**Social Engineering’s Sabotage of Cybersecurity**

Capstone Paper – Final

Alice Mace

Cybersecurity, Bellevue University

CYBR 650: Current Trends in Cybersecurity

Dr. Franklin Hughey

November 6, 2023

**Table of Contents**

**Introduction………………………………………………………………………………….3**

**Social Engineering Tactics…………………………………………………………...…..4**

**Methods of Social Engineering…………………………………………………………..4**

* **Pretexting………………………………………………………………………….…4**
* **Elicitation……………………………………………………………………….……4**
* **Persuasion……………………………………………………………………….….5**
* **OSINT Collection………………………………………………………….………..6**
  + **Figure 1: Social Engineering Pyramid………………………………….7**
  + **Figure 2: Sample OSINT Questions……………………………………..8**

**Cialdini’s Principles of Influence………………………………………………………10**

**Social Engineering Vectors………………………………………………………..……11**

**Phishing…………………………………………………………………………………….12**

* **Figure 3: Spear Phishing Email Example……………………………….…….13**

**Vishing………………………………………………………………………………………14**

**Smishing………………………………………………………………………………..…..14**

* **Figure 4: Wells Fargo SMiShing Attack Example……………………………15**

**Impersonation………………………………………………………………….……..……16**

**Social Engineering in Practice…………………………………………………….……17**

**Attack Locations…………………………………………………………………...……..17**

**Vulnerabilities……………………………………………………………………….….…18**

**Social Engineering Prevention……………………………………………….………..19**

**Physical & Network Security……………………………………………………...……19**

**Mitigation and Prevention Plans…………………………………………………….…20**

**Training and Education………………………………………………………………….20**

**Conclusion………………………………………………………………….…………..….21**

**Bibliography……………………………………………………………………….………23**

**Introduction**

Approximately 98% of cyberattacks incorporate social engineering to be successful (Praveen, 2023). Even the best security methods can fail if a social engineer is given the way in or around these measures. People are both the first line and last line of defense to a network. Developers of security strategies and mechanisms can be defeated by not realizing a potential concern or sharing the precise methods that were designed to protect a network. Users or other personnel can be fooled into sharing information that could be critical to infiltrating a facility, individual account, or the network in whole.

“Social engineering is a type of cyber attack where threat actors attempt to retrieve sensitive information by manipulating people into providing sensitive data, account credentials, or granting access to networks or systems” (PurpleSec, 2023). It can be broken down into four main vectors: Phishing, Vishing, Smishing, and Impersonation; and these ultimately work to “take advantage of the fact that gender bias, racial bias, age bias, and status bias (as well as combinations of those biases) exist” (Hadnagy & Wozniak, 2018). These vectors are successful due to the implementation of persuasion, commonly referenced as Cialdini’s Principles of Influence (Cialdini, 2021). Anybody can be a social engineer. So long as there’s something the social engineer desires and they have the capability to get it, anyone can be their target. Delving into the threat, impacts, and security measures to protect against social engineering attacks will educate organizations on why and how to better protect their networks. Organizations must incorporate strong enough cybersecurity methods to resist common social engineering tactics and limit the impacts of these incursions.

**Social Engineering Tactics**

**Methods of Social Engineering**

* **Pretexting**

There are multiple methods in which to conduct and prepare for social engineering attacks, this section will highlight a few of the key components. Pretexting is “the practice of presenting oneself as someone else in order to obtain private information (Hadnagy & Wozniak, 2018).” This method can be used to impersonate people or create whole new identities that assist in getting the information needed to infiltrate a network and/or facility. The author of *Social Engineering: The Science of Human Hacking*, Christopher Hadnagy, has used this method in nearly every real-world infiltration he’s conducted and had played the role of a fire extinguisher inspector, pest control serviceman, interviewee, out of state manager, human resources representative, and many more. With each carefully crafted persona, he was able to gain entry to the facility needed and execute the tasks he was hired to do. On some occasions, this included places such as the security operations center (SOC) or the network operations center (NOC), from both of which much damage can be done to an organization (Hadnagy & Wozniak, 2018).

* **Elicitation**

When exploring how to get the details needed to conduct pretexting and other social engineering methods, the act of elicitation is key. Elicitation is “the process of getting or producing something, especially information or a reaction” (Cambridge, n.d.), or more simply put “getting information you never ask for” (Hadnagy & Wozniak, 2018). Being able to unsuspectedly get key information to build a new personality, understand physical or network security measures, and get details on network structure to find vulnerabilities is a necessity for a successful social engineering attack. There are several approaches that can be used to assist in effective elicitation strategies. Using ego appeals by being sincere, having the proper level of rapport, and being realistic with complements or other phrases that make people feel good helps to ease the path of getting them to be comfortable with sharing information. Finding mutual interests works in a similar manner and is a common conversation starting strategy. While it is good to already have some base knowledge on the topic, it can also be a useful strategy to deliberately make false statements. Many people will want to correct inaccurate information they hear, especially if they believe they are helping out others that may be confused or got minor details mixed up. This is a great strategy to get clarification or confirmation of information. Lastly, the use of questioning is a prime elicitation tool. Varying between open-ended, closed-ended, leading, and assumptive questions, it’s possible to guide the target toward whatever specific details are desired while at the same time be open to gathering other useful bits of data that may assist with planning or execution of an attack (Hadnagy & Wozniak, 2018)

* **Persuasion**

Social Engineering is an art form just as other types of acting, writing, and skills that evoke emotion and stimulate thoughts. As was seen in the character formation of pretexting and the careful scripting of elicitation strategies, implementing components of persuasion is also a necessary component of social engineering. Specific details and methods regarding forms of persuasion will be covered later while reviewing Cialdini’s Principles of Influence, but the importance of persuasion cannot be omitted. One of the most critical aspects of persuasion is building rapport. Tony Robbins said “Rapport is the ability to enter someone else’s world, to make him feel that you understand him, that you have a strong common bond” (Hadnagy & Wozniak, 2018). This begins with building on the tribe mentality and establishing a commonality that others view you as a part of. Once accepted into a “tribe” others will be more willing to share information. The principles of rapport building are the following: “using artificial time constraints, accommodating nonverbals, using a slower rate of speech, employing sympathy or assistance themes, suspending your ego, validating others, asking how, why, and when questions, making use of quid pro quo, employing reciprocal altruism, and managing expectations” (Hadnagy & Wozniak, 2018). Imploring these skills and techniques helps social engineers to reach desired outcomes while in their reconnaissance and execution phases of an attack. The amount of details one is willing to share and difference in success rates when persuasion and rapport are implemented into social engineering strategies is staggering.

* **OSINT Collection**

How can any of these tactics be completed? Through open-source intelligence (OSINT) one will be able to gather and analyze information that will be the foundation to all other tactics. OSINT should encompass the most amount of time and because of this, it is the largest piece of the social engineering pyramid depicted below. This pyramid depicts each step necessary to plan, execute, and document results from a social engineering attack to help create a successful execution. OSINT is at the roots of this process because the information collected during this phase feeds the others in which we have already touched on or are understood (Hadnagy & Wozniak, 2018).

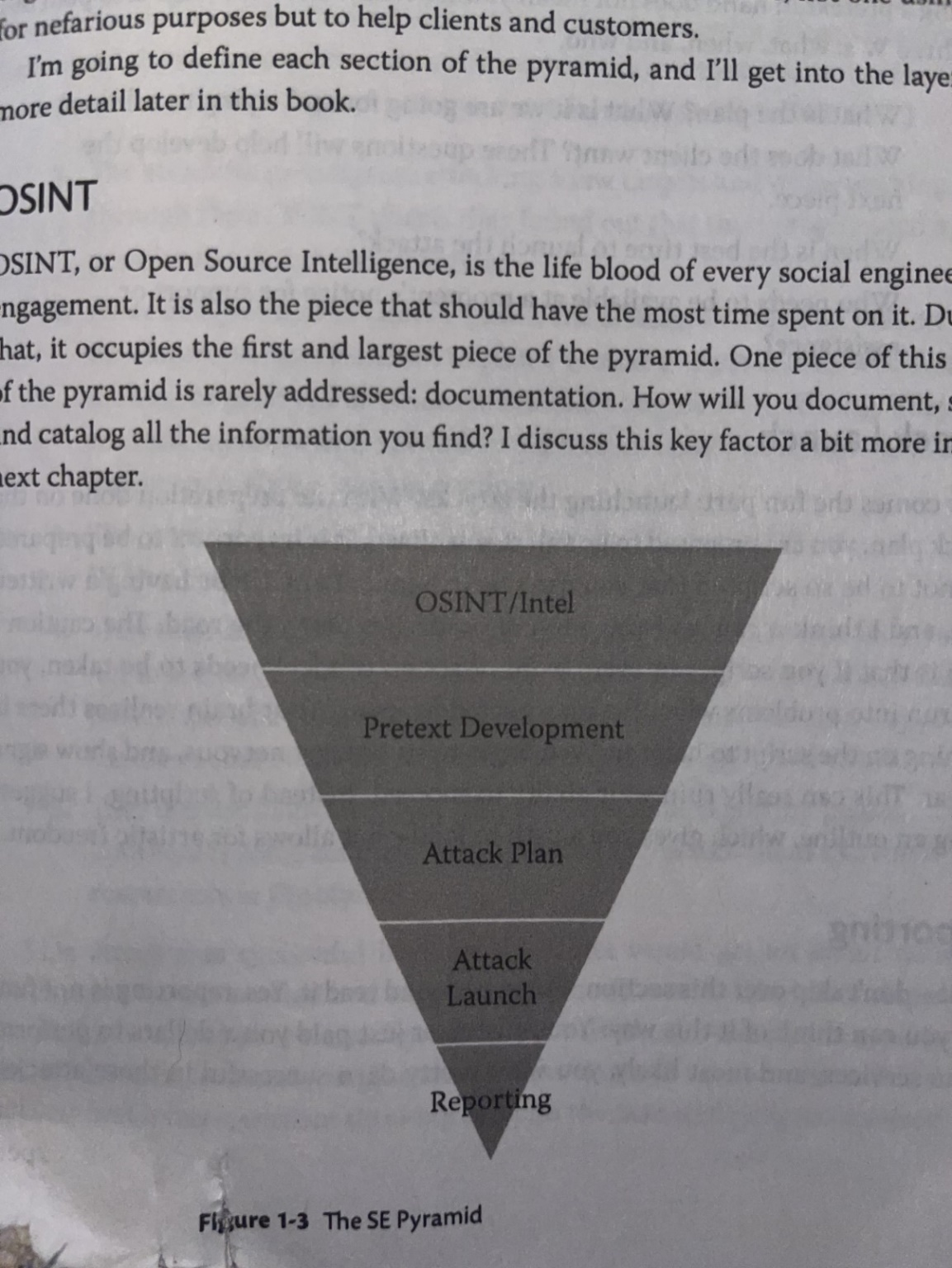


Figure 1: Social Engineering Pyramid (Hadnagy & Wozniak, 2018)

Some forms of OSINT social engineering may not seem that intuitive or foreign processes on their own, but when all combined can create quite a framework for the overview of a target. Establishing potential vectors of approach, parameters of what to dig into, and baselines of how to craft other parts of the social engineering attack are key. The table below provides a useful starting point for corporate or individual targets as to what types of questions should be sought to answer as thoroughly as possible to OSINT means.

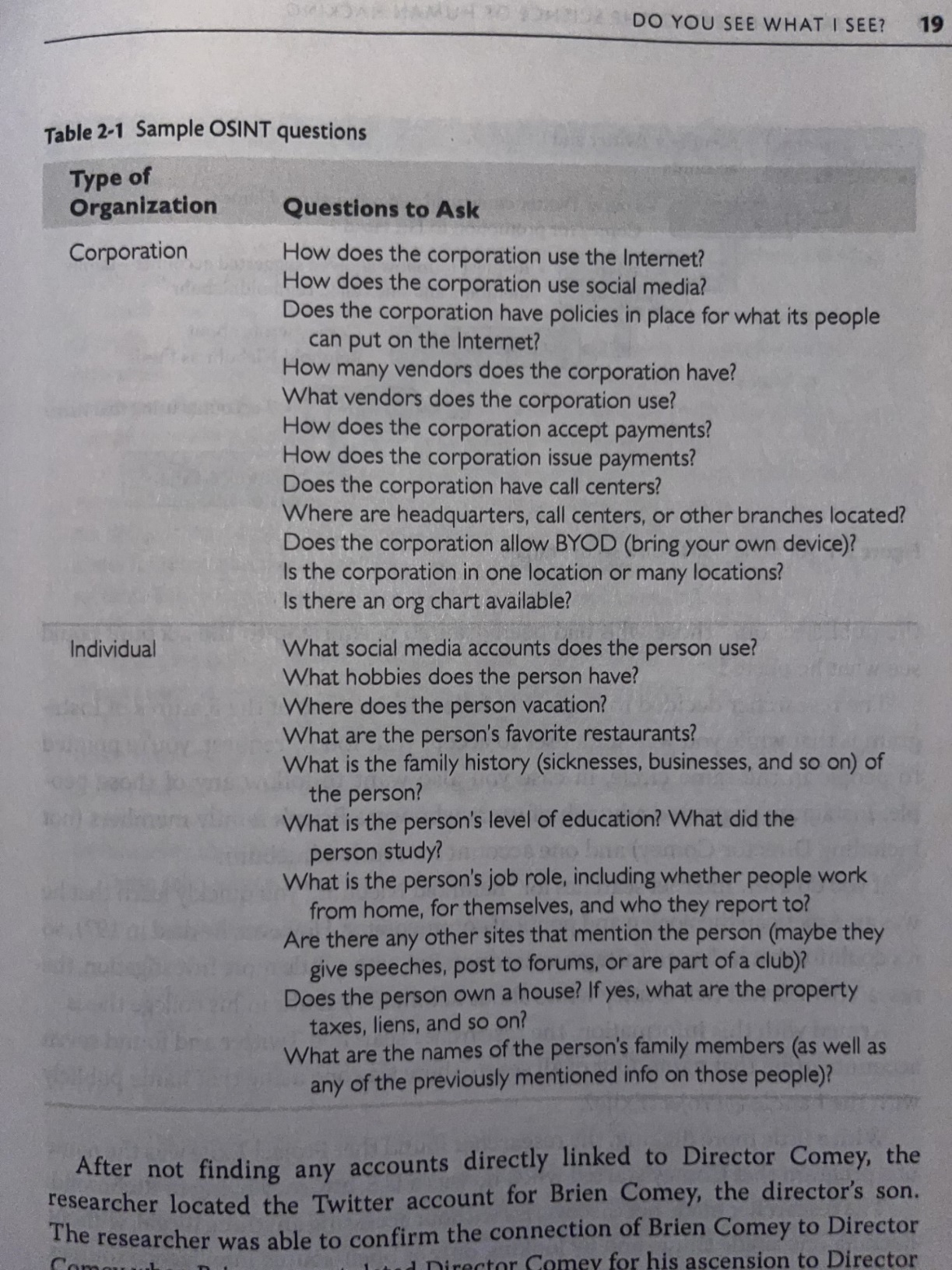


Figure 2: Sample OSINT Questions (Hadnagy & Wozniak, 2018)

Utilizing both technical and non-technical means of collection may be necessary to achieve the level of information desired on a target. Technical OSINT tools involve things like social media digging, probing on various search engines, using translation services to decipher international documentation or determine passwords of foreign targets, accessing webcams that may be openly broadcasting, searching public records, and reviewing other online accounts such as blogs, wish lists, and DNA sites (Hadnagy & Wozniak, 2018). Using other tools with all this data can help truly paint the picture of the target. Maltego is an OSINT tool that “allows you to identify key relationships between information and identify previously unknown relationships between them” (Security Through Education, 2021). There are other technical resources and software, like penetration testing tools, that are more specific to learning about a network, its construct, and potential vulnerabilities it may have. Using whois tools to conduct footprinting and determine IP addresses, domain names, physical addresses, contact information, and more can be an easy method to begin documenting network details.

Using functions through Kali Linux or other tools for scanning and enumeration can provide much more detailed information on IP’s associated with a network, open ports, MAC addresses, and more valuable specifics (Wilson et al., 2021). This information can then be pieced together to determine types of software in use and methods to access the network. Researching Common Vulnerabilities & Exposures (CVE’s) and conducting vulnerability scanning with the data already gained by the previous steps then provides clear targets for social engineers to tailor their efforts on when attempting to infiltrate a network (CVE, n.d.).

For non-technical OSINT collections, one primary ability to have is strong observational skills. Picking up on patterns, processes, and interactions can make or break a scenario because those are what help a social engineer blend into a scenario. Watching facilities and people help to guide on things like clothing, entry/exit points, entry requirements, physical security measures, and facility configuration. Even details such as security guard schedules, common vehicles or deliveries, and security camera locations can be critical to establishing a successful exploitation (Hadnagy & Wozniak, 2018).

**Cialdini’s Principles of Influence**

The prior sections helped to understand how to get the information needed to build a social engineering plan and the methods to be able to construct each process, but execution of the plan is just as important. This section will explore Cialdini’s Principles of Influence which assist the social engineer to get others to believe the role being played and react with the desired outcome. There are seven key principles to the psychology of influence and persuasion (Cialdini, 2021).

1. Reciprocation – The rule or desire to repay someone for what another person provided, usually instilled on feelings of obligation. Ever feel forced to invite someone to a party or get them a gift because they did the same for you? This principle drives that cause.
2. Liking – Getting a “yes” out of someone is easier if they like you. Using strategies to increase likability, such as physical attractiveness or shared similarities, can help get what is desired.
3. Social Proof – This expounds on group think or crowd mentality in that people are more likely to do things they see others doing.
4. Authority – When someone is viewed as in an authoritative position or in charge, others are more likely to do as they’re asked. Even being seen as in union with an authority figure can assist with this influential principle.
5. Scarcity – “People assign more value to opportunities that are less available” (Cialdini, 2021). This is commonly seen in sales practices, but can be used in the essence of deadlines and rushing others to take action now to get what is needed accomplished.
6. Commitment and Consistency – These go hand in hand as they drive how others perceive a person. A security guard stating that written authorization is needed to let you into an area and you come back with a memo or email stating just that with and employee’s name on it will likely get you in, even if they may doubt the written proof. The guard does not want to go back on their word and challenge these two principles.
7. Unity – A more extreme measure of similarities is unity. When someone is considered “one of them” or part of the group, they’re more likely to side with that individual. Unity is typically grouped with those we share identities with and resolve to categories such as race, ethnicity, nationality, family, in addition to political and religious affiliations. It can also encompass class which can be beneficial between working class citizens in equal status helping each other to “just get the job done” and may encourage them to make exceptions to the rules (Cialdini, 2021).

**Social Engineering Vectors**

As previously mentioned social engineering can be broken down into the four main vectors of Phishing, Vishing, Smishing, and Impersonation. These attack vectors “are the methods that adversaries use to breach or infiltrate networks. Malicious actors use a variety of attack vectors to compromise the security of individuals and organizations” (Security Through Education, 2022). Each of these methods incorporate social engineering strategies previously discussed into the attack vectors.

**Phishing**

“In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication” (Security Through Education, 2021b). Goals to be achieved through phishing are described as follows:

* “To deliver malicious payloads that give access to remote attackers
* To gather credentials
* To gather other bits of intel for further attacks” (Hadnagy & Wozniak, 2018).

It’s common practice to use URL and email manipulation by creating a fraudulent website URL or email address that looks similar to a legitimate one to be able to fool targets into believing it is a trustable source. Many phishers will used avenues such as current events, charities, financial institutions, and government agencies to make the phishing attempt seem valid and create a sense of urgency or importance to the email (Security Through Education, 2021b). Once the victim follows the link or opens the attachment to begin the exploit response, the social engineer has already succeeded. The believability and appeal components of developing a phishing attempt are based in social engineering strategies previously discussed. More targeted forms of phishing include spear phishing and whaling. “Spear phishing targets specific higher-profile people who have access to something the attacker wants” (Security Through Education, 2021c). Whaling is similar but targeted to more senior executives, high-level officials, or individuals with access to government information that have credentials or access to valuable information to their business or organization as a whole.

An example of a spear phishing email is below where the target was HR employees and the attacker was posing as the Chief Operating Officer (COO). The attacker’s goal with this approach was to make changes to the payroll direct deposit account. “By posing as the COO, the attacker is hoping for two things; 1.) the HR director will feel pressure to respond quickly and 2.) there will be a higher payout” (Security Through Education, 2021c).

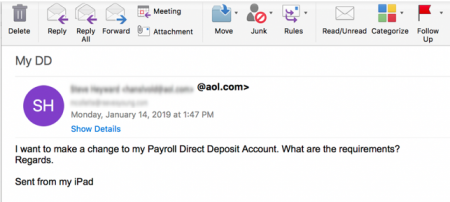


Figure 3: Spear Phishing Email Example

Ransomware is another approach commonly coupled with phishing attacks and executing malicious code that can steal data, lockdown network access, or cause other forms of service stoppages. These coupled with the demand for something in return, usually financials gains, are what make this approach different than another form of cybersecurity attack. This is best summarized with the definition from the FBI, “Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data” (FBI, n.d.).

**Vishing**

The Federal Trade Commission reported in 2020 that phone is still the top way that scammers reach their victims (Vaca, 2022). Vishing, a combination of voice and phishing, is “the practice of eliciting information or attempting to influence action via the telephone” (Security Through Education, 2022c). Vishing can be incredibly useful for a social engineer and provide a great avenue to harvest credentials, collect OSINT, or conduct full compromise of a system with the data achieved (Hadnagy & Wozniak, 2018). The following provides measures used to conduct vishing attacks:

The goal of vishing is to obtain valuable information, contributing to the direct compromise of a target. Attackers may “spoof,” or fake, their outgoing phone number to add authenticity to their attack. Additionally, some bad actors may use voice changers to conceal their identity. They may also use artificial-intelligence based software to mimic authentic voices. In their attacks, bad actors may pose as an authority figure, technician, or fellow employee. (Security Through Education, 2022c)

**SMiShing**

SMiShing is “the act of using mobile phone text messages, SMS (Short Message Service), to lure victims into immediate action. This action may include downloading mobile malware, visiting a malicious website, or calling a fraudulent phone number” (Security Through Education, 2022b). It also aims at influencing victims to return sensitive information such as social security numbers, credit card numbers, account passwords, or provide access to corporate systems. While this did not used to be a widely used attack method, it has increased over the last several years. With organizations allowing Bring Your Own Device policies, it makes this method more appealing to get into a corporate network via the mobile device connections. In 2017, Wells Fargo had a breach due to SmiShing attacks that prompted victims to follow a link containing important information from their security department (Hadnagy & Wozniak, 2018) An example of this attack is shown below:

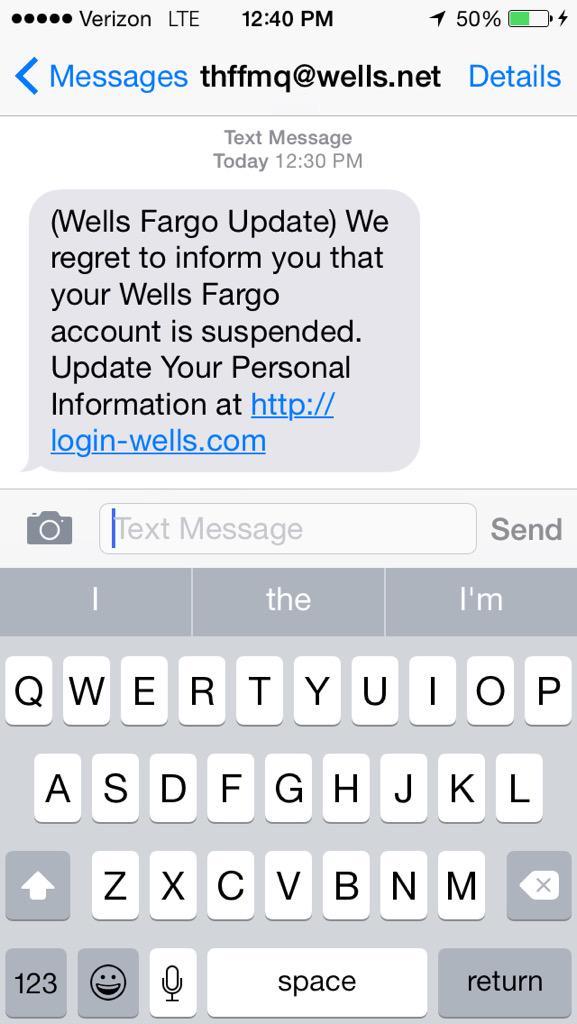


Figure 4: Wells Fargo SMiShing Attack Example

There are three components that have led to the rise of these types of attacks; the increase and widespread use of smartphones, the substantial increase of use of mobile applications for business and financial applications, and COVID-19’s impacts of more remote personnel contributed to an over 300% increase of SmiShing attacks during 2020 (Security Through Education, 2022b).

**Impersonation**

Within the context of social engineering, impersonation is defined as the “practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system” (Security Through Education, 2021c). Pretexting has already been covered, so this section will expound on the implementation of these concepts and give examples of common applications regarding social engineering. Impersonation can be conducted in person or virtually, like phone calls, emails, or text messages. A common impersonation is of technical support personnel. This is an easy method to get individuals to disclose information or allow an attacker into a facility that has restricted access. This makes it easy to insert a USB while “conducting a repair” or gain credentials in the process of “fixing” a user’s account. Another method is of various vendors or delivery personnel like pest control, vending machine supplier, office supply delivery, or DoorDash. Below is a real world implementation of this tactic:

In October 2016, Lukas Yla, posing as a Postmates delivery person, infiltrated some of the largest Bay Area tech and advertising companies delivering donuts. Yla’s intent was not malicious, he just wanted to hand deliver his résume in an unforgettable manner. What made Yla’s impersonation so credible? First, he did research. He started by finding the best donuts in the area. Then, he ordered lunch from Postmates to see how they did delivery. Next, he designed a T-shirt that copied the Postmates logo and found a printing company willing to make the T-shirts. Finally, he hand-delivered donuts and his résume to top executives. How did the executives respond? Yla reports that most were shocked, wondering how he got into the building. (Security Through Education, 2021c)

**Social Engineering in Practice**

**Attack Locations**

It’s easy to get trapped in thinking about social engineering attacks for the purpose of gaining entry to facilities to steal something or exploiting the attack vectors mentioned in the prior section through virtual means. However, understating that social engineering attacks are not bound by location or infiltration method is necessary. Organizations will always have the risk of their physical location being targeted by social engineering experts, as they are the prime target to get direct access to networks and other items of interest. Though, as was noted in the prior section, remote work has increased drastically over the last few years and with it, brought more opportunities to find vulnerabilities and exploit organizations remotely. While the risks of connecting to public networks in coffee shops, hotels, or other locations are well known, it’s often forgotten that home networks can be just as vulnerable. Many organizations have taken to forcing virtual private networks (VPN) to be running before able to access anything within the corporate site, but this does not fully solve device vulnerabilities in someone’s home. Social engineering attacks can occur when the attacker knows there is a corporate device or access to their network in your home and then uses their skills to get inside your own home to conduct their attack. Physical and remote infiltration capabilities make being aware both in the office, on travel, and at home all essential to not falling victim to social engineering attacks.

**Vulnerabilities**

Humans are both the greatest and weakest link in security measures. IT professionals believe new hires to be at high risk as a social engineer’s target and being susceptible to those tactics (Praveen, 2023). New hires, as well as others, fall into the category of unwitting staff that may not intentionally be a vulnerability, but are nevertheless due to their ignorance. The desire to get the job done and to help others to be able to do the same is a common human vulnerability that social engineers exploit to achieve their objectives. The other category of staff vulnerability is insider threats, which is “the threat that an insider will use their authorized access, intentionally or unintentionally, to do harm to the department’s mission, resources, personnel, facilities, information, equipment, networks, or systems” (CISA, n.d.). Keeping tabs on potential indicators like brining in unapproved devices, requesting access to data not needed for duties, uncommon work hours, and unusual data traffic to help prevent social engineering exploitation is a necessary security component (Shastri, 2022).

Network vulnerabilities are challenging to keep track of, but generally are easier to repair. Social engineers will research any details they get on a target organization’s network and try to determine preexisting vulnerabilities. OWASP published a Top 10 vulnerability list and these are the rankings from 2021: Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, and Server-Side Request Forgery (OWASP, n.d.). Many of these that are credential based, or lack thereof, provide the perfect avenue for a social engineer. Others that incorporate different vulnerabilities may still be candidates to exploit depending on what information the attacker is able to uncover about the network. Several of these can cause critical system failures if exploited, so it is essential to mitigate vulnerabilities as soon as possible after discovery.

**Social Engineering Prevention**

**Physical & Network Security**

There are many physical and network security measures that can be put in place to secure a facility and prevent potentially harmful personnel from gaining access, but this section will only name a few key steps. Issuing corporate badges and using multi-factor authentication methods for both physical access and computer access is an effective control mechanism. Visitor policies are necessary to prevent unauthorized personnel from freely wondering around and for employees to escort and hold visitors accountable. Instilling, teaching, and sticking to the policy for visitors is key to prevent social engineers from gaining physical access (Fennelly, 2017). Ensuring the firewall is configured properly is critical for its prime functionality to serve as a defense against harmful data coming in and unauthorized data going out of the network (EC-Council, 2023). Allowing certain automated updates of security software like anti-virus/anti-malware is a good method to keep up with new and evolving threats. Secure data storage and backups that are only accessible by authorized users is valuable and critical to any organization. Verifying that network data storage locations cannot get physically or digitally accessed by potential attackers is vital.

**Mitigation and Prevention Plans (M.A.P.P.)**

A map helps lead toward places and give direction on where to go, and this social engineering M.A.P.P. is no different. The M.A.P.P. has four steps, Identify Social Engineering Attacks, Develop Policies, Perform Regular Checkups, and Implement Security-Awareness Programs. “Help your employee population to understand the value of the information they possess – that emails can be used to breach the whole company; that phone calls are used to get passwords and other sensitive details; that if their mobile device is breached, it can be used to attack their home ad work networks; and that just because a person is smiling and friendly, you can’t ignore the badge policy” (Hadnagy & Wozniak, 2018). Taking the time to have a well thought out policy and ensuring it is understood by employees so they know what to do when an incident occurs is a critical part of a prevention plan. Organizations need a realistic picture of where their employees stand so they know how they might be most vulnerable to a social engineering attack and can take corrective actions. Security-Awareness programs follow this step well in taking that data and developing content that helps to tie all the information together and improve the organization as a whole. This also serves to keep staff updated on new threats and trends and create a security awareness culture in the workplace (Hadnagy & Wozniak, 2018).

**Training & Education**

The mention of annual training requirements is frequently followed by a displeased sigh from employees, but Annual Counter Intelligence Awareness and Reporting (CIAR) training can be much more engaging. While this type of training is primarily focused on counterintelligence, collection by foreign intelligence entities, potential espionage indicators, and signs of terrorism, much of these overlap with social engineering methods and can be applied to detecting insider threats and being more resilient toward other potential threats (DOD CDSE, n.d.). Real world examples of social engineering attack strategies and information gathering methods make a bigger impact on staff. Giving them something realistic followed up with examples of real incidents that social engineering attacks occurred in helps employees to see the application and importance of the training. This can partner with the occasional Red Team exercise to truly test and get real results as to how organizational staff react and respond to social engineering threats.

**Conclusion**

The tactics and methods used in social engineering are not complex on their own and are incorporated in some way into nearly every type of attack. This makes social engineering a greater threat to individuals and organizations than many other types of cybersecurity threats. Understanding and recognizing these tactics can help to ensure the security of both the physical and digital aspects of personal or professional environments. Being aware and cautious toward the social engineering vectors, and incorporating network security parameters to assist in detection and reporting are vital to the safety of organizations. Successful social engineering attacks range widely in their potential impacts, whether physically, digitally, or both. Knowing that it is near certain some component of social engineering will be employed in an attack, it’s essential to have dedicated measures in place to address this strategy. Having strong prevention methods, both standard security and tailored against social engineering, substantially limits the impacts of these methods and attacks. Utilizing two factor authentication, biometrics, access and badge controls, as well as other countermeasures are key to preventing physical access to networks (Fennelly, 2017). Implementing the M.A.P.P. steps of learning to identify social engineering attacks, developing actionable and realistic policies, performing regular real-world checkups, and implementing applicable security-awareness programs is also a valuable prevention practice (Hadnagy & Wozniak, 2018). Organizations must incorporate strong enough cybersecurity methods to resist common social engineering tactics and limit the impacts of these incursions.

**Bibliography:**

Cambridge. (n.d.). Elicitation. Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/elicitation

Cialdini, R. B. (2021). Influence: The psychology of persuasion (Revised). Harper Business.

CISA. (n.d.). Defining insider threats: CISA. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

CVE. (n.d.). Search CVE list. CVE. https://cve.mitre.org/cve/search\_cve\_list.html

DOD CDSE. (n.d.). Counterintelligence Awareness and Reporting Course for DOD. Counterintelligence awareness and reporting course for DOD. https://securityawareness.usalearning.gov/cidod/

EC-Council. (2023, October 27). What is network security? types of network security measures. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/network-security/what-is-network-security-types-network-security-measures/

FBI. (n.d.). Ransomware — FBI. FBI How We Can Help You. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Fennelly, L. J. (2017). Effective physical security (Fifth). Elsevier.

Hadnagy, C., & Wozniak, S. (2018). Social engineering the Science of Human Hacking (Second). John Wiley & Sons, Incorporated.

Praveen. (2023, August 23). Understanding and preventing social engineering attacks. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engineering-attacks/

PurpleSec. (2023, February 22). 2023 Cyber Security Statistics Trends & Data. PurpleSec. https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering

OWASP. (n.d.). OWASP Top 10 2021. OWASP Top 10:2021. https://owasp.org/Top10/

Security Through Education. (2021, February 4). *Maltego*. Security Through Education. https://www.social-engineer.org/framework/se-tools/computer-based/maltego/

Security Through Education. (2021b, March 16). Phishing. Security Through Education. https://www.social-engineer.org/framework/general-discussion/real-world-examples/phishing/

Security Through Education. (2021c, September 7). Impersonation. Security Through Education. https://www.social-engineer.org/framework/attack-vectors/impersonation/

Security Through Education. (2022, February 18). Attack vectors. Security Through Education. https://www.social-engineer.org/framework/attack-vectors/

Security Through Education. (2022b, May 31). Smishing. Security Through Education. https://www.social-engineer.org/framework/attack-vectors/smishing/

Security Through Education. (2022c, May 31). Vishing. Security Through Education. https://www.social-engineer.org/framework/attack-vectors/vishing/

Shastri, S. (2022, July 22). Detecting insider threat indicators - crowdstrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/insider-threats/insider-threat-indicators/#:~:text=Five%20common%20indicators%20that%20an%20individual%20may%20be,of%20recent%20access%20to%20sensitive%20or%20proprietary%20documents

Vaca, M. (2022, May 16). The top frauds of 2020. Consumer Advice. https://consumer.ftc.gov/consumer-alerts/2021/02/top-frauds-2020

Wilson, R. S., Simpson, M. T., & Antill, N. (2021). Hands-on ethical hacking and network defense (Fourth). Cengage Learning.