methods can vary as it depends on what sort of attacks the hackers use, such as a phishing email or a phishing email containing malware to make an attack. However, there are some apparent benefits. For example, within Healthcare, having effective training programs is essential because there is a lot of private patient information that is attractive to hackers. Being able to train healthcare employees with Social Engineering concepts can decrease the success rate for hackers in using Social Engineering attacks as employees would be trained to look out for certain indicators of attacks. Furthermore, since Social Engineering is the easiest hacking method to use, this also means that this vector of attack will become much harder for hackers to implement. This also implies that it will make it even harder for hackers to attain the data that they want because they will need to acquire more advanced skills to perform successful attacks. Ultimately by using text based and adversarial thinking to create training programs, it could result in less probability of attackers being successful, which means that the Healthcare industry is more likely to avoid harm caused by monetary loss, identity theft, fake medical claims, and other fraudulent activities.

This study has some other advantages, and that is from how this study has developed a method that can be transferrable to other industries. Since healthcare is the most commonly attacked industry, it was added to the teaching material to showcase examples of such attacks within this research. However, the method created can be applied to other industries as well by changing the Social Engineering attack examples to add a different context. Since all industries

face issues with Social Engineering attacks, the main topics from the teaching material can be used as it applies to all industries. Furthermore, having created this teaching material that is written for the general public and uses language that can be understood by those who do not have technical expertise makes it easier to transfer to other industries.

Ultimately the importance of this study is that not only were two methods found that can be used to create effective training programs, but also the methodology created can be applied to different industries to aid in lessening the total number of successful Social Engineering attacks across all industries. This study has also added to the previously done research by having made comparisons across three teaching methods. In doing so now, there is further evidence that showcases how text-based and adversarial thinking are good methods to use for teaching and also why further research needs to be done with gamification.

The findings from this study have also opened avenues for possible future works within the area of Social Engineering training programs and teaching methods. One such work would be to apply the methods used within this study in an in-person setting to determine if there is a difference between having teaching material taught in-person versus online teaching. Another study can be done is solely with gamification to find a set of criteria needed to better determine whether a gamification training program would be effective or not. Also comparison across a larger set of teaching methods can be done to determine how teaching methods perform against each other to find other potential effective methods for creating training programs. Lastly, a future work that was initially considered for this study was to include other forms of attacks commonly used to see how many different attacks can be learned by people to combat even more forms of Social Engineering attacks.

REFERENCES

Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. *Journal of medical Internet research*, *22*(5), e18394. https://www.jmir.org/2020/5/e18394

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Aldawood, H., & Skinner, G. (2019, January). An academic review of current industrial and commercial cyber security social engineering solutions. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 110-115). https://doi.org/10.1145/3309074.3309083

Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again - Check Point Software. (2021). Retrieved from https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

Block, James H., and Robert B. Burns. "Mastery Learning." Review of Research in Education, vol. 4, [Sage Publications, Inc., American Educational Research Association], 1976, pp. 3–49, https://doi.org/10.2307/1167112.

Brownlet, K. *Biggest Healthcare Breaches of 2020 - The Top 10 and Why They Matter - Gov Health IT*. (2020). Retrieved October 8, 2021, from https://www.govhealthit.com/biggest-healthcare-breaches-of-2020-the-top-10-and-why-they-matter/

Choo, K. K. R., Morris, T., Peterson, G., & Imsand, E. National Cyber Summit (NCS) Research Track 2021.https://doi.org/10.1007/978-3-030-84614-5

What is a denial-of-service (DoS) attack? (n.d.) Cloudflare. Retrived from *https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/*

Crichigno, J., Ahmed, S., Gerdes, J., & Brookshire, R. (2019, June). Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances. In *ASEE annual conference & exposition*. https://par.nsf.gov/biblio/10112157

Demmese, F., Yuan, X., & Dicheva, D. (2020). Evaluating the Effectiveness of Gamification on Students' Performance in a Cybersecurity Course. *Journal of The Colloquium for Information Systems Security Education*, *8*(1), 6–6. http://cisse.info/journal/index.php/cisse/article/view/129

Davis, J. *FBI, HHS Alert to COVID-19 Vaccine Fraud Schemes Aimed at Data Theft*. (2020). Retrieved October 8, 2021, from https://healthitsecurity.com/news/fbi-hhs-alert-to-covid-19-vaccine-fraud-schemes-aimed-at-data-theft

Davis, J. *Feds Warn of TrickBot Spear-Phishing Attacks Delivering Malware Payload*. (2021). Retrieved October 8, 2021, from https://healthitsecurity.com/news/feds-warn-of-trickbot-spear-phishing-attacks-delivering-malware-payload

Dunham, K. (2004). Phishing isn't so sophisticated: Scary! *Information Systems Security, 13(2), 2-7.* *https://www.proquest.com/scholarly-journals/phishing-isnt-so-sophisticated-scary/docview/229544693/se-2?accountid=13360*

Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas'ud, M. Z. (2011, November). Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In *Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor*. https://www.icact.org/upload/2012/0452/20120452_finalpaper.pdf

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3). https://doi.org/10.1001/jamanetworkopen.2019.0393

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences* (pp. 3025-3034). IEEE. https://doi.org/10.1109/HICSS.2014.377

Hamman, S. T., & Hopkinson, K. M. (2016). Teaching Adversarial Thinking for Cybersecurity. *Journal of The Colloquium for Information Systems Security Education*, *4*(1), 19–19. https://cisse.info/journal/index.php/cisse/article/view/56

Hamman, S. T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M., & Metzler, G. E. (2017). Teaching game theory to improve adversarial thinking in cybersecurity students. *IEEE Transactions on Education*, *60*(3), 205-211. https://doi.org/10.1109/TE.2016.2636125

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Helser, S. (2015, November). FIT: Identity theft education: Study of text-based versus game-based learning. In *2015 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-4). IEEE. https://doi.org/10.1109/ISTAS.2015.7439437

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

Householder D. A. (2002). CERT Incident Note IN-2002-03. *CERT*. Retrived from https://artofhacking.com/tucops3/etc/wetware/live/aoh_in200203.htm

Imarc. (2017). Petya Ransomware Attack: A Wake Up Call. *Security Scorecard*. https://securityscorecard.com/blog/petya-ransomware-attack-wake-call

IC3 Logs 6 Million Complaints. (2021). FBI. Retrived from https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721

JA, Ashiq. Hackers Selling Healthcare Data in the Black Market. *Infosec Resources*. (2015). Retrieved October 10, 2021, from https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

Kiryakova, G., Angelova, N., & Yordanova, L. (2014). Gamification in education. Proceedings of 9th International Balkan Education and Science Conference.

Landers, R. N. (2014). Developing a Theory of Gamified Learning: Linking Serious Games and Gamification of Learning. *Simulation & Gaming*, *45*(6), 752–768. https://doi.org/10.1177/1046878114563660

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014, July). Towards an ontological model defining the social engineering domain. In *IFIP International Conference on Human Choice and Computers* (pp. 266-279). Springer, Berlin, Heidelberg.

Nguyen, T. A., & Pham, H. (2020). A Design Theory-Based Gamification Approach for Information Security Training. *Proceedings - 2020 RIVF International Conference on Computing and Communication Technologies, RIVF 2020*. https://doi.org/10.1109/RIVF48685.2020.9140730

Nguyen, C., Williams, W., Didlake, B., Mitchell, D., McGinnis, J., & Dasgupta, D. (2021, June). Social Engineering Attacks in Healthcare Systems: A Survey. In *National Cyber Summit* (pp. 141-150). Springer, Cham.2021 State of the Phish Report. (2021). *Proof Point.* Retrived from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Ozdem-Yilmaz Y., Bilican K. (2020) Discovery Learning—Jerome Bruner. In: Akpan B., Kennedy T.J. (eds) Science Education in Theory and Practice. Springer Texts in Education. Springer, Cham. https://doi.org/10.1007/978-3-030-43620-9_13

Singer, Bill. (2012). *Feds Catch Their Illegal Limit In Operation Phish Phry*. Forbes. Retrived from https://www.forbes.com/sites/billsinger/2012/05/15/feds-catch-their-illegal-limit-in-operation-phish-phry/?sh=4d0e163f6265

Social-Engineer. (2016). *The DEF CON 24 Social Engineering Capture the Flag Report*. Retrieved from https://www.social-engineer.org/wp-content/uploads/2016/11/Social-Engineer-Capture-The-Flag-DEFCON24-SECTF-2016.pdf.

Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P., & Lehmann, D. (2016). Teaching Phishing-Security: Which Way is Best? *IFIP Advances in Information and Communication Technology*, *471*, 135–149. https://doi.org/10.1007/978-3-319-33630-5_10

Uways Zulkurnain, A., Kamal Bin Kamarun Hamidy, A., bin Husain, A., Chizari, H., Malaysia, T., & Bahru, J. (2015). Social Engineering Attack Mitigation. In *International Journal of Mathematics and Computational Science* (Vol. 1, Issue 4). http://www.aiscience.org/journal/ijmcshttp://creativecommons.org/licenses/by-nc/4.0/

Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. *SN COMPUT. SCI.* **2,** 78 (2021). https://doi.org/10.1007/s42979-020-00443-1

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331.https://doi.org/10.1080/10658980701788165

Yeoh, W., Huang, H., Lee, W. S., al Jafari, F., & Mansson, R. (2021). Simulated Phishing Attack and Embedded Training Campaign. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2021.1919941

Zoto, E., Kowalski, S., Frantz, C., Lopez-Rojas, E., & Katt, B. (2018). A Pilot Study in Cyber Security Education Using CyberAIMs: A Simulation-Based Experiment. *IFIP Advances in Information and Communication Technology*, *531*, 40–54. https://doi.org/10.1007/978-3-319-99734-6_4

APPENDIX A. ASSESSMENTS

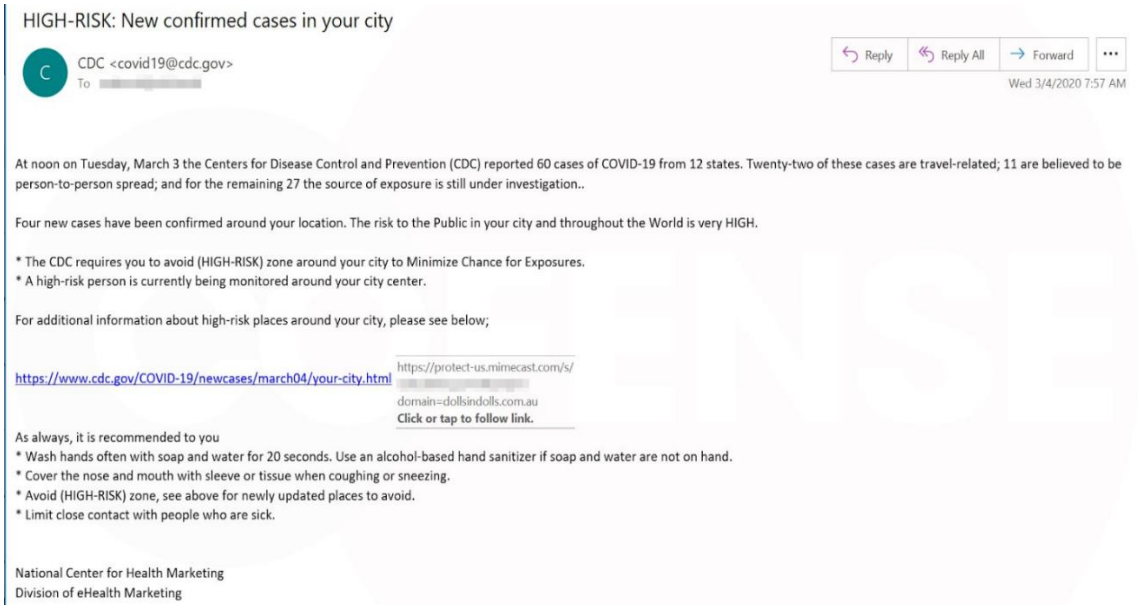
Pre-test

Questions:

1. What do Social Engineering techniques take advantage of what aspect of security to gain information?
   a. Human Aspect
   b. Bugs in Software
   c. Network Misconfigurations

2. Is the following email a legit email or is this a phishing attack?

   Figure 1: Phishing email stating to provide information about COVID-19 from the CDC. Tactic used for this attack was link.



   Note: An example of a phishing email. Reprinted from *Phishing Email Database: Real Phishing Examples & Threats* In *COFENSE,* n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus. Copyright 2021 by Cofense.

   a. Legit Email
   b. Phishing Email

3. An email claiming that you have won a prize and asking you to go to some website to enter some personal information to receive the prize is an example of what attack?

a. Phishing

b. Vishing

4. What is the difference between a phishing attack and a spear-phishing attack?
    a. Phishing attacks use SMS messages, while spear phishing attacks use emails as the means of delivery
    b. Phishing attacks and Spear phishing attacks can both be done through email, but the target is the difference. Spear phishing targets a specific victim, while phishing does not.
    c. There is no difference. These two attacks are the same.

Attention Check: The FBI reported that from 2019 to 2020 there was an increase in the number of complaints of cyber related crimes. By how much was this increase in reported cyber related crimes? The answer to this question is D: About 70%.

a. About 20%

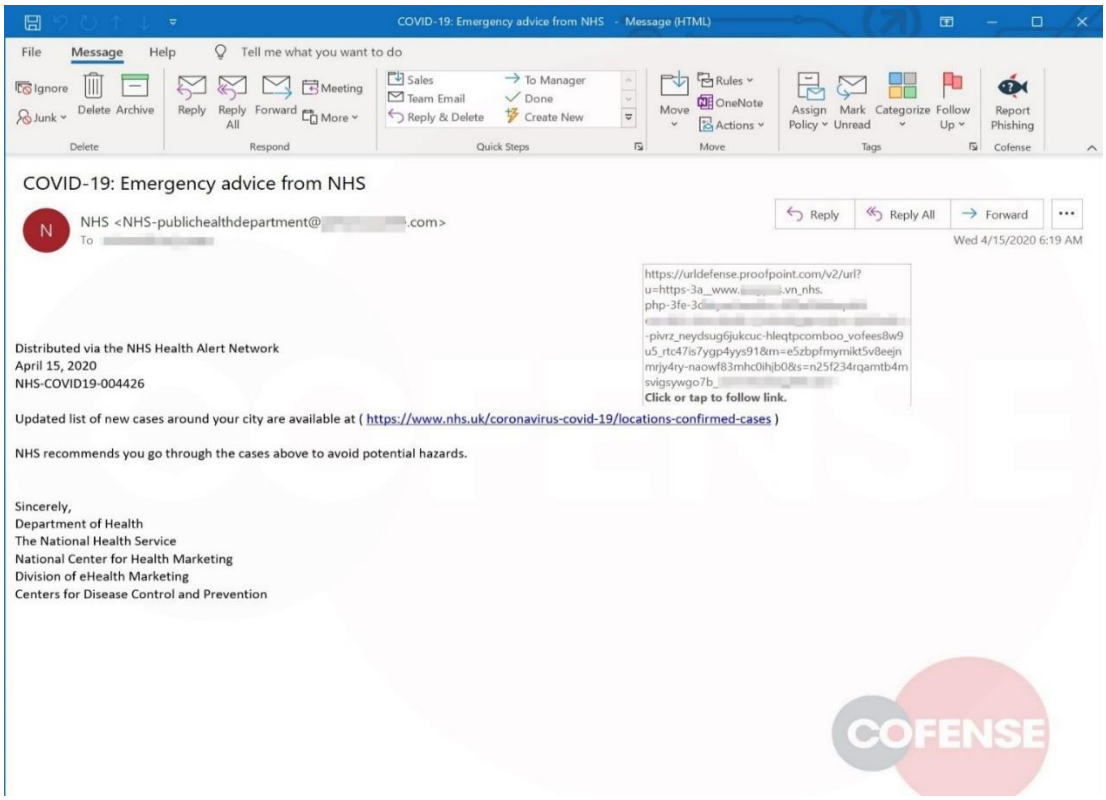
b. About 50%

c. About 10%

d. About 70%

5. From this phishing email example, which aspect of the email tells you that it is possibly a phishing attack and not a legit email?

Figure 2: Phishing email stating to have updates on the COVID-19 cases. Tactic used is link.



Note: An example of a phishing email. Reprinted from *Phishing Email Database: Real Phishing Examples & Threats* In *COFENSE*, n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus. Copyright 2021 by Cofense.

a. Misspelling and Grammar Issues

b. Inconsistent Links

c. Suspicious Attachments

d. This is a legit email

6. To whom should you report to if you think you are a victim to a Social Engineering attack if you work within a big organiaztion?
   a. IT Team
   b. Manager
   c. Incident Response Team
   d. A coworker

7. What is a step you can take if you have clicked on a link found within a phishing email and something began to download on your personal computer?
   a.Disconnet your computer from the internet and Wifi
   b.You do not need to do anything
   c.Restart your computer

8. In the event that you have inserted your credentials into a fake website linked to by an email what should you do?
   a. Delete the email
   b. Report it to the police
   c. Change passwords of any accounts using the same password you inserted
   d. You do not need to do anything

9. To whom should you report that you have been a victim of identity theft?
   a. The police
   b. The Federal Trade Commission
   c. The Department of Defense
   d. The National Security Agency

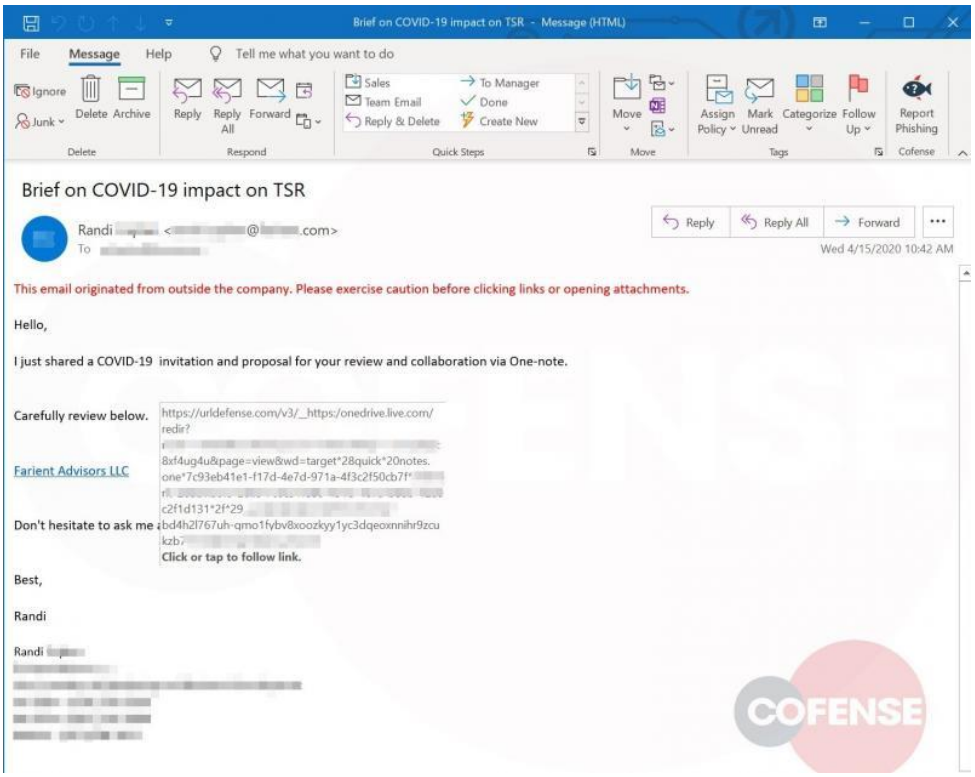
10. Are indicators of attack a good way by which you can learn to identify Social Engineering attacks?
    a.True
    b.False

Post-test

Questions:

1. Is this email a legit email or is it a phishing email?

Figure 3: Phishing Email attack inviting to review information about COVID-19. Tactic used is Link.



Note: An example of a phishing email. Reprinted from Phishing Email Database: Real Phishing Examples & Threats In COFENSE, n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus . Copyright 2021 by Cofense.

a. Legit email

b. Phishing Email

2. Hackers use Social Engineering attacks to get access to sensitive information by:

a. Hacking into Computers

b. Hacking into the Network

c. Gaining the trust of employees

3. What are some of the most common indicators of attack found in emails? Select all that apply.

a. Misspelling and Grammar Issues

b. Emails that contain a Subject line

c. Links that are not consistent with the origin sender/website

4. What is a spear phishing attack?

a. An attack where a hacker calls a person to try and get information from them

b. When an attacker tries to enter the perimter of an organization

c. An attack where a hacker sends an email to a specific target to get them to do something

Attention Check: What was the Operation Phish Phry attack? The answer to this question is C: Phishing campaign that targeted bank customers.

a. An attack where a hacker was able to get into the networks of a school district and obtain personal student information

b. Vishing campaign that targeted the Healthcare industry to gain medical information to sell in the black market

c. Phishing campaign that targeted bank customers by asking them to insert sensitive financial information into a fake website

d. Phishing campaign that targeted various companies by sending emails with attachment files that would download malware.

5. An email that is sent to a group of low-level managers of a company and asks them to click on a suspicious link is an example of what attack?

a. Vishing Attack

b. Phishing Email

c. Spear Phishing

d. Impersonation Attack

6. What is the goal of a hacker when doing an impersonation attack? Select the best answer.

a. To trick a person into thinking they are someone else

b. To impersonate a legit party and trick someone to give you some information

c. To scam a person into buying something

d. To steal money from someone

7. Why is it important to contact the Incident Response Team when you think you have been a victim of a social engineering attack within an organization?

a. To not get in trouble at the company

b. To let everyone in the company know that there has been a potential breach

c. To be able to contain the potential atatck from spreading over the company network

d. So that the Incident Response Team can figure out who the hacker was

8. Why is it important that you learn about the indicators of attack?

a. To be less likely to fall victim to an attack

b. To have new knowledge

c. To be able to learn who the hacker is

d. To then be able to create your own attack to send to the hacker

9. What is the most targeted industry?

a. Financial

b. Manufacturing

c. Oil and Gas

d. Healthcare

10. What are some common file extensions that malware files end with? Select all that apply.

a. jpj

b. zip

c. exe

d. zir

APPENDIX B. TEACHING MATERIAL

Text-Based

What is Social Engineering?

- Social Engineering attacks target people by attempting to gain their trust to manipulate them into doing beneficial actions for the attacker.
- Various attacks fall under Social Engineering attacks. Some of the most common attacks are phishing, spear phishing, and impersonation attacks
- Various industries are victims of Social Engineering attacks, but Healthcare is the most targeted industry because of the value that private information has. These same common attacks are used in the context of Healthcare and have been quite effective.

Why do hackers commonly use Social Engineering attacks?

- Unlike other attacks that require attacking a computer or some other device, the target for Social Engineering attacks is a human. Hence, compared to the skills required to hack into a system, it can be easier to target a person than to attack another machine, especially if that other machine has a lot of security in place.
- In fact, in some Social Engineering attacks, there isn't even a requirement for a laptop to do them. For example, a vishing attack is performed over a phone where an attacker aims at obtaining information from the person being called.
- Another important reason is that since these attacks target a person, they tend to be more successful than other attacks because humans tend to trust others and hence can be tricked into doing things they should not do.

What are some of the most common attacks?

- As mentioned before, some of the most common Social Engineering attacks are phishing, spear phishing, and impersonation attacks. However, what exactly are these attacks?
- What is phishing?
    - Beginning with phishing attacks. You have probably seen many of these before. An example can be an email claiming that you had won a prize and that to collect it, you needed to click on a link to go to some website where they would ask you

for more information. Well, this is most likely a phishing email attack, and if not, then that person is rather lucky and actually won something.
    - One important characteristic of phishing email attacks is that they do not have a specific target and can be sent in mass numbers just to try and get information from anyone.
- What is spear phishing?
    - Spear phishing is very similar to phishing attacks in the sense that they are after obtaining information from someone. However, the spear-phishing attack is more specific as to who the target is. Within a spear-phishing email, attackers aim to get information from a specific target. This requires doing some research on the target so that the email sent to them can be more realistic by containing information that pertaining to that specific target to make the email more convincing or credible
    - This target can be a certain group people from a specific company such as mid-level or low-level managers in a financial company
- What is impersonation?
    - This is an attack by which the attacker is impersonating to be some legit party in the attempt to trick someone into giving the attacker some wanted information.
    - Impersonation can be used in many forms and is often used within phishing email attacks to trick someone into thinking that they are a legit party.

What are some indicators of attack?

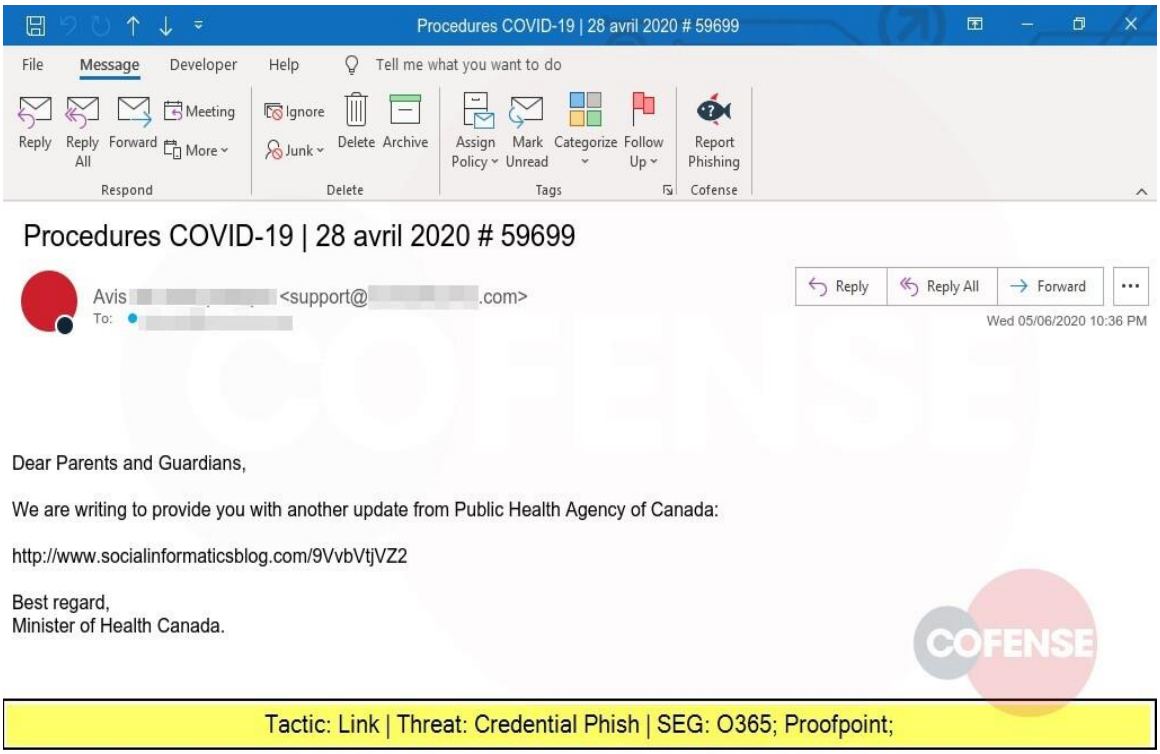
- Let's look at some real cases of phishing email attacks and look at some of the details in the email that tells us they are not legit emails.

- Some of the most common indicators of an attack are:
    - Spelling and grammar errors
    - Links, emails, and domain names are not consistent
        - this can be in a case where the email is allegedly from some website and the link you are sent to does not match that alleged website
            - You can check if the links match by hovering over the link in the email to see if the url that pops up is the same one as the original

link in the email. If it is not then that is a link mismatch and you should not click on it.

- There is a sense of urgency in the email requiring you to take action
- There is some suspicious attachment in the email.
  - Some common files used for malware end with (.zip, .exe, .scr, .js, etc..) so look out for these
  - If you see some suspicious attachment you should not click on it

Figure 4 Example Phishing Email with misspelling errors. Shows an indicator of attack in having spelling errors.



Note: An example of a phishing email. Reprinted from *Phishing Email Database: Real Phishing Examples & Threats* In *COFENSE*, n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus. Copyright 2021 by Cofense.

- In this phishing email, if we start from top to bottom, we can see that there is a spelling error in the Subject line: “avri”. This is an indicator that this is, in fact, not a legit email as you would expect the word April to be spelled correctly.

What to do in the event you are victim to a Social Engineering Attack? (Treatment Phase)

- Within an organization, in the event that you are to fall victim to an attack there are some actions that you can take to try to control the situation.
    - For one it is important that you contact the incident response team if you believe you are a victim of a Social Engineering attack as they will be able to evaluate the attack and see what is going on
        - The importance in doing so is to be able to contain the attack and esure that the spread of the attack can be as limited as possible. The reason is that if the attack is not contained quickly then this can cause for the further spread of the attack onto the network and hence potentially be able to affect multiple machines within an organization
- In the case that you suspect you are a victim to a Social Engineering attack there are various things that you can do depending on the type of attack that you have encountered
    - If you have accidentally downloaded some suspicious attachment from some phishing email or you have clicked on a link on an email and something began to download onto your computer, then it is important that you disconnect your computer from the WiFi/Internet as this may be a way to stop an attacker from installing some malware and attempting to gain remote access to your machine
    - If you find that you have clicked on a link that led you to another website to input your credential for some site then you should ensure that you go and change your passwords to any account that you have that has that same password you have entered into that website
        - It is recommended that you also use a password manager so that this manager can create random passwords for you and store them for you so that you are not using the same password across multiple accounts. This password manager can save all of these random passwords so you do not need to worry about remembering them all.
    - If you think that there is some information that has been stolen or if you see some identity theft activity happening hen you need to report this to the Federal Trade Commission to get as much help as possible as to what to do if it is the case that sensitive information was stolen from you

- Now while the amount of things that can be done are various depending on the form of the attack and what exactly happened after the Social Engineering Attack occurred, by understanding the previously mentioned indicators of attack you are less likely to fall victim to such attacks and have to go through these countermeasures.

Gamification

Let's play a quiz game where you can see if you can outsmart the hacker. You will be prompted with the option to play or go to the leader board where you can see how other players have done by viewing their scores. Once you play the game you can insert your own username which can be whatever you want.
After completing the game return to this survey to then continue with the next step which will be a post-assessment.

Note: No information from you is being collected through this website.

Open another tab in your browser, copy this link, and go to the website to play the game:

https://segamification-57495.web.app/index.html

After completing the game return to this survey to then continue with the next step which will be a post-assessment.

What is Social Engineering?

- Social Engineering attacks target people by attempting to gain their trust to manipulate them into doing beneficial actions for the attacker.
- Various attacks fall under Social Engineering attacks. Some of the most common attacks are phishing, spear phishing, and impersonation attacks

- Various industries are victims of Social Engineering attacks, but Healthcare is the most targeted industry because of the value that private information has. These same common attacks are used in the context of Healthcare and have been quite effective.

Why do hackers commonly use Social Engineering attacks?

- Unlike other attacks that require attacking a computer or some other device, the target for Social Engineering attacks is a human. Hence, compared to the skills required to hack into a system, it can be easier to target a person than to attack another machine, especially if that other machine has a lot of security in place.
- In fact, in some Social Engineering attacks, there isn't even a requirement for a laptop to do them. For example, a vishing attack is performed over a phone where an attacker aims at obtaining information from the person being called.
- Another important reason is that since these attacks target a person, they tend to be more successful than other attacks because humans tend to trust others and hence can be tricked into doing things they should not do.

What are some of the most common attacks?

- As mentioned before, some of the most common Social Engineering attacks are phishing, spear phishing, and impersonation attacks. However, what exactly are these attacks?
- What is phishing?
    - Beginning with phishing attacks. You have probably seen many of these before. An example can be an email claiming that you had won a prize and that to collect it, you needed to click on a link to go to some website where they would ask you for more information. Well, this is most likely a phishing email attack, and if not, then that person is rather lucky and actually won something.
    - One important characteristic of phishing email attacks is that they do not have a specific target and can be sent in mass numbers just to try and get information from anyone.
- What is spear phishing?
    - Spear phishing is very similar to phishing attacks in the sense that they are after obtaining information from someone. However, the spear-phishing attack is more

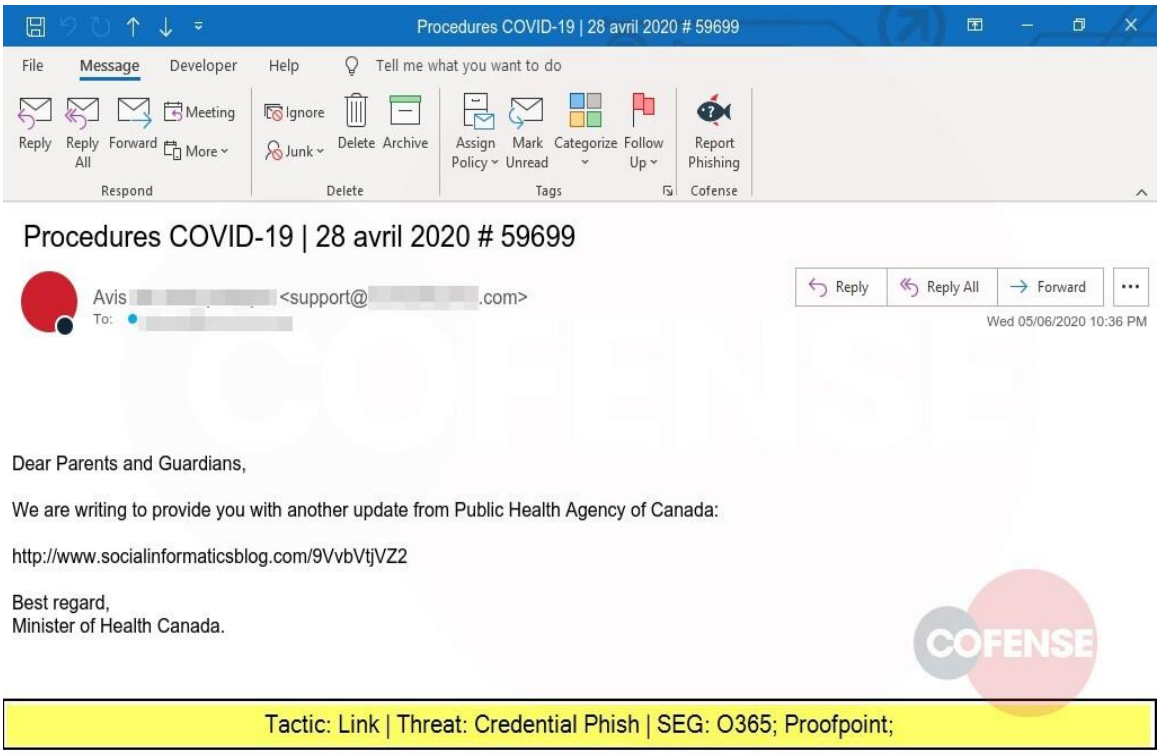
specific as to who the target is. Within a spear-phishing email, attackers aim to get information from a specific target. This requires doing some research on the target so that the email sent to them can be more realistic by containing information that pertaining to that specific target to make the email more convincing or credible
    - This target can be a certain group people from a specific company such as mid-level or low-level managers in a financial company
- What is impersonation?
    - This is an attack by which the attacker is impersonating to be some legit party in the attempt to trick someone into giving the attacker some wanted information.
    - Impersonation can be used in many forms and is often used within phishing email attacks to trick someone into thinking that they are a legit party.

What are some indicators of attack?

- Let's look at some real cases of phishing email attacks and look at some of the details in the email that tells us they are not legit emails.

- Some of the most common indicators of an attack are:
    - Spelling and grammar errors
    - Links, emails, and domain names are not consistent
        - this can be in a case where the email is allegedly from some website and the link you are sent to does not match that alleged website
            - You can check if the links match by hovering over the link in the email to see if the url that pops up is the same one as the original link in the email. If it is not then that is a link mismatch and you should not click on it.
    - There is a sense of urgency in the email requiring you to take action
    - There is some suspicious attachment in the email.
        - Some common files used for malware end with (.zip, .exe, .scr, .js, etc..) so look out for these
        - If you see some suspicious attachment you should not click on it

Figure 5 Example Phishing Email with misspelling errors. Shows an indicator of attack in having spelling errors.



Note: An example of a phishing email. Reprinted from *Phishing Email Database: Real Phishing Examples & Threats* In *COFENSE*, n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus. Copyright 2021 by Cofense.

- In this phishing email, if we start from top to bottom, we can see that there is a spelling error in the Subject line: “avri”. This is an indicator that this is, in fact, not a legit email as you would expect the word April to be spelled correctly.

What to do in the event you are victim to a Social Engineering Attack? (Treatment Phase)

- Within an organization, in the event that you are to fall victim to an attack there are some actions that you can take to try to control the situation.
    - For one it is important that you contact the incident response team if you believe you are a victim of a Social Engineering attack as they will be able to evaluate the attack and see what is going on

        - The importance in doing so is to be able to contain the attack and esure that the spread of the attack can be as limited as possible. The reason is that if the attack is not contained quickly then this can cause for the further spread of the attack onto the network and hence potentially be able to affect multiple machines within an organization
- In the case that you suspect you are a victim to a Social Engineering attack there are various things that you can do depending on the type of attack that you have encountered
    - If you have accidentally downloaded some suspicious attachment from some phishing email or you have clicked on a link on an email and something began to download onto your computer, then it is important that you disconnect your computer from the WiFi/Internet as this may be a way to stop an attacker from installing some malware and attempting to gain remote access to your machine
    - If you find that you have clicked on a link that led you to another website to input your credential for some site then you should ensure that you go and change your passwords to any account that you have that has that same password you have entered into that website
        - It is recommended that you also use a password manager so that this manager can create random passwords for you and store them for you so that you are not using the same password across multiple accounts. This password manager can save all of these random passwords so you do not need to worry about remembering them all.
    - If you think that there is some information that has been stolen or if you see some identity theft activity happening when you need to report this to the Federal Trade Commission to get as much help as possible as to what to do if it is the case that sensitive information was stolen from you
    - Now while the amount of things that can be done are various depending on the form of the attack and what exactly happened after the Social Engineering Attack occurred, by understanding the previously mentioned indicators of attack you are less likely to fall victim to such attacks and have to go through these countermeasures.

If you would like you can try the quiz game again now that you have learned more about social engineering.

After completing the game return to this survey to then continue with the next step which will be a post-assessment.

Open another tab in your browser, copy this link, and go to the website to play the game: https://segamification-57495.web.app/index.html

After completing the game, return to this survey to then continue with the next step which will be a post-assessment.

Gamification Website Created:

Figure 6: Homepage of the Gamification website

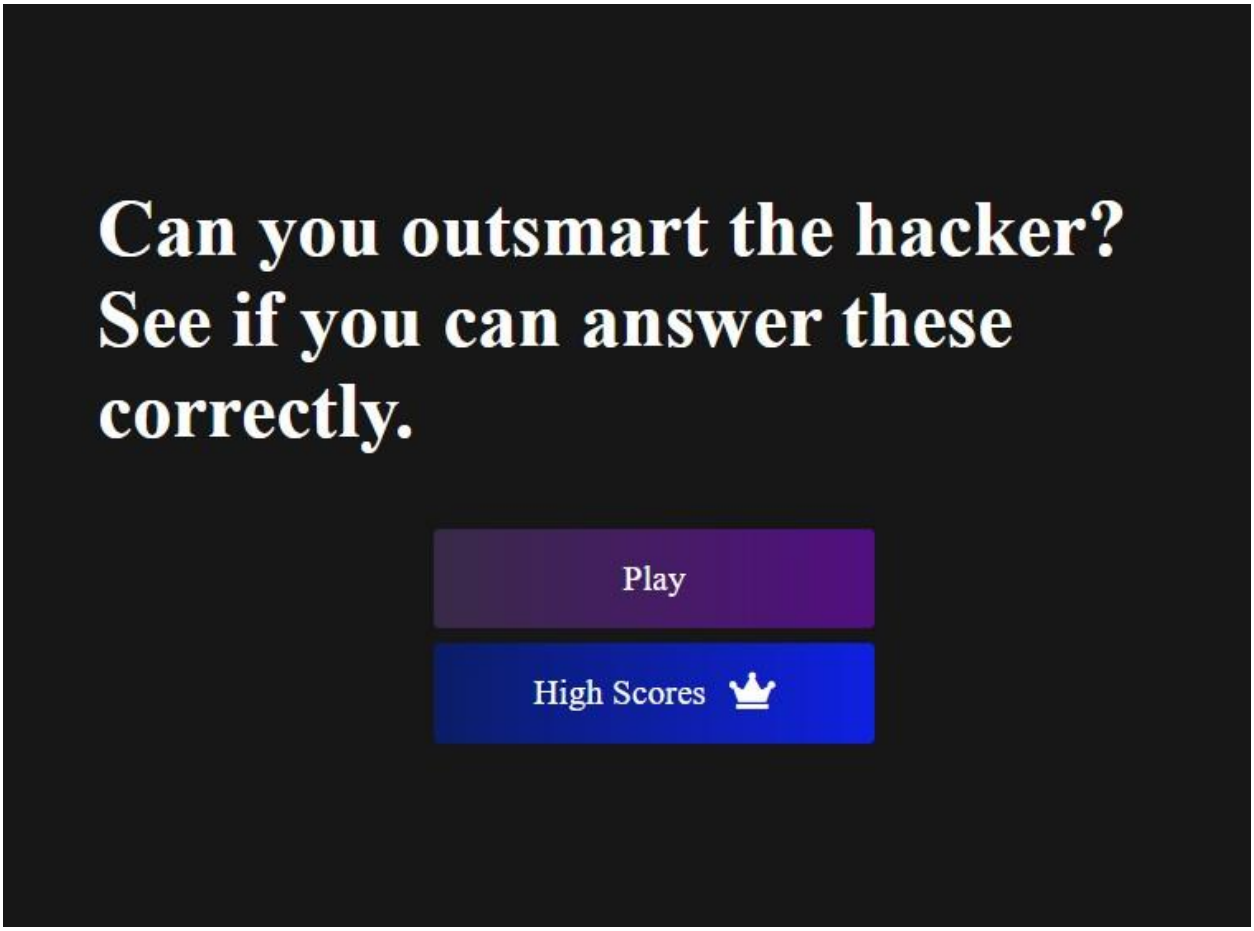


Figure 7: A question from the Gamification Website

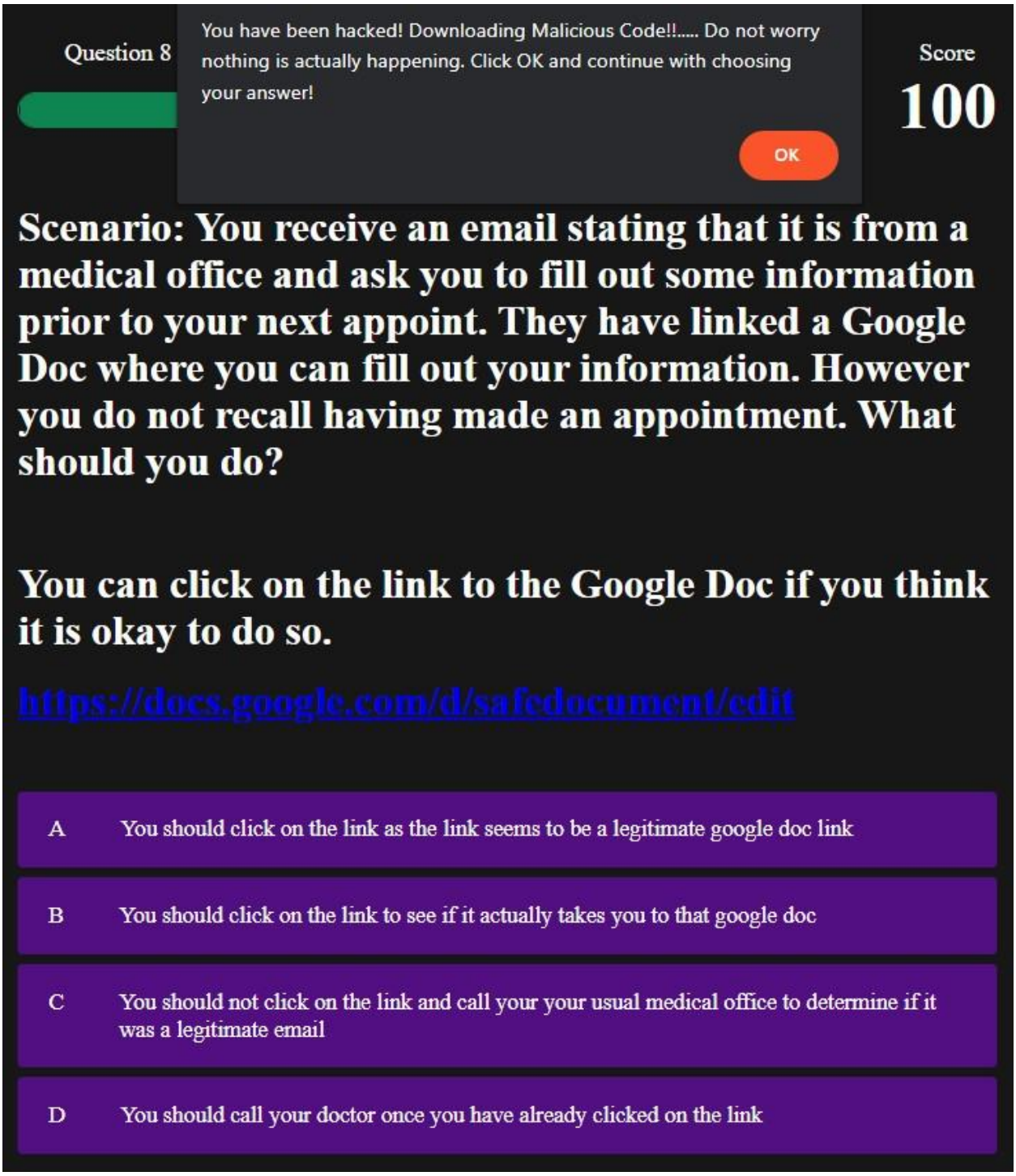


Figure 8: Another question from the Gamification Website

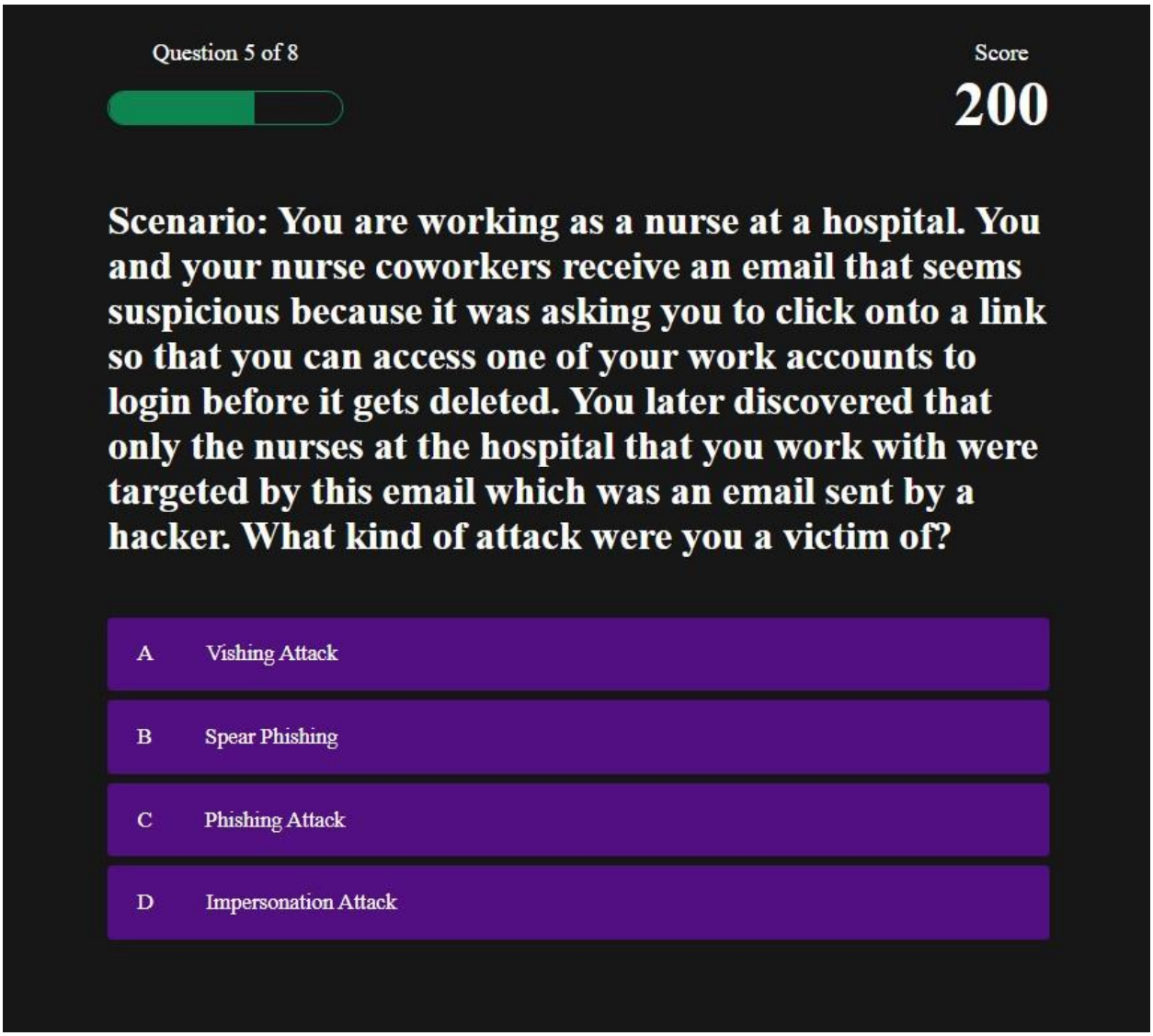
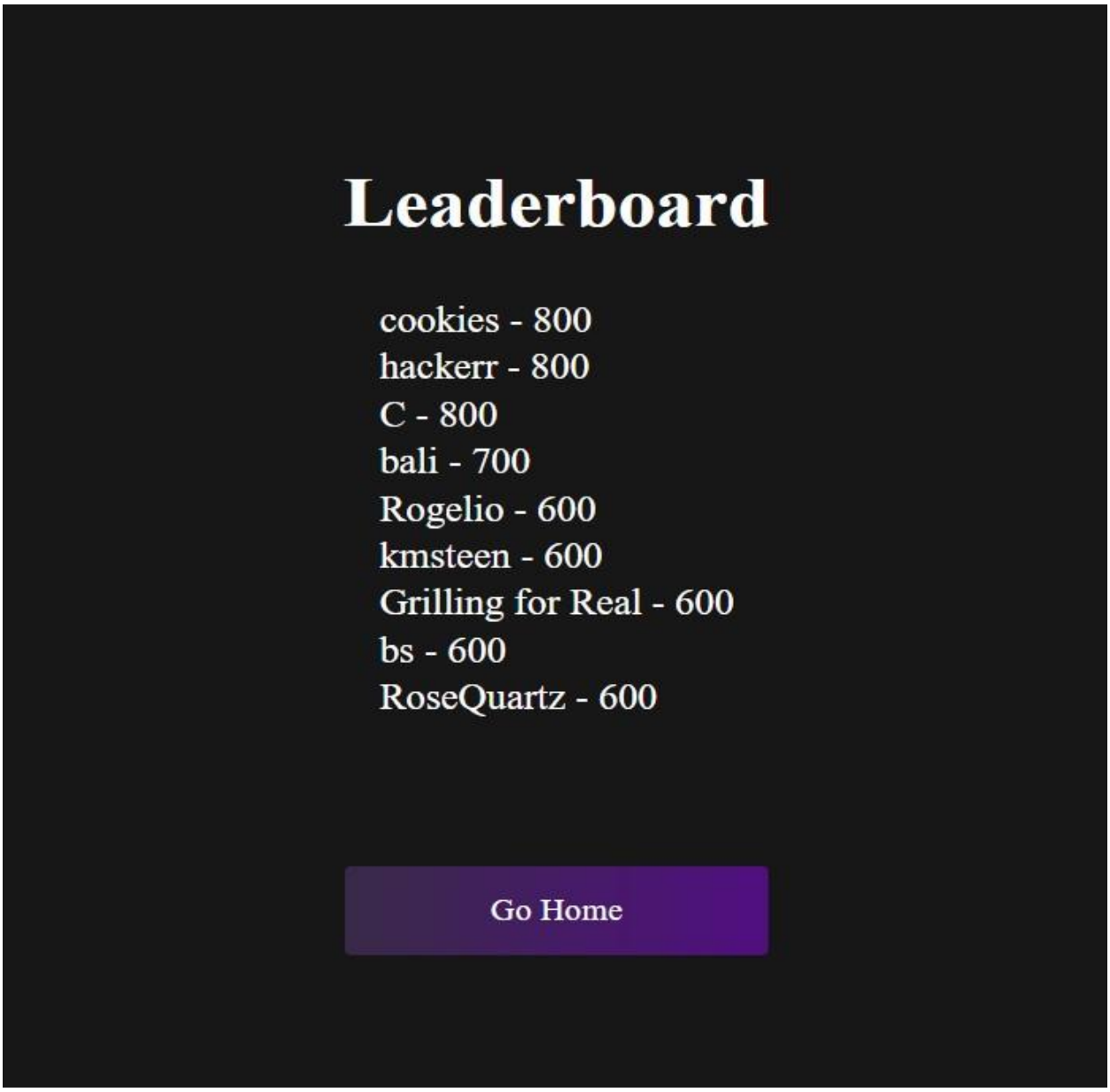


Figure 8: Leaderboard with player scores



Adversarial Thinking

For this training imagine that you are a hacker and you want to gain some information from a target. In this lesson, you will learn about how you can use Social Engineering techniques to conduct attacks that can aid you in getting the information that you want.

What is Social Engineering?

- Social Engineering is used to get someone to fall victim to your attack and manipulate them into giving you the information you want. Depending on what that information is, you can use that you get access to more things. For example, if you can trick the victim into giving you their credentials for an email account, you can use that you get full access to that account and all the information within it.
- As an attacker, you have various attacks which you can use within the scope of Social Engineering, and some of them are phishing, spear phishing, and impersonation attacks.
- One of the most attractive industries you can target is the healthcare industry because of the value of personal information. If you were to sell that information within the black market, you could make a lot of money.

Now, why would you want to use Social Engineering attacks instead of other hacking techniques?

- Unlike other attacks that require you to know how a computer works or how some other device works, Social Engineering attacks target the human vulnerability of an infrastructure. Hence it can be much easier to do Social Engineering attacks since it requires less technical skills depending on how you approach the attack.
- In attacks such as Vishing which is an attack that involves the use of a call to trick people into giving you information, does not even require any advanced technical skills but rather skills in conversation and tricking people.
- Another important reason why Social Engineering attacks can be a good choice for an attack is that they tend to be more successful, given that humans tend to trust others and hence can be tricked into doing things that they should not.

Interactive Question: Why would we want to use a Social Engineering attack and not another hacking technique to get some Sensitive information?

a. We would prefer to use Social Engineering attacks because they are more technical to do

b. We would prefer to use Social Engineering attacks beause they require less technical skills to do

c. We prefer to use Social Engineering attacks because they are both less technical intensive and because tend to trust other so these attacks tend to be more successful

d. There is no advantage in using a Social Engineering attack over other techniques

What are some of the most common attacks?

- As mentioned before, some of the most common Social Engineering attacks, especially in the healthcare industry, are phishing, spear phishing, and impersonation attacks. Now how can we conduct such attacks, and how can we increase our success in tricking people into falling for these attacks?

- What is phishing?
    - Phishing attacks are commonly in the form of an email where the attacker tries to trick someone into giving some information. For example, this could be an email claiming that you have won something and that you can redeem the prize by going to some attached link where you need to supply some personal information to get it.
    - One distinct characteristic about phishing emails is that you do not have a certain target for whom you are attempting to trick when you create them. Rather you are simply sending it around to see whoever falls for it.

- What is spear phishing?
    - Spear phishing is a similar attack to phishing, except in this case, you know who you are targeting and are aiming to get information from that specific target. This form of attack requires you to do a little bit more research on that target to develop a good attack to be able to trick them.
    - The target for these attacks can be a group of people within an organisation such as low-level or mid-level managers at a financial institution

- What is impersonation?
    - This is an attack by which you can act the role of some legit party to trick someone into giving you information that you want.
    - Impersonation can be used within a phishing attack and can aid in creating more realistic attacks.

Interactive Question: In a scenario where we want to send a phishing email to a mass number of people where we do not have a specific target, which attack would this require us to do? Choose the best answer.

a. Phishing attack

b. Spear Phishing attack

c. Vishing Attack

d. Impersonation Attack

What are some errors you should avoid making the attacks more realistic?

Let's look at some real cases of phishing email attacks and look at some of the details in emails that have some errors that we need to try to avoid to create a more realistic attack.

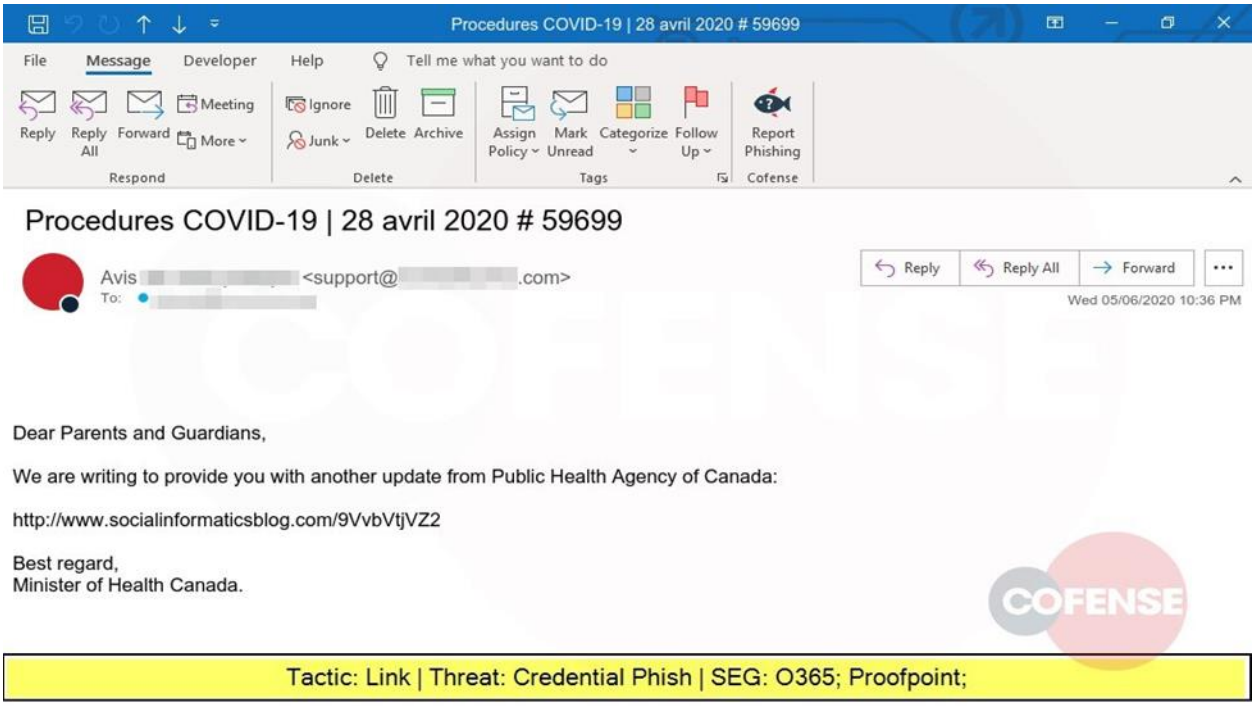
- Some of the most common indicators of a phishing attack are:
    - Spelling and grammar errors
    - Links, emails, and domain names are not consistent
        - this can be in a case where an email contains a link to some website and upon clicking the link you are sent to another website that does not match the website link in the email
        - You can check if the links match by hovering over th elink in the email to see if the url that pops up is the same one as the original link in the email. If it is not then that is a link mismatch
    - There is a sense of urgency in the email requiring you to take action
    - There is some suspicious attachment in the email.

- Some common files used for malware, which are malicous programs, end with (.zip, .exe, .scr, .js, etc..)
    - Malware can be used to do various things such as have remote control over a victim's computer

However, for our purposes, this means that we need to construct phishing emails that have as few obvious errors as possible.

Let's look at an example and see what the issue is with this email and what we can do to ensure that the phishing attack is able to look more realistic.

Figure 9: Example Phishing Email with misspelling errors. Shows an indicator of attack in having spelling errors.



Note: An example of a phishing email. Reprinted from Phishing Email Database: Real Phishing Examples & Threats In COFENSE, n.d., Retrieved October 8th, 2021, from https://cofense.com/real-phishing-examples-and-threats/?_seg_theme=coronavirus. Copyright 2021 by Cofense.

- In this phishing email, if we start from top to bottom, we can see that there is a spelling error in the Subject line: “avri”.
    - We need to ensure that when we construct an email, we do not make any spelling mistakes like this because a knowledgeable person in Social Engineering attacks will be able to know that this is not a legit email. As well as it can cause any other person to have some suspicion.

Interactive Question: To ensure that our phishing email attack is effective in tricking our victim what are some things we can do to ensure that our attack looks legitimate? Select all that apply.
a. Ensure that the email we send our attack to is a legit email
b. Ensure that we do not have any misspellings and grammar issues within our email
c. Ensure that the fake website that is linked within the email closely resembles the real website domain link
d. Ensure that we use attachements with files that are not commonly known to contain malware

Things to consider that a victim might to in case you are successful with your attack:

- Within an organization, in the event that a target does fall victim to an attack there are some actions that they may take to control the situation.
    - For one they may contact the incident response team if they think that they are a victim of a Social Engineering attack
        - If the incident response team does begin to look into the situation, then they will try to limit the spread of certain attacks over their network and hence an attack will not be able to affect multiple machines within an organization.

- Within a victim’s own computer, in the event that your target suspects they are a victim to a Social Engineering attack there are various things they can try to do depending on the type of attack they encounter
    - If they download a malicious attachment from a phishing email or they clicked on a link within an email and something begins to download, they may try to

disconnect their computer from the WIFI/Internet. This can potentially then prevent us from downloading malicious malware onto the target's computer which will not allow us to do things such as gain remote access to their computer.

- If the target realizes that they have clicked onto a link that took them to a fake website and they inserted their credentials for some real website then they may change their credentials for any website account they own which uses those same credentials. This would then make us unable to access their accounts if they change their credentials before we can log into their account.
    - They also may be using a Password Manager which is a program that automatically creates random passwords for a user and then has the passwords stored for them so that they do not have the same credentials used within various accounts. For us as an attacker this would mean that in the event that we were to get access to one account's credentials, we would not be able to use those same credentials to get access to any other accounts they own.
- If the target thinks that they have had information stolen or if they think they are victims of identity theft, then they may report this situation to the Federal Trade Commission and if so as an attacker we need to be careful as any activity that is linked to their identity could get traced back to us if we are not careful.

While it may be the case that the target may know indicators of Social Engineering attack which can aid them in not fall victim to Social Engineering attacks, there are many people that do not know about these indicators so Social Engineering attacks are still very effective and often used.

APPENDIX C: CONSENT FORM & IRB APPROVAL

Consent Form & IRB Approval

Study: Comparing Social Engineering Training In The Context Of Healthcare
PI: Ida Ngambeki
Department of Computer & Information Technology Purdue University
IRB #2021-1693

Key Information

Please take time to review all of the information provided carefully. This is a research study. Your participation in this study is voluntary, which means that you may choose not to participate at any time without any penalty or loss of benefits to which you are otherwise entitled. You may ask questions to the researcher about the study whenever you would like. If you decide to take part in the study, you will be asked to indicate your acceptance, be sure you understand what you will do and any possible risks or benefits. The research study will investigate the effectiveness of three teaching methods in teaching Social Engineering concepts. The study consists of one assessment and a lesson which will take approximately 30 minutes.

What is the purpose of this study?

The purpose of this study is to investigate the effectiveness of three types of teaching methods in teaching Social Engineering concepts. Social Engineering is the psychological manipulation of people into giving private information which is commonly used by hackers to get sensitive information from their victims. The reason for doing this study is that educating in Social Engineering concepts is known to be a good way to combat the susceptibility of falling victim to Social Engineering attacks. Hence, this study will aim to uncover what is a good teaching method that can be used to effectively teach people about Social Engineering and help lessen the number of successful Social Engineering attacks.

You are being asked to participate in this study because you are a student who uses information and communication technologies such as a computer. We would like to enroll 300 people in this study.

What will I do if I choose to be in the study?

If you choose to be in the study, you will answer a pre-assessment followed by a small lesson and, finally, a post-assessment based on the information taught in the lessons. The assessment questions will be about Social Engineering concepts that are going to be taught in the lessons. The Social Engineering concepts within the lessons consist of concepts such as what are some of the common Social Engineering attacks and what are some common indicators of attack. This study will collect basic demographic information and your email address.

How long will I be in this study?

You will be in the study for approximately 15-30 minutes, during which you will complete two assessments and a lesson.

What are the possible risks or discomforts?

The possible risks or discomforts associated with this study are minimal. The risks are no more than you would encounter in an online class. Breach of confidentiality is always a risk with data, but we will take precautions to minimize this risk as described in the confidentiality section.

Are there any potential benefits?

The potential benefit is that you may learn some indicators for when you may see a Social Engineering attack which can help you not fall victim to it.

Will I receive payment or other incentive?

If you choose to participate in the study, you will have the chance to win one of four 100$ Amazon Gift Cards. The odds of winning a gift card are 4 in 300.

Will information about me and my participation kept confidential?

The study will only be collecting your email to contact you in case you win an Amazon Gift Card and basic demographics. However, your survey responses will not be linked back to you to ensure confidentiality. Your email will be linked to an identifier, and that identifier will then be used to link to your survey responses. However, this identifier and your email will be separated, and hence there will be no identifying information that can be linked to the identifier. All the data collected will be stored in password-protected files, which will only be accessible by the researcher, and only the survey response data will be stored indefinitely. After all the data has been collected and the gift cards have been issued, all identifying information will be deleted.

What are my rights if I take part in this study?

You do not have to participate in the study. If you do agree to participate, you can withdraw your participation at any time without any penalty.

Who can I contact if I have questions about the study?

If you have any questions, comments, or concerns about this study, you can talk to the researcher. Please contact Giovanni Ordonez by email at gordonez@purdue.edu.

To report anonymously via Purdue's Hotline see www.purdue.edu/hotline If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to:

Human Research Protection Program - Purdue University Ernest C. Young Hall, Room 1032 155 S. Grant St. West Lafayette, IN 47907-2114

By clicking the consent button below, I consent to participate in this study.

Note: If you do not consent, you will automatically be taken to the end of the survey and no information will be recorded.

I consent.

I do not consent.