SURVEY OF SOCIAL ENGINEERS AND THE VALIDITY OF DEFENSIVE TECHNIQUES

By

Adrian Dana Austin

May, 2022

Director of Thesis: Dr. Te-Shun Chou

Major Department: Department of Technology Systems

ABSTRACT

In the context of information technology, social engineering is a nexus of computers and humans. Defenders need to know how hackers and other deviant actors attempt to interact with users. Social engineers are sometimes the professionals who perform deviant behavior for a positive purpose to assist users in knowing what to look for when another actor performs a deviant act for fraudulent purposes.

The purpose of this research was to ask questions of social engineers on both sides of the rule of law to determine if the current defensive techniques used to protect against deviant actors are having a positive effect on defense against said actors. The project utilized an Internet-based mixed methods survey sent to social engineers found using Reddit, a social media site.

The project was begun with a series of questions devised to reduce the project's scope further. The questions were left with open-ended sections to allow for further research later. The questions were then placed in a survey created in Redcap, a

program designed for distributing surveys included on the Internet. The social media site Reddit was chosen to distribute the survey. This was due in part to the Reddit being one of the world's top visited sites and the groups that were surveyed tended towards being more deviant than others based on the subject matter viewed. The survey was conducted for 2 months, and only 12 partial surveys were completed, at which point an interview was conducted with a person from the National Institute of Standards and Technology (NIST). Per the interview, it was determined that the main reason the survey did not succeed was due in part to the lack of being known in the community. Paraphrasing Stewart (2003), Borum (2010), and Karlins & Navarro (2008), a person known in the community of social engineers would have had a better chance of getting completed surveys. Much of this interpersonal trust would have come due to in-group status and the theory of trust transfer. The idea behind in-group status is that one would interact with the group to be surveyed; the researcher would then be seen as part of the group and not an interloper. Trust transfer theory is a concept that has been used in the consumer market for a while. This idea is that if a party trusts another person or entity and the new person or entity is associated with something already trusted, some of the trust can be transferred to the new entity. Trust transfer theory and in-group status contributed to the potential responders not completing the survey. Future research on this topic should endeavor to obtain in-group status before continuing; for a future researcher, this may take months to years to achieve.

SURVEY OF SOCIAL ENGINEERS AND THE VALIDITY OF DEFENSIVE TECHNIQUES

A Thesis

Presented to the Faculty of the Department of Technology Systems

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Network Technology

by

Adrian D. Austin

May, 2022

Survey of Social Engineers and the Validity of Defensive Techniques

By

Adrian Dana Austin

APPROVED BY:

Director of Thesis _____

Te-Shun Chou, PhD

Committee Member _____

Michael Behm, PhD

Committee Member _____

Carolyn Dunn, PhD

Chair of the Department of Technology Systems _____

Tijjani Mohammed, PhD

Dean of the Graduate School _____

Paul J. Gemperline, PhD

ACKNOWLEDGEMENTS

I would like to thank my private thesis coach, Casey Casas and Mary Rinn. Your help in holding my hand through this process made mole hills out of mountains. I would also like to thank my parents for their encouragement and my professors at ECU for not giving up, even though COVID-19 made this an arduous task at times.

Table of Contents

CHAPTER 1. INTRODUCTION

Cyber security is a subset of the information technology field. Within cyber security is a subcategory that covers actors trying to get access to systems fraudulently through the humans involved. This subcategory is called social engineering and includes phishing, smishing, vishing, baiting, and impersonation (Hadnagy, 2014, 2018; Talamantes, 2014). Currently, several defensive techniques make up the “defense in depth” strategy used to protect systems as a whole. Defense in depth is a strategy that allows for the idea that even if one layer fails, other layers will keep out intrusions. The best method for defending against social engineering typically falls into more than one of the in-depth categories of policy, information technology tools, and user education (Grimes, 2017; Mitnick & Simon, 2003).

Education and correction of activities undertaken by humans that negatively affect the security of information technology systems is the area of study for social engineering defense. Humans are both the greatest asset and the biggest problem with information security. The breadth and depth of knowledge about this issue vary greatly. While user education is the most widely discussed portion of the defense in depth against social engineering, policies and tech tools are also important.

Given the state of social engineering attacks and their rise, more data needs to be gleaned about how persons performing social engineering attacks feel defensive techniques are working. Much of the existing research has defined what techniques are being used currently, but not their effectiveness.

Social engineers are persons that perform a wide variety of tasks that relate to human interaction. For this research, we limited the scope to activities related to

acquiring data and/or access to secured information systems. Social engineers also make the time to study the individual or organization being targeted before making initial contact. They may be studying the entities' trash, social media information, or other publicly available information. They may also be performing varying forms of surveillance. These individuals take the time to study verbal and nonverbal cues when interacting with other humans. Interactions are not always in person, as an interaction could occur through e-mail, SMS text, voice applications, or with a software program that a person created without paying attention to security needs.

Social engineering attacks occur frequently and happen all over the globe. These attacks can be started with research to breach a local installation or with the click of a button to breach some remote location where personnel are not even aware of the attack. These social engineering attacks can occur at any time, day or night, and can even occur when the target is asleep.

The current state of defensive techniques against social engineering is largely insufficient. Hackers and social engineers are trying to gain information from the humans involved in the security system. This is because the technology and systems have been hardened to the point where humans are the weak link in the system. There have been many reviews of current defensive techniques and how they go about solving the issue of social engineering breaches. The question we asked within this thesis is: According to social engineers, what is the best defensive technique available against social engineering attacks?

To give statistics to this discussion, according to Galov (2021):

> [I]n 2021 Cybercriminals used social engineering in 98% of attacks... 75% of companies world wide were victim of phishing attacks in 2020… A

> ransomware attack is successful every 11 seconds. 60% of employees in the US click on emails even if they think them suspicious… Around 17,700 is lost every minute due to phishing. That equates to 1,062,00 million per hour and 25,488,000 million per day...The US government allocated nearly 19 billion for cybersecurity in 2021.

The need to reduce social engineering attacks is not about reducing the attempts but reducing their success rates. Who better to ask than the people who are succeeding? The purpose of asking the validity of current defensive techniques is to ask a follow-up question to the social engineers about what they feel would be a viable solution to social engineering attacks.

The desired future to be discussed with this research is to continue a conversation that began with what current defensive techniques are and if these techniques are effective. If a discussion between social engineers and researchers can happen, that may decrease the use of social engineering as a point of entry into information technology systems.

Mitigation of risks associated with social engineering will be more of a viable option. The future state desired by this research is to continue a dialogue working towards a solution from the rampant use of social engineering to breach information technology systems. To that end, I began by asking persons who perform social engineering tasks their opinion of the current state of social engineering defensive techniques. Then I asked if they, the persons doing the attacking, know of any techniques that would be more viable for defense. The reason to ask the deviant actors that are performing social engineering about defensive techniques is twofold. First during a search of the research available, no one else has asked them these questions. A number of persons have done research on social engineering; however, no one that this researcher could find, has asked the actors their perspective on the subject. And

second, the thought that arose, was from the use of this technique on other deviant behaviors. The thought here is similar in that social engineers would know best about social engineers. A side thought here is that most of the human aspects of Computer Science are being left out in a manner of speaking. Much of the research is either on the psychological side or the computer science side of the subject. Much of the research does not tend towards the meshing of both sides of this human aspect. This mesh between the two sides includes such areas as why certain libraries are always reused and not tested for malicious activity on a regular basis (this is beginning to be done). Also why are there the same kinds of holes in code from new programs as there were found in older codes, did a new generation of coders not learn all the lessons of the previous generation? And errors in hardware design causing external access to a computer simply because the right testing may not have been done in a rush to market. But this thesis focuses on social engineering, one aspect of the human side of computer science.

The main issue is that defenses against social engineering techniques are not keeping up with the number of attacks to promote security. The rate at which defenses succeed needs to increase to change this perception. There are many facets to social engineering, and as such, each facet must be asked separately about each aspect. Furthermore, different aspects of social engineering are more affected by different defensive techniques than others.

E-mail filters and user training defend against phishing. Smishing and vishing are defended by user training. Baiting is defended by network tools and user training, while impersonation is defended by user training. However, while the most useful defense,

user training also relies on the human aspect of security. Part of involving computers and information technology in our everyday lives was to reduce the dependency on humans for many aspects of life, including security. So, the question that needs to be asked is, “What is a better way to defend against social engineering techniques?”

One of the critical aspects of this project is that we asked social engineers what they think is the best way to defend against social engineering. It makes sense to ask the people who are breaking into your house what the best way is to keep them out. Social engineers are the ideal group to ask questions such as:

- How do you start gathering information on a target?
- What is the best technique in an in-depth defense strategy?
- Which defensive technique warrants more user education than others? (See Appendix D for the survey questions)

1.1. Statement of the Problem

The problem for this study is to determine from social engineers the most effective defensive techniques against social engineering attacks.

1.2. Research Questions and Hypotheses

- R1: Are defensive techniques against phishing currently in use viable as positive defense techniques, according to social engineers?
    - H01: Current techniques have a positive outcome on defense.
    - H02: E-mail filters are the best tool to defend against phishing.
    - H03: E-mail filters need to be updated vigilantly to maintain a positive position in a defense strategy.
    - H04: There is not a better technique outside of user training than e-mail filtering.

- R2: Are defensive techniques against smishing currently in use viable as positive defense techniques, according to social engineers?
    - H01: Current techniques have a positive outcome on defense.
    - H02: User training is the best tool to defend against smishing.
    - H03: Frequency of user training is not often enough for the breadth of threats.

    - H04: SMS filtering, similar to e-mail filtering may be a viable alternative outside of user training.

- R3: Are defensive techniques against vishing currently in use viable as positive defense techniques, according to social engineers?
    - H01: Current techniques have a positive outcome on defense.
    - H02: User training is the best tool to defend against vishing.
    - H03: Frequency of user training is not often enough for the breadth of threats.

- R4: Are defensive techniques against baiting currently in use viable as positive defense techniques, according to social engineers?
    - H01: Current techniques have a positive outcome on defense.
    - H02: Limiting access by unknown hardware is the best defense against baiting.
    - H03: Network tools that keep unknown hardware from accessing the network are the best.
    - H04: Current defensive techniques are valid but need constant updating.

- R5: Are defensive techniques against impersonation currently in use viable as positive defense techniques, according to social engineers?
    - H01: Current techniques have a positive outcome on defense.
    - H02: User training is the best tool to defend against impersonation.
    - H03: Frequency of user training is not often enough for the breadth of threats.

- R6: Is multifactor authentication a positive defensive technique?
    - H01: Current techniques have a positive outcome on defense.
    - H02: Using a physical device as the second factor will be shown to be the best type of MFA.

- R7: Are e-mail filters a positive defensive technique?
    - H01: E-mail filters will be found to be a positive technique.
    - H02: There are so many variants and rankers of e-mail filters it is difficult to determine an outcome as to the best choice.

- R8: Does system patching positively affect system defenses?
    - H01: System patching will positively affect system defenses.
    - H02: Using a third party tracking software program will be the best technique for making system patching a positive effect.

- R9: Does a well done security policy have a positive effect on defense?

    - H01: Well done security policies will have a positive effect on defense of systems.
    - H02: Having a strategic, operational, and tactical policies and procedures will be the best portion of a policy for defense.

- R10: Does user education positively affect system defenses?
    - H01: User education does positively affect system defenses.
    - H02: The best technique for user education is to train on the security policy and procedures, because a well done security policy that is followed by users through education is the best practice.

- R11: Will age affect the outcomes of the previous research questions?
    - H01: Age will have an effect on the answers to the open-ended questions.

- R12: Will geographical location have an effect on the answers to the open-ended questions?
    - H01: Geographical location will affect the answers significantly to the open-ended questions.

1.3. Statement of Purpose

The purpose of this research was twofold: first, to determine from a social engineer's perspective the best defense techniques against social engineering, and second, to ask if other techniques would be better suited for part of an in-depth defense solution.

1.4. Significance of the Study

The significance of the study is that we have found that being a known entity in the social engineering community would have had a significant positive impact on this survey. Not being a known presence in that community caused a lack of responses to this survey.

1.5. Limitations

- The scope of this survey was limited by the number of questions and types of questions being asked.

- The survey questions did not get into specifics of each general defense topic. Vast differences can appear even in e-mail filtering based on the solution procured for use.
- The survey questions allowed for limited responses to the open-ended questions. They did not allow for ‘if, then’ questions that would come up in an interview.
- The number of cases may not be large enough to generalize to the larger population of social engineers.
- We sampled social engineers as a whole, We did not predict that the sample would be random enough or large enough to analyze the data by gender, race, religion, or any other demographic not mentioned

1.6. Terminology

Communication Modeling

A concept brought up by Hadnagy (2010) states that communication is a basic interaction between two entities, “[a] two-way process in which there is an exchange of information and a progression of thoughts, feelings, or ideas toward a mutually accepted goal or direction” (Hadnagy, 2010, p. 43). As it applies to the social engineer, they plan to create a common goal.

Elicitation

> “Elicitation is the art of getting information without asking direct questions” (Hadnagy, 2014, p. 30).

Influence

We define influence as the ability of a person to cause another person to perform some task that they would not otherwise do on their own that ‘appears’ to have a positive outcome for both individuals.

Manipulation

We define manipulation as the ability of a person to cause another person to perform some task that they would not otherwise do that ‘appears’ to keep a negative outcome from happening for the target.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) uses two or more verification methods to identify an entity (typically a user) before allowing them onto the system. Typically, this includes a username, password, and either a token/smartcard, phone, or something else that a person has on them at all times, such as a biological aspect (krb1, 2019).

Nonverbal Cues (Communication)/Body Language

> Nonverbal Communication, often referred to as nonverbal behavior or body language, is a means of transmitting information—just like the spoken word—except it is achieved through facial expressions, gestures, touching (haptics), physical movements (kinesics), posture, body adornments (clothes, jewelry, hairstyle, tattoos, etc.), and even tone, timbre, and volume of an individual's voice (rather than spoken content). (Karlins & Navarro, 2008, pp. 2, 4)

Personal Identifiable Information (PII)

We define PII as any information (data) that can define a particular person and distinguish them from another individual. Several sources inform our definition, including Hadnagy (2014) and Talamantes (2014).

Phishing

> A form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion. Such communications are most frequently done through e-mails that direct users to fraudulent websites that in turn collect the credentials in question. (Jakobsson & Myers, 2007, p. 1)

Pretexting

> "Pretexting is fabricating invented scenarios and stories in order to persuade a target to divulge information or do something." (Talamantes, 2014, p. 60)

Smishing

> “Smishing is a variant of phishing in which smishers (an attacker who uses SMS for phishing) send text messages to the victim’s smartphone that appears similar to genuine messages.” (Sonowal & Kuppusamy, 2018, p. 1143)

Vishing

> “Voice phishing (vishing) is a type of phishing attack where social engineers manipulate individuals during phone conversations into divulging sensitive information.” (Maseno, 2017, p. ii)

CHAPTER 2. REVIEW OF LITERATURE

2.1 Introduction

Technology has much to do with our daily lives in our modern world. Technology has moved from individual parts such as home phones, alarm clocks, audio playback devices, and video playback devices to Internet-connected devices that include smartphones, computers, smart TVs, monitored alarm systems, and medical devices that are all monitored in some fashion by companies that we as consumers have allowed into our homes for one reason or another. This monitoring is not data that is viewed and thrown away; instead, it is stored somewhere on a device of some kind.

Information technology is defined by Merriam-Webster (n.d.) as “technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.” This also means that information technology includes all the components required to support the Internet. It begins with computers and devices that connect them over short and long distances. This connection has brought about the need for security and keeping persons, or entities, from knowing what is stored in a particular data set. In part, these datasets can and often do include personally identifiable information (PII).

We define PII as any information (data) that can define a particular person’s data and distinguish their data from that of another individual. Several sources inform our definition, including Hadnagy (2014) and Talamantes (2014). Security of the information that we have allowed companies to collect on us is necessary. The necessity comes from the fact that much of the PII collected is typically used in some fashion for securing online accounts. Within the context of securing online accounts, if someone loses or

forgets their password, users utilize things such as their mother's maiden name, the name of their first pet, the street where they grew up, and some sort of favorite item as answers to challenge questions required to change passwords, in addition to other uses. PII is also used in many areas to assist in the verification of an individual who is logging onto a secured system.

Defense of this PII has helped create a whole industry called cyber security. Cyber security includes people involved in the defensive aspects of security and people playing the bad entities trying to breach systems. Without the people who are, in a civilized way, taking on the role of the deviant actors, the security personnel would not know what areas to improve upon to keep the bad actors out of their system. Much research has been done on hardening computer systems and components. However, within the research, there is a gap where humans are involved, specifically human interaction and the ability to use humans to access computer systems. Both fall into the category of social engineering. To further narrow the definition of the gap here, we are talking about asking these deviant actors about what techniques would work best against them.

2.2 Social Engineering Methods

We define social engineering as using deception to manipulate individuals into divulging confidential or personal information used for fraudulent purposes. Our definition of social engineering is based on many of the works cited in this thesis, including Hadnagy (2014, 2018), Talamantes (2014), and Gulati (2003). Social engineering includes the act of using e-mail to solicit action. For example, clicking on a link or providing credentials or other confidential information is known as phishing. A

similar act done by using an SMS text message is called smishing. The same act done with voice applications is called vishing. Baiting, in social engineering, is the use of some sort of physical media such as a flash drive, an audio player, or other devices that can be connected to a computer to transfer some file that will infect the host computer. The last act is impersonation, which implies direct contact of some kind. The social engineer acts the part of someone trusted by the victim to acquire information or other gains through fraudulent attempts.

2.2.1 Phishing.

Phishing is one means that a social engineer uses to gather information and data. Typically, a phisher will use e-mail to perform their attempts to gather information (Jakobsson & Myers, 2007)

Phishing was first mentioned in a paper by Jerry Felix and Chris Hauck at the Interex conference in 1987 (as cited in Chang, 2017). However, it was first found in the wild in the era of America Online's (AOL's) dialup network in the mid-1990s. Phishing is the act of using e-mail to convince the mark (or the victim) that they need to provide the phisher with information for potential illicit gain. A typical phishing attack contains three components, "the lure, the hook, and the catch" (Jakobsson & Myers, 2007, p. 5).

> ***The Lure.*** This first component consists of a phisher spamming a large number of users with an e-mail message that typically looks convincingly to be from some legitimate institution that has a presence on the Internet. The message often uses a convincing story to encourage the user to follow a URL hyperlink encoded in the e-mail to a website controlled by the phisher and entices the victim to provide it with certain requested information. The social engineering aspect of the attack normally makes itself known in the lure, as the spam gives some legitimate sounding reason for the user to supply confidential information to the website that is hyperlinked by the spam.

> ***The Hook*.** This typically consists of a website that mimics the appearance and feel of that of a legitimate target institution. In particular, the site is designed to be as indistinguishable from the target's site as possible. The purpose of the hook is for victims to be directed to it via the lure portion of the attack and for the victims to disclose confidential information to the site. Examples of the type of confidential information that is often harvested include: usernames, passwords, social security numbers in the U.S. (or other national identification numbers in other parts of the world), billing addresses, checking account numbers, and credit card numbers. The hook website is generally designed both to convince the victim of its legitimacy and to encourage the victim to provide confidential information to it, with as little suspicion on the victim's part as possible.
>
> ***The Catch*.** The third portion of the phishing attack is sometimes known as the kill. It involves the phisher or a catcher making use of the collected information for some nefarious purpose such as fraud or identity theft. (Jakobsson & Myers, 2007, pp. 5–6)

2.2.2 Smishing.

Smishing is a version of phishing that includes using the mobile phone's short message service (SMS). In smishing, the bad actor sends a text message to the victim through the SMS system purporting to be a trusted entity. A message is then sent telling the victim that something needs to be done about a stolen identity or frozen account (Kang et al., 2014; Yeboah-Boateng & Amanor, 2014).

2.2.3 Vishing.

Vishing is another version of phishing that includes voice interactions. Vishing is "the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward" (Ollmann, 2007, p. 3).

2.2.4 Baiting.

In this aspect of social engineering, the bad actor uses physical media and relies on the curiosity or greed of the victim (Salahdine & Kaabouch, 2019). Salahdine and

Kaabouch (2019) and Talamantes (2014) further state that this typically involves a USB drive specifically left in an area to be found by a victim. The media is then plugged into a system, after which the malicious software starts up and infects the system and pivots to other systems in the network.

2.2.5 Impersonation.

This social engineering aspect includes almost all the other options where a person talks face-to-face with the person being engineered. This category implies that technology was used for purposes other than contact. In these cases, technology may be used as props to gain access. It should be noted that a subcategory called tailgating used by Salahdine and Kaabouch (2019) would fall under this section. Tailgating includes the idea that a person acts as if they belong and should be allowed access to the same areas as the person they are following.

2.3 Social Engineering Techniques

The above phishing, smishing, vishing, baiting, and impersonation methods are accomplished using the techniques discussed below. These techniques include communication modeling, pretexting, influence and manipulation, elicitation, reverse social engineering, and using nonverbal cues against the person being socially engineered.

2.3.1 Communication Modeling.

Communication modeling is a technique discussed by Hadnagy (2014, 2018). Communication modeling is about how to interact with other people. Hadnagy breaks down his model into three parts.

The first part is the approach which involves knowing how to present oneself to someone with whom one wishes to interact. “It is those first crucial seconds of interaction between you and a stranger that will set the tone for the rest of the engagement” (Hadnagy, 2018, p. 66). Sizing a person up and determining what can be ascertained based on their attributes and then deciding upon the approach to get a positive outcome can be very difficult. In the approach, one needs to be able to answer the following four questions in the first 5-10 seconds of the interaction: “Who are you? What do you want? Are you a threat? How long will this take?” (Hadnagy, 2018, p. 67).

Secondly, Hadnagy (2018) utilizes his DISC acronym using four quadrants of a circle as Direct/Dominant, Influencing, Supporter/Steady, and Conscientious/Compliant. The wording of the acronym quickly demonstrates the different types of communicators involved.

Thirdly, understanding where the mark or victim lies within the circle and where the social engineer lies within the circle can also influence the outcome of an interaction between the two. The social engineer will be more successful and gain a positive outcome if they use the first few moments of an interaction to determine what quadrant of the circle the person being engineered falls into and how that will mesh with the engineer’s own location on the DISC circle. There are techniques Hadnagy says to use based on where the two persons fall within the circle, but that is outside the scope of this document.

Finally, Hadnagy (2018) discusses the limitations of using his DISC acronym. He discusses how this is not some sort of magic wand and that communication modeling

takes time. The good news, according to Hadnagy, is that this will work in all of the areas of social engineering mentioned in the previous section.

2.3.2 Pretexting.

In his book, Talamantes (2014) devotes an entire chapter to the topic of pretexting. He states that research and planning go into performing this particular activity. In addition, he discusses body language and non-verbal cues that influence its effectiveness. Pretexting involves creating a scenario that is presented in a manner that is believable and induces trust by the persons being engineered. This scenario includes the social engineer's background information and potentially using disguises and identity impersonation. Talamantes also states that pretexting goes beyond simple flattery or being ignorant of a subject.

2.3.3 Influence and manipulation.

Manipulation is a form of influence. In an article published by Forbes, Duncan (2018) interviewed Bob Burg, a famous author, on influence and manipulation related to business. He stated that the actual divide is between manipulation on the negative side and persuasion on the positive side. In the article, Burg states that influence in and of itself is neutral.

> It's sort of like the physical law of gravity. Gravity in and of itself is neutral. It manifests itself as good when keeping us floating aimlessly up into space. It manifests itself as bad when we fall off a seven-story building… Both manipulators and persuaders understand human nature, human motivation, what drives people to take action on certain ideas. But while manipulators will utilize that knowledge for their own ends only, persuaders will never do that. (as cited in Duncan, 2018, para. 14)

Maxwell (2013), Talamantes (2014), and Hadnagy (2018) go into a bit more depth on the following subtopics in their work: authority, concession, likability, obligation, reciprocity, and scarcity. I describe each in more detail below.

Regarding *authority*, social engineers position themselves in a position of authority over the intended target in some manner. This form of social engineering typically works in larger business entities and when the social engineer is not physically present.

In an influence operation that includes *concession*, Maxwell (2013) defined it as letting go of something you appear to want and settling for something smaller—in other words, telling the subject being social engineered that you want something big and a little out of reach and when they say no, accepting that and asking for something within reach and smaller. This smaller thing that is within reach is actually what the social engineer wanted in the first place.

Likability is an influence technique that involves the engineered feeling liked in some manner. With *likability*, it can be difficult to judge the level of compliment necessary to keep the person from being too skeptical. Talamantes (2014) discusses how following up a small compliment with a question is a good example of gauging the proper level. The example he uses is, “That’s a great looking watch. May I ask where you bought it?” (p. 41).

Obligation types of influence include having the subject being engineered to feel obligated to respond to questions that are asked due to, in some situations, societal norms. These societal norms include gratitude or feeling that they owe the engineer the information. According to Talamantes (2014), this could be something as simple as

holding the door open for the target. *Obligation* also includes the idea that the social engineer may give up tidbits of information that appear to be about themselves, thereby obligating the one being engineered to reciprocate.

With *reciprocity*, one must simply apply the rule of treating others as you would wish to be treated. The previous example of giving up information about oneself could also fall under reciprocity. “This feeling of indebtedness triggers reciprocity in your target and makes them much more likely to fulfill a request” (Maxwell, 2013, para. 5).

Scarcity is the last concept upon which the three authors agree. Talamantes (2014) succinctly states,

> In social engineering, scarcity is used to create a situation or feelings of urgency necessitating the target to make a quick and rash decision. Of course, the scarcity situation itself is one that is fabricated by the social engineering and the choices provided are not in the best interest of the target. The desired outcome is one that forces the target to go against their instinct and comply with the social engineer’s request. (p. 39)

There are two additional topics under influence that only Maxwell (2013) and Hadnagy (2014) discuss—*social proof* and *commitment & consistency.* Simply put, *social proof* states that everybody is doing it, and you should as well. Social proof is the idea that a target will perform a task or provide information based on the idea that everyone else is doing said task or providing said information, and the target does not wish to be left out (Hadnagy, 2018; Maxwell, 2013)—in other words, using the concept of herd mentality against a target for fraudulent gains of some kind.

The last subtopic mentioned by Maxwell (2013) and Hadnagy (2018) is *consistency & commitment.* In this subtopic, the social engineer knows that the target wants to be consistent with their answers to the social engineer. For example, the social engineer will start with something small, with which the target will comply and build from

there to the information they truly wish to know. Starting small and inconspicuous will get the target going in the right direction. The target will wish to be consistent with their interaction, allowing the social engineer to gather the information they are looking for in the conversation.

2.3.4 Elicitation.

Elicitation is the art of getting information without asking direct questions. Both Talamantes (2014) and Hadnagy (2014) define this in similar ways; it is about having a regular conversation discussing typical topics and throwing in leading questions that allow the victim to offer the information the social engineer is seeking. According to Hadnagy (2014), there are ten techniques he refers to from a book by Dreeke (2011). Talamantes (2014) advises many of the same techniques, and the ten are as follows:

Artificial time constraints.

When talking to a subject, the engineer will create artificial time constraints, where they will appear to have someplace else they need to be in a short time. This will make the subject more comfortable because they can clearly see that there will be an end to the conversation. This clear ending point makes it so that the subject can feel more in control and able to realize that with a few short conversing words, they can quickly get on to what they were doing previously. Dreeke (2011) states that it is about threat level instead of controlling the situation.

Accommodating Nonverbal.

Dreeke (2011), Talamantes (2014), and Hadnagy (2014) all talk about nonverbal communication, specifically body language. The idea here is that you appear

approachable in your stance and attitude. There will be more discussion about body language later in the chapter.

Slower Rate of Speech.

Another nonverbal cue that is discussed is a slower rate of speech. Dreeke (2011) states that speech can be changed and that the speed at which we speak can affect how listeners will view the speaker. He uses the analogy of fast-talking to that of a used car salesman. More rapid speech is regularly associated with someone attempting to sell something not as high in quality as they would have the buyer believe. Therefore, a person with slower and more deliberate speech is perceived as honest and forthright.

Sympathy/assistance.

> With this idea in elicitation, the thought is to find [a] third-party reference … a topic used to initiate that isn't too personal about the individual targeted for discussion. The topic is also not about you. Individuals typically do not like talking to strangers about either of these topics, at least not in the first few seconds. (Dreeke, 2011, p. 36)

Ego suspension.

Ego suspension is the concept of suspending your egotistical thoughts and putting the wants and needs of another person ahead of your own in the interaction. This can deescalate the situation where a conversation may occur when otherwise it would not have occurred. Additionally, putting the engineer's ego on hold can elevate the other person's ego whereby they may continue to give information, after which otherwise they would have ceased.

Validation.

Dreeke (2011) splits validation into three components: listening, thoughtfulness, and validating thoughts and opinions. The first is simply the act of listening. This

listening is a way to validate what the person is saying in a simple form. The next is thoughtfulness, which includes providing small gestures that show one is placing another's needs, wants, and welfare above their own. Dreeke states this in a simple example of having hand sanitizer or chewing gum and offering them a portion of the items during a conversation. The final component of validation is to validate the thoughts and opinions of the target. Dreeke provides this example:

> While at the meeting, I asked my source, "So, what do you think about country X?" His response was perfect. He said, "I think they are doing great harm to the United States." I responded, "That's an interesting point of view, why do you think that?" Following his response, I validated his thoughts again, and then asked him what he thought we could do about it. The entire dialogue and process was centered on my source's ideas and me validating them to have him take action. (Dreeke, 2011, p. 54)

Specifically, ask how, when, and why questions because there is a socially accepted way to ask these questions. Once you have led with the other techniques to get the conversation started, the how, when, and why questions keep the conversation going. For clarity, these are not one-word questions you should ask but the beginning of a longer question that shows interest in the topic of conversation. Alternatively, the question goes from the path of the first conversation down a path that veers away from the original path towards another topic of conversation.

Quid pro quo.

This concept is the Latin phrase "something for something." The idea here that all three authors (Dreeke, 2011; Hadnagy, 2014; Talamantes, 2014) bring up is that when the social engineer is interacting with the subject, they must give up some information about themselves to get the subject to also offer information. The social engineer should

not push too hard with this but to “slowly build trust through non-threatening dialogue” (Dreeke, 2011, p. 67).

Reciprocal Altruism.

With this technique, also known as gift-giving, the social engineer will give the subject something. Reciprocation of that gift is a psychological need. An example is when someone holds open the door. A social person would, in turn, hold the door open for the first person at some nearby time, such as when there are double sets of doors.

Manage Expectations.

> This final technique is one where being able to mask one’s actual agenda or shift the agenda to appear to be altruistic is a positive for the social engineer. Every conversation or engagement with another human being has an agenda. Another definition of agenda might be objective or desired outcome. Sometimes the agenda is to sell you a used car. Sometimes the agenda is to share a secret. Other times, it is simply to make another person feel better. Regardless of the situation, whether it is an altruistic intention or not, there is an agenda. The individuals in life that are able to either mask their agenda or shift the agenda to something altruistic will have great success at building rapport. (Dreeke, 2011, p. 77)

2.3.5 Nonverbal cues.

For a social engineer, most nonverbal cues typically happen in a face-to-face meeting. Many of these subtle expressions of emotion are lost when the discussion moves to the written word or text messages. “These nonverbal cues or nonverbal communication include facial expressions, gestures, haptics (touching), physical movements (kinesics), posture, body adornment, tone, timbre, and volume of the voice as well as previously mentioned the speed of speech” (Karlins & Navarro, 2008, pp. 2–4).

2.3.6 Reverse social engineering

In reverse social engineering, the engineer makes contact with the subject and implies that they can solve a problem for the subject. This could be a current problem that the subject has called them about or a problem that the social engineer creates later, or one that happens to arise.

2.4 Information Gathering

2.4.1 Open-source intelligence (OSINT).

Open-source intelligence (OSINT) is information on an entity being researched that is available to anyone who wants it. According to Chauhan (2015), “OSINT is the intelligence collected from the sources which are presently openly in the public … such as:

- Academic publications …
- Media Sources …
- Web Content … [and]
- Public data” (p. 16)

One way to access much of this information is through the Internet. Using advanced search methods and researching is sometimes all it takes to gather information on a target entity. This information is a great way to build what is necessary for a social engineering attack.

2.4.2 Surveillance.

The other option for gathering information without directly interacting with people is surveillance. This method of intelligence gathering involves watching the target and observing through various means and technologies. Surveillance does not just mean finding a place to sit and watch a person like in the movies. Instead, surveillance

includes listening to phone conversations, watching video cameras, going through the trash, and tracking. There are many means to accomplish surveillance, but many are electronic. Talamantes discusses these techniques and others in his subsection on the topic in his book (Talamantes, 2014)

2.5 Social Engineering Defensive Techniques

> Companies that conduct security penetration tests report that their attempts to break into client company computer systems by social engineering methods are nearly 100 percent successful. Security technologies can make these types of attacks more difficult by removing people from the decision-making process. However, the only truly effective way to mitigate the threat of social engineering is through the use of security awareness combined with security policies that set ground rules for employee behavior, and appropriate education and training for employees. (Mitnick & Simon, 2003, p. 245)

Things have changed since the publication of the previously mentioned piece by Mitnick and Simon (2003); there have been many advances in defensive techniques that were not widely used in 2003. The main topics of defense will be discussed below.

2.4.1 User training.

> Security training must have a significantly greater aim than simply imparting rules. The training program designer must recognize the strong temptation on the part of employees, under pressure of getting their job done, to overlook or ignore their security responsibilities. Knowledge about the tactics of social engineering and how to defend against the attacks is important, but it will only be of value if the training is designed to focus heavily on motivating employees to use the knowledge. The company can count the program as meeting its bottom-line goal if everyone completing the training is thoroughly convinced and motivated by one basic notion: that information security is part of his or her job. (Mitnick & Simon, 2003, p. 250)

Hadnagy (2014, 2018), Mitnick and Simon (2003), and Talamantes (2014) agree on the idea that knowing how a social engineer will act is also a large part of understanding how to defend against attacks.

2.4.2 Multi-factor authentication.

Multi-factor authentication is a method of proving one's identity that requires more than just a password. "To palliate password weakness, multi-factor authentication protocols combine several authentication factors. Typically, instead of using a login and password, the user proves possession of an additional device, such as his mobile phone, or a dedicated authentication token" (Jacomme & Kremer, 2018, p. 1).

2.4.3 E-mail filters.

E-mail filtering is a way to keep out many phishing attempts from even reaching the end user. Almomani et al. (2013) break down filtering into three categories: basic features, latent topic model features, and dynamic Markov chain features. Each of these categories is a way to keep social engineers from phishing end users but is beyond the scope of this research project.

2.4.4 System patching.

> [M]issing security patches are one of the biggest problems that allow successful exploitation … to give yourself or your computers the best protection against software vulnerability exploitation, all you have to do is apply security patches in a timely and consistent manner … Unfortunately, effective patching remains overly difficult and elusive. (Grimes, 2017, p. 239-240)

Grimes states the following about patching:

1. Most exploits are caused by old vulnerabilities for which patches exist.
2. Most exploits are caused by a few unpatched programs.
3. The most unpatched program is not always the most exploited program.
4. You need to patch hardware too.

Grimes also lists some common patching problems:

1. Detecting missing patching isn't accurate.
2. You can't always patch.
3. Some percentage of patching always fails.
4. Patching will cause operational issues.
5. A patch is a globally broadcasted exploit announcement.

2.4.5 Physical security.

Physical security is something just as important as cyber security of your networks. Mitnick and Simon (2003), Hadnagy (2014, 2018), and Talamantes (2014) all discuss how to get around physical security in their respective books. A majority of the concepts behind social engineering can be used either through electronic means or in person. Having good security training for your people that provide security and having appropriate locks and security systems are equally important.

2.4.6 Security policies and controls.

Grimes (2017) and Mitnick and Simon (2003) discuss security policies and controls as defensive measures. A good security policy includes "clear instructions that provide the guidelines for employee behavior … and are a fundamental building block in developing effective controls to counter potential security threats" (Mitnick & Simon, 2003, p. 260). Policies and controls should be written so that non-technical people can understand them. Grimes (2017) and Mitnick and Simon (2003) discuss how explaining policies and breaking them down for non-technical people will make them more likely to be followed. Understanding why (explained appropriately) will keep users from just bypassing policies they feel are just a burden.

2.4.7 Unknown hardware limiting.

Limiting unknown hardware is a defense that speaks directly to the baiting technique listed above. Unknown hardware could be any electronic equipment that can

attach to your computer or network, such as USB drives, CD drives, DVD drives, audio players, smartphones, tablets, laptops, and others.

CHAPTER 3. METHODOLOGY

Social engineering and its subcategories are the most widely used attack techniques against electronic systems today. From phishing, smishing, vishing, and baiting, to impersonation, elicitation, pretexting, and reverse social engineering techniques, social engineering attack vectors are things that need to be defended against using proper techniques. The question then becomes whether these techniques are viable solutions, within which lies the premise that no one technique will solve the problem but that a defense in-depth approach will be the proper solution. A gap was found in the literature in that asking social engineers how they felt about current defensive techniques was not covered. The idea of doing a pilot survey to get a beginning down on paper to determine where the research should go was viewed as the right place to start. A mixed methods approach was chosen to allow for qualitative and quantitative results, giving the broadest overall picture of the desired results. It was deemed appropriate to use the university's REDCap software for data collection due to several factors, including collection ability, data storage and integrity, and data usability from this source.

3.1. Participants

There are two groups of people that fall under the heading of the social engineer. One group is those performing the task as part of a penetration test authorized by a client that has control of the data, location(s), and personnel to be tested. The second group includes those performing social engineering for a delinquent means of some sort. This second group represents individuals who may answer the social engineering

post but are not the intended target. The intended participants of the survey were users of Reddit, specifically some subreddits that had potential social engineers.

3.2. Survey distribution

The survey was distributed via a link to the REDCap data capture application. The survey was first sent out by e-mail to known cybersecurity firms listing penetration testing and social engineering services. There was no response from the companies to which the survey was sent. Next, Reddit was used, namely the r/Socialengineering subreddit. It has engineers who self-identify as social engineers and could add some insight into those who are more delinquent in the nature of their social engineering activities. Next, due to lack of responses, the survey was also sent out to r/hacking and r/Cybersecurity.

3.3. Data Collection and Storage

> Study data was collected and managed using REDCap electronic data capture tools hosted at East Carolina University. REDCap (Research Electronic Data Capture) is a secure, web-based application designed to support data capture for research studies, providing 1) an intuitive interface for validated data entry; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for importing data from external sources. (Harris et al., 2009, “Citing REDcap,”).

3.4. Methodology

The intention was to use a mixed methods approach because little academic research on the topic exists. Mixed methods approaches have been used to explore other novel topics accurately and thoroughly. I used a modified version of an *explanatory sequential mixed methods design* in this survey. Creswell (2014) defines this as an approach that has two phases “in which the researcher collects quantitative

data in the first phase, analyzes the results, and then uses the results to plan (or build on to) the second, qualitative phase" (p. 224). In the first phase, which is being done for this thesis project, both qualitative and quantitative questions were used to give me questions for the second phase of qualitative questions left in the further study section of this research that will be done at a later date. First, quantitative questions determine some basic information gathering about social engineering techniques. Next, questions using a Likert scale define more quantitative information; this allowed me to perform statistical analyses to test my hypotheses. However, for the main questions not asked in reference to basic information, the questions were followed up with a qualitative, open-ended question to determine if further investigation into a particular area was warranted. Furthermore, if warranted, categories for the analysis of the qualitative questions could be created for further analysis.

3.5 Survey validation

3.5.1 Establish face validity.

First, face validity was determined through discussions with the research coach. Next, the committee discussed the survey questions and reviewed for common errors such as leading, confusing, or double-barreled questions. For clarity, a double-barreled question is "one where the question is about two things that could have opposing responses" (Saris, 2014, p. 83).

3.5.2 Pilot test run.

The survey was sent to professionals via e-mail. Professionals in the social engineering field were asked about their opinion on the validity of the questions.

Unfortunately, none of the professionals to whom the survey was sent commented on the survey.

3.5.3 Internal consistency.

Once the initial evaluation of the survey was completed, it was determined that some of the questions were redundant and needed to be changed or removed from the questionnaire. This was partly done due to a belief that a shorter survey would be more likely to be answered.

3.5.4 Revising the survey.

At this point, the survey was revised based on analysis from 3.4.4; then, the process was discussed with the thesis coach and the committee as a group to determine how to proceed with the survey. Only minor changes needed to be made to the survey, so the project proceeded.

3.5.5 Survey run time.

The survey was available online for 2 months, and only 10 started responses, of which none of them were completed.

3.6 Limitation in Methodology

- The scope of this survey was limited by the number of questions and types of questions that were asked.
- The survey questions do not get into specifics of each general defense topic. Vast differences can appear even in e-mail filtering based on the solution procured for use.
- The survey questions allowed for limited responses to the open-ended questions. They did not allow for ‘if, then’ questions that would come up in an interview.
- The number of cases was not large enough to generalize to the larger population of social engineers.
- The project sampled social engineers as a whole. It did not predict that the sample would be random enough or large enough to analyze the data by race, religion, or other demographic.
- Persons answering the survey were limited to those with access to e-mail and the subreddit into which the full survey was posted.

- REDCap has its limitations that are discussed in the literature.
- There was the limitation that some individuals may deem the survey invasive and therefore will either not answer or will attempt to skew the results due to their need for deviant behavior.
- It should be noted here that the researcher realized the limitations of the data storage and collection methods. The act of data storage and collection is inherently flawed and biased in some manner that will not be apparent until later. These flaws may be as simple as asking for identifying characteristics that lead back to an individual who wished to remain anonymous. Much of this flaw has been eliminated by not asking for information that will lead to a conclusiveness of identity of individuals that do not wish to be identified. The survey asked for an e-mail address at the end to allow for some way to identify individuals; however, they would be able to hide behind electronic protection from most entities that would attempt to identify them directly. Although this will limit follow-up in the future, it is vital to the integrity and trustworthiness to not ask for any more identifying information. The survey did not ask Jessica Rabbit of Turkey, North Carolina, what her opinions were specifically and then go into detail as to why she had those opinions. The survey asked people who self-identified as social engineers what they felt answers were to the questions.
- The concept that Heisenberg (1958) introduced is that the act of observing (i.e., giving a survey) may, in fact, change the natural order of the relationships being observed in the survey. This is very similar to the Hawthorne effect in nature related to this topic.

3.7 Authorship Validation and Intent

An academic study was created to highlight ideas that have been expressed in the industry for several years. The idea was to begin with a basic step and then build upon it. For example, one cannot understand the properties of complex molecules without understanding the basics of atomic structure. Here the same principle applies, as we must first understand the basic building blocks as they appear from a social engineer’s perspective. Once this is complete, more research is needed to discuss how persons from the other side feel about the situation. It must be assumed that when talking to both groups, the mere fact of talking to them will change their perspective. The intent is that persons who wish to be left unknown will remain unknown. This, however, will affect the outcome in that follow-up of the questions will not be possible.

CHAPTER 4. SURVEY RESULTS

4.1 Introduction

Several obstacles kept the survey from being completed by potential respondents. Some of these issues came directly from the author's understanding of what needed to be done to prepare for the survey, and some resulted from limitations placed on the research from the university's Institutional Review Board. However, it was thought that out of 1,839,937 potential respondents from r/hacking, 266,855 from r/Cybersecurity,139,488 from r/SocialEngineering, and 214 profiles on Facebook that were accessible from the researcher's profile, there would be more responses. However, there were only 12 partial responses. It should be noted that this did not include the potential submissions from reposts on Reddit or Facebook, which were unable to be counted.

4.2 Question Findings

There were more sociological findings than computer science findings for the surveys that were answered. However, while there were only 12 people who answered the survey (and those mostly partial answers), a direct synopsis of what was collected can be found in Appendix E-Synopsis of results. And a discussion on the results is here.

4.2.1 Likert scale.

In 1932, Rensis Likert published a paper titled "A Technique for the Measurement of Attitudes," in which he discussed a psychological measurement scale that employs questionnaires. Almost since the beginning of the usage of his scale, there have been several discussions on its use. For example, in Willits et al. (2016), the

authors discuss how there should be multiple questions on a single topic to make the validity of the research more prevalent and accurate. They also state that “single items are appropriate when the referenced concept is singular, concrete, and understandable to the respondent” (Willits et al., 2016, p. 134). Willits et al. also discuss how a scale of “at least four are needed for evaluation of internal consistency” (Diamantopoulos et al., 2012). Moreover, while reliability measures increase as the number of items increases above five, each addition has progressively less impact on the scale reliability (Carmines & Zeller, 1979; Hinkin, 1995).

For the Likert scale questions, it was found that, for the most part, people marked *strongly agree* or *agree* for this section. There were two partial surveys indicated *disagree* with all of the Likert scale questions. There is no scientific evidence to support the idea that these two survey takers were trying to skew the results, however there is also no data to suggest this idea is wrong. This was the most complete section of the 12 surveys. Unfortunately, no one answered the qualitative component about which techniques work better. Even with the interviewee from NIST, they stated that they did not feel comfortable giving out their preferences. This finding is partly due to trust issues and the idea that the interviewee was not sure of how much I would reveal and who would be reading this to what end. Some of the reasons that the Likert scale was the most responded to part of the survey may be the ease of answering compared to the open-ended questions. Discussed later will be the point that technical word use may also have negatively impacted the comparative levels of the answerability of the Likert questions.

4.2.2 Open-ended questions.

Open-ended questions in this survey were used to gather further information. Although these questions were included to help elucidate answers to quantitative questions,

> The literature on open-ended questions has established that answering these questions places a greater burden on respondents' cognitive abilities than selecting a response category in a closed-ended questions, since respondents must formulate the answer in their own words and express it verbally or in writing. (Neuert & Lenzner, 2021, p. 466)

Additionally, they found no significant difference in the level of response to open-ended questions based on the number of questions. They did state that this may be affected by being able "to recruit participants who are trained in answering survey questions (and cognitive probes)" (Neuert & Lenzner, 2021, p. 466). Other research suggests how many questions are answered is based on the quantity presented. The open-ended portion of the Likert scale questions were not answered. Question 9 (What do you feel is the best defensive technique against Communication Modeling and why?) of the opened ended only section was the only one answered, and by only one person. Their answer:

> User education in combination with strong IT sec[urity] practices. Getting people to retain some amount of skepticism towards what's asked of them in combo with IT making sure standards are followed so that those in authority are never asking for PII over unapproved channels.

This person also asked how this question on Communication Modeling was different from the others discussing Pretexting, Convincing, Influence, Manipulation, Elicitation, and Nonverbal cues. This tells the researcher that what the person stated was important for them to state, however, the response gives proof that they may not have understood the difference between the techniques. Based on research into the

sociology of why people do not answer these questions, and the interview with the person from NIST, these questions were most likely not answered because of the lack of knowledge of how the questions were going to be used.

For the section of the questionnaire involving what works for defense against Phishing, Vishing, and Smishing, the one person to answer put the same answer for all of them: “User education in combo w/ consistently followed protocols within the company.” This consistent thought gives rise to the idea that the research may have been too granular for these as phishing, vishing, and smishing are all basically the same thing using different platforms. This section shows that this person sees user education, security protocols, and consistent implementation of security protocols as the best defense to phishing, vishing, smishing.

For the last question in this section about Impersonation this same person stated:

> Giving people an easy way to look up a person within their organization. Impersonation works best in large organizations where it’s conceivable to interact with someone you’ve never met before who has just been hired yesterday. If you’re worried about this kind of attack, making sure people have swift access to an org chart is essential [.]

This is a well-thought-out response and it tells the researcher that Impersonation is something this person sees as a high potential of happening. This answer gives more credence to the idea that phishing, smishing, and vishing should have been one question and that this could have shortened the survey.

Of the 12 surveys, only one person answered this section. It shows that to that one person this was important enough to take the time to answer. However, there is not enough data to give statistical evidence of the significance of any outcomes.

4.2.3 Nominal variable questions.

For our survey, we asked three nominal choice questions. The first question:

1. What forms of information gathering do you perform?

This solicited all three answers, although as noted in Appendix E, a majority of the respondents stated both A & B. This question was not in the list of research questions to be answered but was merely an ice breaker for the survey. It was believed that actual social engineers would answer *both* or *online*. But it was shown that all three answers seemed viable. Based on my research none of the social engineers should have answered just “Physical gathering of information through surveillance or going through trash or other physical means.” This seems like the answer of someone who is a confidence man, and not a social engineer.

Both of the following questions required specific knowledge of the topic of social engineering:

2. Which of these defensive techniques warrants more user education than others?

For this question the two persons that answered both answered that “Defense against phishing” warrants more user education. This is consistent with the fact referenced from the Verizon DBIR for 2021 that phishing consists of 36% of all attacks reported.

3. Of the vectors that have been used to start a social engineering contact which do you feel is most productive?

This question was answered by 2 persons. One person answered *Impersonation* and one person answered *Phishing*. Impersonation can imply in person, over the phone (Vishing), through text message (Smishing), even phishing, or more specifically spear phishing. Spear phishing, not already defined, is a form of phishing that targets specific persons for an attack.

The three questions were not answered by enough persons to warrant any form of statistical analysis. The last two questions were answered in a manner consistent with industry articles and reports, some of which were mentioned in this thesis. This consistency with industry opinion may mean that the persons that answered have read these articles or may mean that they have actually answered in earnest.

4.2.4 Demographic questions.

The demographic section was only answered by two people. Both respondents were female, one a public servant, one a technical program manager. One respondent was from the Triad (the piedmont region of North Carolina), the other was from San Francisco, CA. One of the respondents that answered was in the 25-34 range and the other was in the 35-44 range. Much of the reason this section was not answered may be due to the private nature of social engineering.

The section about what could have been done differently was not answered by any participants. This is partly due to individuals giving up at an earlier point in the survey. Only one person left an additional comment; a quote from a movie “be excellent to each other.”(Kroopf,S.,Murphy,M.S.,Soisson,J.,Herek,S. 2002) No other comments were made.

It should be noted that the research did not anticipate the necessity of trust relationships that are required for the completion of a successful survey with this population. The interviewee confirmed the researcher’s assumption that after 2 months of the survey being available, the survey would have gotten better responses had the researcher been a known entity to the groups being surveyed. This would have been

helped by going to message boards and posting, asking questions, and giving tips and hints to relevant topics to prove the researcher's in-group status.

4.3 General Findings

The general findings of the survey project were more sociologically related than they were computer science-related. The findings show that for the attempt to interact with persons defining themselves as social engineers, coming at them from being an unknown in their social circles is not the approach to get answers to a survey about what defensive techniques work best against them. These questions would have worked better coming from a known entity, such as a known hacker, social engineer, or someone with credentials better verifiable than a student at a university. This was made clear through an interview. While surveys of this nature have been done in other disciplines involving deviant behavior, the researcher's approach was not fruitful. In the discussion section of this thesis, the researcher discusses how a future investigator could rectify what was done incorrectly here.

CHAPTER 5. DISCUSSION

5.1 Introduction

In this section, the discussion covers why and how the survey did not collect enough data to reach its full potential. First, the researcher did not take the time necessary to become a visible part of the online community. Becoming a known entity in the cybersecurity community and potentially more worthy of trust would have allowed more acceptance of guidance in completing a survey. Next, potential participants may have decided that the survey was too long for the reward. Also, there are several reasons why certain questions may not have been answered; these potential reasons are discussed. Finally, social interaction and the human aspect of computer science are side topics that have not been explored in depth. The human aspect of social engineers and their disapproval of “outsiders” is discussed in this chapter.

5.2 Social interaction

Attempting to interact with social engineers can be difficult at best. A group of people who know how to prey on the trust of others is not likely to easily assume that other people are trustworthy. This in and of itself points to a particular need to distrust others as their social engineering activities take advantage of trust for deviant activities.

5.2.1 Defining interpersonal trust.

The first step in understanding the human interaction for this survey is *interpersonal trust* or understanding how people trust others. This is not a simple concept to define and has been interpreted differently by many researchers. For my work, I use Borum’s (2010) work that states that interpersonal trust has:

> elements that referred to (1) a subject, (2) an action/behavior, and (3) a future action (i.e. an intention) and/or expectation (i.e. belief). The future element, which involves predicting or anticipating another's actions, is a distinctive and critical feature of trust. Deception, for example, is about something that has happened or is happening. Trust, however, involves present decisions, often based on another person's past behavior, that require anticipating some action that hasn't yet happened. (p. 8)

Borum's (2010) synopsis of trust research is very in-depth. From this point, he discusses several research projects that have been done in this area going back to Homans in 1958. In Homan's project, he discusses how trust is formed by associations already made. For instance, if someone you trust trusts someone, you can begin to trust from the point of a positive trust attitude with that person instead of a zero-trust point or some negative trust beginning point. Other social beginning points for trust include predeterminations based on someone's mode of dress and previous interactions with persons in that mode of dress. He outlines other beginning points, but they are not relevant due to the survey being online, and the only starting point for a social basis of trust would be from a screen name and first words in a chat room.

Borum (2010) also discusses how there is a neurobiological aspect of interpersonal trust. In this part, he discusses how different parts of the brain have a great deal to do with the trust spectrum. Borum explains that people who are not neurotypical do not start from a zero-trust point. That is partly due to the development, or lack thereof, of certain portions of the brain that contribute to many people being unable to start from this zero-trust point. Because of their brain development, some people are more predisposed to trust people, while people on the other end of the spectrum start from a negative-trust point. Borum also discusses how the brain, or the injection of certain chemicals, can change the point on the spectrum a person starts from given differing levels of oxytocin, vasopressin, and dopamine. While these

chemicals are involved in other activities in the brain, they are also involved in trust and trustworthiness.

Here concerning Borum (2010), and due to the nature of social engineering and its innateness of negative trust, social engineers had no previous trustable actions upon which to base future actions, i.e., taking the survey. They started from a point where they do not typically trust many people outside their social group. This lack of trust is partly due to the nature of social engineering and its taking advantage of trust for deviant activities and results. Had the researcher taken the time to gain some trust in the group, there would have been previous trustable acts to base the future action of taking the survey. Another perspective is that given Homan's ideas, had the researcher made posts to the Reddit forum in the past, joined group discussions, asked questions, and answered questions to the point of acceptance within the group, there would have been a past basis of trust. Then it would have been acceptable to complete the survey as something they were doing as a benefit for a group member to get some of the cost back later.

5.2.2 In-group status.

As defined in this thesis, interpersonal trust is presented to show that the NIST interviewee was correct from a scientific perspective. A person would have been more likely to answer the survey if the researcher had been associated in some manner with the group being surveyed. There would have been no need for deception, as a simple acknowledgment from the majority of the group to which the researcher belonged would suffice for In-group status. Borum (2010) cited research stating,

> Within the in-group there exists a depersonalized bond of trust that extends to all its members; one that is not contingent on other social

> knowledge or affective connections between individual parties. Group membership itself carries the imprimatur of trustworthiness. Some have referred to this as a form of “Category-based trust” (Kramer, 1999) and there is some evidence, as we have seen, that such a category-based trust can help reduce cognitive load in humans by providing mental shortcuts: you can trust person X because they are part of group Y. (Borum, 2010, p. 42)

Because of the lack of face-to-face interaction in an online chat, the people in the group would have only had this association from which to work. The ability to transfer trust is the next theory I discuss.

5.2.3 Trust Transfer Theory.

Stewart (2003) discusses trust transfer in online contexts in her research, specifically how trust can be transferred from known individuals to unknown individuals. She also finds that it can be transferred from a place or an industry association to an individual (Stewart, 2003). She states,

> Campbell (1958) suggested that such perceptions are based on the similarity, proximity, and common fate of entities. He introduced the term ‘entitativity’ to describe the degree to which a collection of individuals is perceived as forming a group. The concept of entitativity allows for the study of collections of individuals who vary along a continuum in the extent to which they are perceived as forming a cohesive unit, rather than forcing such collections to be categorized in a dichotomous fashion as forming a group or not. (Stewart, 2003, pp. 2–3)

This entitativity is varied in its perception from the perspective of entities within the group.

Thus, joining a group of social engineers and fulfilling a role within the group (starting as the new person trying to gather information through asking questions and eventually getting to the point where one contributes to discussion as an equal) is a goal for future research with this population. Once this point has been reached, a certain amount of trust would be transferred, leading to better survey response rates. Ideally,

this would also lead to more honest and thorough survey responses for qualitative and quantitative components. To put this more aptly, the researcher sees that becoming part of the group cohesion through a shared bond would have changed the cost-benefit analysis scale in favor of group members completing the survey as a benefit of being part of the group.

5.3 Use of an Online Survey in General

The value of using an online survey is magnified for social engineers. For example, this may be the only way to contact them as they like to remain anonymous, and sending things to a street address or calling them on the phone would eliminate much of that anonymity. Evans and Mathur (2005) discuss nine potential weaknesses to using online surveys, as discussed below.

5.3.1 Perception as junk mail.

According to Cisco (2021), 84.14% of all e-mails sent in September 2021 were spam. Because of this, survey recipients would likely believe that a survey received via e-mail is some kind of spam, specifically perceiving it as a potential phishing scheme. Part of the reason I surveyed through an interview with the person from NIST was that he stated that I was most likely going to be sending a link to the survey from a source that was not trusted enough for him to open. Because the nature of social engineers is to take advantage of others' trust in the general good nature of people, it could be inferred that social engineers would assume that the survey may have been sent by another social engineer trying to phish them.

5.3.2 Skewed attributes of the Internet population.

While Internet usage can be seen as varying greatly from high-income populations (89%) to low-income populations (14%; World Bank, 2021), Evans and Mathur (2005) also believe from their research that Internet users are typically male. This demographic evidence indicates that the survey is more likely to get answers from affluent males than from impoverished females.

5.3.3 Questions about sample selection.

Using Reddit and Facebook as survey distribution mechanisms was inherently problematic for this population because these two platforms preclude social engineers who do not use these sites frequently enough to see the survey link. Additionally, the previously discussed issue about not being a known quantity in these online communities further skewed the sample population.

5.3.4 Respondent's lack of online experience/expertise.

In this section in Evans and Mathur's (2005) article, the authors discuss the potential that the possible participants would not have the expertise or experience to know that the survey was legitimate or have a frame of reference to know what taking an online survey would mean to them directly. I feel this is currently less of an issue than it may have been when the article was published. The user's expertise identifying as a social engineer would be much higher than the average Internet user. This is partly due to how the typical social engineer uses the Internet to gather information on a potential victim.

5.3.5 Technology variations.

Research by Evans and Mathur (2005) has aged regarding this topic; however, the idea that technological variations would affect the survey is still a valid point. Since many, if not most social engineers want to maintain some level of anonymity online, their trust levels may vary regarding a survey creator and their ability to maintain their chosen level of anonymity. These technological variations would also alter the trust levels in the link used for the survey and may result in the need for interview-style survey responses. Interview style survey responses would most likely need to be Internet chat-based interviews; this is partly due to the need to remain anonymous by the groups to be interviewed.

5.3.6 Unclear answering instructions.

Evans and Mathur (2005) discuss how unclear instructions may cause frustration by the survey taker and therefore result in the survey taker exiting the survey without completing it. This may have been part of the problem with this survey, although more likely due to the technical level of the terminology used in the instructions. While common in industry and academia, these terms may not be as widely used in the common vernacular of social engineers. Their goal is to blend in and seem like they belong in whatever situation they are trying to perform deviant behavior in; as such, many situations do not involve technical jargon unless necessary.

5.3.7 Impersonal.

Evans and Mathur (2005) discuss how online surveys may seem impersonal. This impersonality may be a strength from the perspective of social engineers maintaining their anonymity. On the other hand, the impersonality of the survey does

seem to inversely correlate to the trust of the researcher and the use of the survey itself past the needs of a master's program.

5.3.8 Privacy issues.

Much information has been leaked to the world through the Internet, and social engineers are trained to gather information that does not want to be gathered. However, these social engineers know how to gather information and know that confidentiality is an illusion. Because of this illusion, the social engineers would have to rely on the relative level of trust in the researcher's integrity and the research institution. As such, it was not a surprise when my informant at NIST stated concern about the confidentiality of the survey.

5.3.9 Low Response Rate.

Online surveys "at best attain response rates equal to other modes and sometimes to do worse; and they suggest that the reasons for this merit more study" (Evans & Mathur, 2005, p. 202). Speculation on this would be that the level of trust between two entities online is less than in person. In fact, beyond using a credit card or debit card to buy items offline in a store, there may be little if any trust transferred between the same two entities that then interact online. This is in some situations contraindicated due to the level of persons giving out information or pictures over the Internet to persons who would not be given this information if met in person.

5.3.10 Word choices.

While researching the lack of data collection of the survey, the researcher saw notes in some sources not to use technical jargon with the general population. This is largely due to the idea that varying backgrounds would make knowledge of specific

technical terms not being broadly known. This may have added to the survey not being completed properly as well. The researcher was trying to balance being technical enough to maintain some brevity while not being too concise with the wording of the survey questions. An assumption was made about the widespread knowledge of the jargon used in the survey that should not be repeated; note here that this may make the questions a bit long and therefore present a different reason for not being completed.

5.4 Future Research

It should be noted that a future researcher could take a few years and become a known quantity in the social engineering world, and maybe even attempt to win the social engineering challenge at Black Hat. Another less attainable option is to survey somewhere on the deep web, but this thesis does not recommend that. A third option would be to get involved with a community of social engineers and do interviews with that group. In this option, the idea would be that doing the interviews would further increase the group's trust and give the interviewer a chance to quell any fears of repercussions directed against the individuals who answered the survey through this method. The interviewer would have to assure the interviewee that they would remain anonymous by not asking personal identifying questions.

CHAPTER 6. CONCLUSION

The researcher began by surveying on the Internet. A survey was generated using some Likert-type scale questions, some open-ended questions, a few nominal variable questions, and finally, demographics questions to accomplish this objective. After 2 months of attempting to get answers from the potential 2,246,494 responders, only 12 partial responses were logged. At this point, further research was done as to why the project did not succeed. The researcher recognized the need for interpersonal trust increase to raise the level of data collection. Additionally, research was done on in-group status needs to recruit respondents, and Trust Transfer Theory was discussed concerning the survey project. Finally, there was further discussion about the possible lack of data collection due in part to using an online survey.

The lesson learned here is that the researcher could have received a much higher response rate if there had been a known quantity in the social engineering field. Given the possibility, respondents would have trusted an in-group person well enough to feel confident enough to answer the questions without them being skewed. Lack of trust is part of the nature of social engineers, as their whole existence depends upon taking advantage in some manner of the trusting nature of individuals. The researcher also acknowledges that some of the terms used in the survey are not as widely accepted for their connotation and may not have been understood.

In conclusion, some things could have been done differently with this project. First, the researcher should have taken the time to become part of the social engineering community, as being part of the community would have allowed for a better response to the survey. As a community member, the researcher would have been

seen as an individual with a better cost-benefit analysis that would be beneficial to acquiring responses to the survey. This would have been partly due to the persons feeling that they would receive some benefit in the future from assisting with the survey. Finally, the survey should be undertaken again to improve the understanding of social engineering to better grasp the techniques used and improve defenses.

References

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing e-mail filtering techniques. *IEEE Communications Surveys & Tutorials*, *15*(4), 2070–2090. https://doi.org/10.1109/SURV.2013.030713.00020

Borum, R. (2010). The science of interpersonal trust. *Mental Health Law & Policy Faculty Publications.* 574. http://scholarcommons.usf.edu/mhlp_facpub/574

Carmines, E. G., & Zeller, R.A. (1979) *Reliability and validity assessment.* SAGE Publications, Inc. Https://dx.doi.org/10.4135/9781412985642

Chang, D., Mishra, S., & Sanadhya, S. K. (2017). *Design and analysis of password-based authentication systems* (Doctoral dissertation, IIIT-Delhi).

Chauhan, S. (2015). *Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques* (1st ed.). Elsevier.

Cisco(2021) Vulnerability information. E-mail and Spam Data || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence. (n.d.). https://talosintelligence.com/reputation_center/email_rep

Creswell, J. W., (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Dreeke, R. (2011). *It's not all about "me": The top ten techniques for building quick rapport with anyone.* Robin K. Dreeke.

Diamantopoulos,A.,Sarstedt,M.,Fuchs,C.,Wilczynski,P.,Kaiser,S.,(2012) Guidelines for choosing between Multi-Item and Single-Item Scales for Construction Measurement: A Predictive Validity. *Journal of the Academy of Marketing Science, 40(3),434-49*

Duncan, R. (2018). *Influence versus manipulation: Understanding the difference.* Forbes. https://www.forbes.com/sites/rodgerdeanduncan/2018/12/21/influence-vs-manipulation-understand-the-difference/#1ed7136d470c

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195–219. https://doi.org/10.1108/10662240510590360

Galov,N. (2021,September28) *17+ Sinister Social Engineering Statistics for 2021.* HostingTribunal, Retrieved March 19,2022, from Https://hostingtribunal.com/blog/social-engineering-statistics

Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Wiley.

Gulati, R. (2003). *The threat of social engineering and your defense against it.* SANS Reading Room.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Hadnagy, C. (2014). *Unmasking the social engineer: The human element of security.* John Wiley & Sons.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. John Wiley & Sons.

Harris, P, Taylor, R., Thielke, R., Payne, J. Gonzalez, N., & Conde, J. (2009). Research electronic data capture (REDCap) – A metadata-driven methodology and workflow process for providing translational research informatics support. *Journal of Biomedical Informatics*, *42*(2), 377–381. https://doi.org/10.1016/j.jbi.2008.08.010

Heisenberg, W. (1958). *The physicist's conception of nature* (1st ed.). Harcourt, Brace.

Jacomme, C., & Kremer, S. (2018). *An extensive formal analysis of multi-factor authentication protocols.* CSF'2018 – 31st IEEE Computer Security Foundations Symposium, Jul 2018, Oxford, United Kingdom p1-15. https://doi.org/10.1109/CSF.2018.00008 HAL id: hal-01922022

Jakobsson, M., & Myers, S. (Eds.). (2007). *Phishing and countermeasures.* John Wiley & Sons

Kang, A., Lee, J. D., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security considerations for smart phone smishing attacks. In *Advances in computer science and its applications* (pp. 467–473). Springer.

Karlins, M., & Navarro, J. (2008). *What everybody is saying: An ex-FBI agent's guide to speed-reading people.* Harper Collins.

krb1. (2019, September 25). Back to basics: Multi-factor authentication (MFA). https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

Kroopf,S., Murphey,M.S.,Soisson,J.,(Producers), & Herek,S.(Director). (2002).*Bill & Ted's Excellent Adventure* [Motion Picture}. (Avaiable from Paramount Pictures, 5555 Melrose Avenue, Hollywood, CA 90038)
Likert, R. (1932). *A technique for the measurement of attitudes.* Archives of Psychology.

Maseno, E. M. (2017). *Vishing attack detection model for mobile users* (Doctoral dissertation, KCA University).

Maxwell, E. (2013). Influence vs. Manipulation. *Security Through Education*, *4*(45). https://www.social-engineer.org/newsletter/Social-Engineer.Org%20Newsletter%20Vol.%2004%20Iss.%2045.htm

Merriam-Webster (n.d.) Information technology. https://www.merriam-webster.com/dictionary/information%20technology

Merzougui, W. H., Myers, M. A., Hall, S., Elmansouri, A., Parker, R., Robson, A. D., Kurn, O., Parrott, R., Geoghegan, K., Harrison, C. H., Anbu, D., Dean, O., & Border, S. (2021). Multiple-choice versus open-ended questions in advanced clinical neuroanatomy: Using a national neuroanatomy assessment to investigate variability in performance using different question types. *Anatomical Sciences Education*, *14*(3), 296–305. https://doi.org/10.1002/ase.2053

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: controlling the human element of security*. Wiley.

Neuert, C. E., & Lenzner, T. (2021). Effects of the number of open-ended probing questions on response quality in cognitive online pretests. *Social Science Computer Review*, *39*(3), 456–468. https://doi.org/10.1177/0894439319866397

Ollmann, G. (2007). *The vishing guide.* http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf

Reddit.com: notes from reddit were retrieved on June 19, 2021.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/fi11040089

Saris, W. E. (2014). *Design, evaluation, and analysis of questionnaires for survey research* (2nd ed.). Wiley.

Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science*, *14*(1), 5–17. http://www.jstor.org/stable/3086029
Sonowal, G., & Kuppusamy, K. S. (2018). SmiDCA: An anti-smishing model with machine learning approach. *The Computer Journal*, *61*(8), 1143–1157.

Talamantes, J. (2014). *The social engineer's playbook: A practical guide to pretexting.* Hexcode Publishing.

Verizon (2021), Verizon 2021 Data Breach Investigations Report. Retrieved March 21, 2022 from: https://www.verizon.com/business/resources/reports/dbir/

Willits, F. K., Theodori, G. L., & Luloff, A. E. (2016). Another look at Likert scales. *Journal of Rural Social Sciences*, *31*(3), 126–139. https://egrove.olemiss.edu/jrss/vol31/iss3/6

World Bank(2021) Individuals using the Internet (% of population). Data. (n.d.). https://data.worldbank.org/indicator/IT.NET.USER.ZS

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.

Appendix A- Human Review Board Correspondence

EAST CAROLINA UNIVERSITY
University & Medical Center Institutional Review Board
4N-64 Brody Medical Sciences Building· Mail Stop 682
600 Moye Boulevard · Greenville, NC 27834
Office **252-744-2914** · Fax**252-744-2284** ·
rede.ecu.edu/umcir b/

Notification of Exempt Certification

From: Social/Behavioral IRB
To: Adrian Austin
CC: Te-Shun Chou
Date: 10/22/2020
Re: UMCIRB 20-000735
Survey of Social Engineers

I am pleased to inform you that your research submission has been certified as exempt on 10/22/2020. This study is eligible for Exempt Certification under category # 2ab.

It is your responsibility to ensure that this research is conducted in the manner reported in your application and/or protocol, as well as being consistent with the ethical principles of the Belmont Report and your profession.

This research study does not require any additional interaction with the UMCIRB unless there are proposed changes to this study. Any change, prior to implementing that change, must be submitted to the UMCIRB for review and approval. The UMCIRB will determine if the change impacts the eligibility of the research for exempt status. If more substantive review is required, you will be notified within five business days.

Document	Description
Reddit group Post(0.03)	Recruitment Documents/Scripts
Survey Consent form ADA(0.02)	Consent Forms
Survey of Social Engineers and the validity of Defensive Techniques(0.02)	Study Protocol or Grant Application
Survey Questionaire for Social Engineering defensive techniques(0.05)	Surveys and Questionnaires

For research studies where a waiver or alteration of HIPAA Authorization has been approved, the IRB states that each of the waiver criteria in 45 CFR 164.512(i)(1)(i)(A) and (2)(i) through (v) have been met. Additionally, the elements of PHI to be collected as described in items 1 and 2 of the Application for Waiver of Authorization have been determined to be the minimal necessary for the specified research.

The Chairperson (or designee) does not have a potential for conflict of interest on this study.

Appendix B- Informed consent to participation

Dear Participant,
I am a student at East Carolina University in The Department of Technology Systems. I am asking you to take part in my research study entitled “Survey of Social Engineers and the validity of Defensive Techniques” The purpose of this research is to determine what methods of defense Social Engineers find to be most effective against their penetration methods. By doing this research, I hope to learn which defensive techniques are effective. Your participation is completely voluntary. At the end of this Survey there is a chance to win 1 of 4 amazon gift cards
that will be raffled off. You are being invited to take part in this research because you are part of a group that may identify as social engineers. The amount of time it will take you to complete this Survey is approximately 5-20 minutes. If you agree to take part in this survey, you will be asked questions that relate to social engineering and demographics. This research is overseen by the University and Medical Center Institutional Review Board (UMCIRB) at ECU. Therefore, some of the UMCIRB members or the UMCIRB staff may need to review your research data. However, the information you provide will only be linked to you through a provided e-mail address, if you choose to provide one. Your identity, via the e-mail address will be evident to those individuals who see this information. However, I will take precautions to ensure that anyone not authorized to see your identity will not be given that information. Identifiers might be removed from the identifiable private information, and, after such removal, the information could be used for future research studies or distributed to another investigator for future research studies without additional informed consent from you or your Legally Authorized Representative (LAR). However, there still may be a
chance that someone could figure out the information is about you. Please call Adrian D. Austin at 336-688-2257 for any research related questions. If you have questions about your
rights when taking part in this research, call the University and Medical Center Institutional Review Board (UMCIRB) at 252-744-2914 (days, 8:00 am-5:00 pm). If you would like to report a complaint or concern about this research study, call the Director of Human Research Protections, at 252-744-2914
You do not have to take part in this research, and you can stop at any time. If you decide you are willing to take part in this study, check the Agree box below and the research questions will appear.
Thank you for taking the time to participate in my research.
Sincerely, Adrian D. Austin Principal Investigator

- Yes
- No

Appendix C – Reddit group post

Redditors,

I am a Graduate Student trying to conduct a research study. I have a few questions about Social Engineering/Pen testing and the general consensus on defensive techniques employed to prevent them. At the end of the survey, you be entered for a chance to win one of four $50 Amazon gift cards as a thank you for participating.

For more information feel free to e-mail me at SEResearchECU@gmail.com

(Social Engineering/ Pen Testing are defined as the use of deception to manipulate individuals into divulging confidential or personal information that can be used for fraudulent purposes.)

https://redcap.ecu.edu/surveys/?s=ED7C374MNL

Appendix D - The Questions

1. What forms of information gathering do you perform?
    a. Online search using OSINT tools
    b. Physical Gathering of information through surveillance or going through trash or other physical means
    c. Both A and B
2. Do you find that Multifactor Authentication is a positive defensive technique as part of defense in depth approach?
    a. Strongly disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly agree
        i. If d or e -Have you found a MFA that you find works better as a defense than others what is it?
3. Do you find that e-mail filters are a positive defensive technique as part of a defense in depth approach?
    a. Strongly disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly agree
        i. If d or e - Have you found an e-mail filter that you feel works better as a defense than others what is it?
4. Do you find system patching to be a positive defensive technique as part of a defense in depth approach?
    a. Strongly disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly agree
        i. If d or e -Have you found a preferred method of patching such as use of tracking software, that you feel works better than others what is it?
5. Do you find that good physical security is a positive defensive technique as part of a defense in depth approach?
    a. Strongly disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly Agree
        i. If d or e -Have you found a method of physical security that you feel works better than others what is it?

6. Do you find that Good Security Policy is a positive defensive technique as part of a defense in depth approach?
    a. Strongly disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly Agree
        i. If d or e - Have you found a Security Policy portion that you feel works better than others what is it?
7. Have you found that limiting access by unknown hardware is a positive defensive technique as part of a defense in depth approach?
    a. Strongly Disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly Agree
        i. If d or e -Have you found a limiting technique that works better than others what is it?
8. Do you find User Education is a positive defensive technique as part of a defense in depth approach?
    a. Strongly Disagree
    b. Disagree
    c. Indifferent
    d. Agree
    e. Strongly Agree
        i. If d or e -Have you found a User Education technique that works better than others what is it?
9. What do you feel is the best defensive technique against Communication Modeling and why?
    a. Open ended
10. What do you feel is the best defensive technique against Pretexting is and why?
    a. Open ended
11. What do you feel is the best defensive technique against Convincing people to like the engineer and why?
    a. Open ended
12. What do you feel is the best defensive technique against Influence by the engineer and why?
    a. Open ended
13. What do you feel is the best defensive technique and why against Manipulation by the engineer?
    a. Open ended
14. What do you feel is the best defensive technique and why against Elicitation techniques by the engineer?
    a. Open ended

15. What do you feel is the best defensive technique and why against Nonverbal ques discerned by the engineer?
    a. Open ended
16. Which of these defensive techniques warrants more user education than others?
    a. Password creation techniques
    b. Multifactor Authentication
    c. Defense against phishing
    d. Defense through Security Policy
    e. Defense through Physical security awareness programs
    f. Other [Open ended]
17. Of the vectors that have been used to start a Social Engineering contact which do you feel is most productive
    a. Phishing
    b. Vishing
    c. SMishing
    d. Impersonation
    e. Other [open ended]
18. For Phishing do you feel that there is a defensive technique that works positively against this?
    a. Other [open ended]
19. For Vishing do you feel that there is a defensive technique that works positively against this?
    a. Open ended
20. For SMishing what do you feel is a defensive technique that works positively against this?
    a. Open ended
21. For Impersonation what do you feel is a defensive technique that works positively against this?
    a. Open ended
22. Job title
    a. Open ended
23. Geographical location (no closer than City please, at minimum what region (i.e. Triad area of North Carolina, or Bavaria, Germany)
    a. Open ended
24. Gender
    a. Open ended
25. Age bracket
    a. 18-24
    b. 25-35
    c. 35-45
    d. 45-55
    e. 55-65
    f. 65+
26. Is there anything I did not ask that I should have asked in my survey?
    a. Blank _____

27. If willing would you leave an e-mail address for a follow up on your open-ended questions or to win one of four $50 amazon cards
    a. Blank _____
28. Are there any additional comments that you would like to leave for the survey team?
    a. Open ended.

Appendix E- Survey Synopsis

Of the partially filled out surveys the following information was input into the survey;

1. What forms of information gathering do you perform?
    a. Four of the respondents said both A & B
    b. One respondent stated Physical Gathering
    c. Two respondents stated Online Search using OSINT tools
2. Do you find that multifactor authentication is a positive defensive technique as part of a defense-in-depth approach?
    a. Two respondents Disagree
    b. One respondent was Indifferent
    c. One respondent Agreed
    d. Two respondents Strongly Agree
3. Do you find that e-mail filters are a positive defensive technique as part of a defense-in-depth approach?
    a. Two respondents Disagree
    b. Three respondents Agree
    c. One Strongly Agree
4. Do you find system patching to be a positive defensive technique as part of a defense-in-depth approach?
    a. Two respondents Disagree
    b. One respondent was Indifferent
    c. Three respondents Strongly Agree
5. Do you find that good physical security is a positive defensive technique as part of a defense-in-depth approach?
    a. Two respondents Disagree
    b. One respondent was Indifferent
    c. Three respondents Strongly Agree
6. Do you find that Good Security Policy is a positive defensive technique as part of a defense-in-depth approach?
    a. Two respondents Disagree
    b. One respondent Agree
    c. Three respondents Strongly Agree
7. Have you found that limiting access by unknown hardware is a positive defensive technique as part of a defense-in-depth approach?
    a. Three respondents Disagree
    b. One respondent Agree
    c. Two respondents Strongly Agree
8. Do you find User Education is a positive defensive technique as part of a defense-in-depth approach?
    a. Two Disagree

    b. One respondent Agree
    c. Three respondents Strongly Agree
9. What do you feel is the best defensive technique against Communication Modeling and why?
    a. Only one person answered this question, and they stated the following:

    User education in combination with strong IT sec practices. Getting people to retain some amount of skepticism towards what's asked of them in combo with IT making sure standards are followed so that those in authority are never asking for PII over unapproved channels.

10. – 15 the person basically asked how these things were different from question 9
11. Which of these defensive techniques warrants more user education than others?
    a. Two respondents replied with “Defense against phishing”
12. Of the vectors that have been used to start a Social Engineering contact which do you feel is most productive?
    a. One respondent replied with Impersonation
    b. One respondent replied with Phishing
13. For Phishing do you feel that there is a defensive technique that works positively against this?
    a. One respondent replied with
    “User education in combo w/ consistently followed protocols within the company”
14. For Vishing do you feel that there is a defensive technique that works positively against this?
    a. One respondent replied with
    “User education in combo w/ consistently followed protocols within the company”
15. For Smishing what do you feel is a defensive technique that works positively against this?
    a. One respondent replied with
    “User education in combo w/ consistently followed protocols within the company”
16. For Impersonation what do you feel is a defensive technique that works positively against it?
    a. One respondent replied with:

    “Giving people an easy way to look up a person within their organization. Impersonation works best in large organizations where it’s conceivable to interact with someone you’ve never met before who has just been hired yesterday. If you’re worried about this kind of attack, making sure people have swift access to an org chart is essential”

17. Job title
    a. One respondent replied “Technical program manager”
    b. One respondent replied “Public servant”
18. Geographical location
    a. One respondent replied “San Francisco, CA”
    b. One respondent replied “Triad”
19. Gender
    a. Two respondents left “Female”
20. Age bracket
    a. One respondent left “35-44”
    b. One respondent left “25-34”
21. Is there anything I did not ask that I should have asked in my survey?
    a. Left blank
22. One person was willing to be entered into the drawing for the gift cards
23. Additional comments
    a. One respondent left “Be excellent to each other”[Kroopf,S.,Murphy,M.S.,Soisson,J.,Herek,S. 2002]