Cody Cusey

Professor Bryon Steinwand

Application Security – CSCI 276

3 December 2023

**Social Engineering, A Walking Zero-Day Vulnerability**

Social engineering is a manipulation technique used to exploit humans to gain access to confidential information, systems, or physical locations. Unlike traditional hacking methods that rely on technical vulnerabilities, social engineers feast on humans. This can occur through different mediums, including in-person interactions, phone calls, emails, social media. Additionally, it can manifest itself through physical items like fake IDs or USB drives. In this paper, my goal is to delve deeper into understanding the importance of social engineering including: a brief history and evolution, the different attack types, precautionary measures, culture, awareness, mitigation techniques, education, real world examples, and future trends.

**HISTORICAL BACKGROUND**

While the term "social engineering" gained traction in the realm of cybersecurity, its techniques have been used for centuries. Social engineering tactics have been employed in espionage and military strategies throughout history. Spies and agents used deception, manipulation, and impersonation to gather intelligence, infiltrate enemy territories, or gain advantage in conflicts. Before the digital age, confidence tricks, cons, and scams were used by individuals to build trust, deceive, and to swindle money or resources from unsuspecting victims.

**EVOLUTION**

With the advent of telephones, social engineering tactics shifted to exploit this communication medium. Phone-based techniques like pretexting emerged, where individuals posed as authoritative figures or someone trustworthy to extract sensitive information from unsuspecting targets.

Additionally, the rise of the internet and electronic communication further facilitated evolution. Email-based scams became widespread, where cybercriminals sent deceptive emails, posing as legitimate entities, in attempts to trick recipients into providing personal information or clicking on malicious links. Attackers leverage psychological principles, such as urgency, curiosity, authority, and fear, to manipulate victims.

The ever-present use of social media opened new avenues for social engineering attacks. Cybercriminals can easily gather personal information from social media profiles to craft more precisely targeted attacks. Social engineering continually evolves and has gone beyond traditional channels to now attempt exploiting emerging technologies like smart devices, the Internet of Things (IoT), and cloud services.

Attackers are constantly refining their approaches to exploiting human vulnerabilities. They are leveraging new tools and platforms to successfully deploy social engineering attacks. As a result, the landscape of social engineering remains dynamic, demanding ongoing education, awareness, policies, and security measures to aid in mitigating risks.

**ATTACK TYPES**

One of the earliest attack types is known as Phishing. This involves sending emails or messages that appear to be from legitimate sources, tricking recipients into disclosing personal information, passwords, or clicking on malicious links. These emails typically contain urgent requests, alarming statements, or enticing offers, prompting recipients to act immediately, without considering the potential implications.

A less direct method of social engineering is called Pretexting. This is where attackers create a fabricated scenario or pretext to gain a target's trust. They might pose as someone trustworthy, such as a colleague, authority figure, or service provider, to extract sensitive information. They then use this information to perform a secondary attack.

Baiting is another type of attack that functions primarily on physical devices. This relies on the idea of human curiosity. An example is leaving things like infected USB drives in public places to entice individuals to use them. Once the bait device is used or connected to a system, it can install malware or compromise security, enabling the attacker to use said system for personal gain.

Tailgating or Piggybacking is a form of physical security breach where an unauthorized person gains access to a restricted area by following an authorized individual through security checkpoints. Attackers can exploit courtesy by appearing to be in a rush or claiming they forgot their access card. Additionally, they can replicate the attire of employees to attempt to gain access. Regardless of methodology, the attack heavily relies on someone else's access to gain entry without proper authentication.

Another type of social engineering tactic is a classic Quid Pro Quo attack. This typically will involve offering something in return for sensitive information or access. Attackers promise a benefit, such as a gift, service, or assistance, in exchange for the victim's personal information or access to their system. This type of attack stems from historical usage of exploiting people for goods or services.

Each type of social engineering attack exploits human vulnerabilities, leveraging trust, curiosity, or the desire to help. The goal is to deceive individuals or organizations for malicious intent. Being able to recognize these tactics is paramount. Implementing strategies to raise awareness and educate individuals is crucial in defending against social engineering attacks.

**PRECAUTIONARY MEASURES AND CULTURE**

Regardless of technical defenses, the human element will always be the primary vulnerability. Social engineering attacks attempt to exploit human emotions, trust, and behavior to bypass security measures. Companies need to emphasize the importance of ongoing cybersecurity awareness and offer education and training for employees who may potentially fall victim. It is best to encourage a culture of skepticism towards requests for sensitive information or atypical communications.

A security-conscious environment instills a sense of responsibility and accountability amongst all employees. When strict security practices and reporting policies are ingrained in the organizational culture, employees are more likely to comply. If the employee knows the importance of reporting attempted attacks, and to follow the established security policies and guidelines, best practices will likely be implemented by each individual.

**MITIGATION TECHNIQUES AND EDUCATION**

A great way to educate employees is to conduct regular training sessions. These can be used to inform employees about different and emerging types of social engineering attacks. This will also teach them how to recognize attacks as well as best practices for responding to suspicious communications or requests. A more active way to train and test employees is to implement simulated phishing campaigns. This will test employees' ability to identify and report phishing attempts. Additionally, a company should utilize technical controls such as email filtering systems and anti-phishing software to detect and block suspicious emails, reducing the likelihood of phishing attacks reaching employees' inboxes.

Multi-Factor Authentication (MFA) is another great way to enforce security across systems and applications. This control will add an extra layer of security, requiring additional verification beyond passwords for access. Having a secondary layer of employee authentication will greatly reduce the impact of a successful social engineering attack.

Having a schedule for software and system updates is a necessity for any security minded organization. This ensures that all software, operating systems, and applications are regularly updated with the latest patches and fixes to mitigate vulnerabilities that attackers might have or potentially could be exploited.

Physical security measures such as visitor management should be implemented as well. Strict visitor management protocols can be used to prevent unauthorized individuals from gaining physical access to secure areas through tailgating or piggybacking. Along with these protocols, employees should be trained to verify the identity of unfamiliar individuals attempting to gain access to restricted areas or sensitive information.

Conducting regular security assessments, audits, and penetration testing is paramount to identify weaknesses in systems, policies, or employee practices. Use these assessments to improve and update security measures accordingly.

**REAL-WORLD EXAMPLES**

The Equifax Data Breach - In 2017, Equifax, one of the largest credit reporting agencies, suffered a massive data breach that exposed sensitive personal information of approximately 147 million individuals. Attackers exploited a widely known vulnerability in Equifax's website software to gain access to the system and subsystems within. The breach exposed names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers, leading to severe financial and identity theft risks for affected individuals. Equifax faced extensive legal and financial repercussions, including lawsuits and regulatory penalties.

The Twitter/Bitcoin Scam - In July 2020, a significant security breach occurred on Twitter, affecting high-profile accounts like Elon Musk, Barack Obama, and Bill Gates, among others. Attackers targeted Twitter employees through a phone-based social engineering attack, convincing them to provide access to internal tools. Subsequently, the attackers used these tools to compromise and take control of several verified accounts. The compromised accounts posted tweets promoting a Bitcoin scam, asking followers to send cryptocurrency to a specified address, promising to double the amount sent. This scam resulted in financial losses for individuals who fell victim to the fraudulent scheme.

The Bangladesh Bank Heist - In February 2016, cybercriminals attempted to steal nearly $1 billion from the Bangladesh central bank's account at the Federal Reserve Bank of New York. The attackers used a combination of social engineering and malware to gain access to the Bangladesh Bank's systems. They initially sent phishing emails with malicious attachments to bank employees, allowing malware to infiltrate the SWIFT network and obtain credentials. While most of the attempted transactions were blocked, the attackers managed to transfer approximately $81 million to accounts in the Philippines. This incident highlighted vulnerabilities in banking systems and the significant financial risks associated with social engineering attacks.

These real-world examples illustrate how social engineering attacks exploit human vulnerabilities to penetrate even well-protected systems. Despite sophisticated technical defenses, attackers often find success by manipulating individuals through tactics like phishing, pretexting, or exploiting employee trust, resulting in severe consequences for organizations and individuals affected by the breaches.

**FUTURE TRENDS**

As cyber threats continue to evolve, so do social engineering tactics. Several emerging trends in social engineering have been observed, reflecting cybercriminals' ability to adapt to technological advancements including:

AI-Powered Social Engineering, which is where cybercriminals are leveraging artificial intelligence (AI) and machine learning algorithms to create more sophisticated and personalized social engineering attacks. AI tools can rapidly generate convincing phishing emails, chatbots, or voice-based scams that mimic human interaction, making them harder to detect.

Deepfake technology, that enables the creation of highly realistic fake audio or video content. This technology poses risks in social engineering by impersonating individuals in audio or video calls, making it challenging to distinguish between genuine and fabricated communication.

The COVID-19 pandemic, which has given rise to social engineering tactics exploiting pandemic-related fears, misinformation, and remote work scenarios. Scams include phishing emails related to vaccines, fake health organizations seeking donations, or fraudulent COVID-19 relief schemes. This specific trend really emphasizes the psychology of human fear and the ease of abuse and manipulation corresponding to it.

Remote Connections and the increased prevalence of remote work, where cybercriminals exploit vulnerabilities in remote work setups, including insecure home networks, lack of employee training, and reliance on personal devices, to launch social engineering attacks.

**CONCLUSION**

In conclusion, social engineering remains a major threat in the realm of cybersecurity. It’s not just in its technical sophistication but also in its ability to exploit human trust for personal gain. The concept of leveraging humans to breach defenses, compromise sensitive information, and manipulate individuals or organizations will remain prominent. Mitigating this threat requires a multifaceted approach that combines technological advancements, continuous education and training, and robust policies.

Looking ahead, the future landscape of social engineering poses challenges and demands proactive research, innovative defenses, and adaptability to emerging trends. As technology evolves and attackers become more sophisticated, efforts in education, technology development.

**Works Cited**

“Black Hat.” *Five Social Engineering Trends to Watch*, [www.blackhat.com/sponsor-posts/10052021-five-social-engineering-trends-to-watch.html](http://www.blackhat.com/sponsor-posts/10052021-five-social-engineering-trends-to-watch.html). Accessed 4 Dec 2023

“Carnegie Mellon University.” *Social Engineering,* [www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html](http://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html). Accessed 4 Dec 2023

“KnowBe.” (2023, December 1). *Social Engineering: Definition & Examples,* [www.knowbe4.com/what-is-social-engineering/](http://www.knowbe4.com/what-is-social-engineering/). Accessed 2 Dec 2023

“What is Social Engineering?” *What is Social Engineering? | IBM*. (n.d.). [www.ibm.com/topics/social-engineering](http://www.ibm.com/topics/social-engineering). Accessed 2 Dec 2023

“What Is Social Engineering in Cybersecurity?” *Cisco*, 12 Oct. 2023, [www.cisco.com/c/en/us/products/security/what-is-social-engineering.html](http://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html). Accessed 3 Dec 2023

*Avoiding social engineering and phishing attacks | CISA*. (2021, February 1). Cybersecurity and Infrastructure Security Agency CISA. [www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks](http://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks). Accessed 3 Dec 2023

Farrier, Ellie. “What Is Social Engineering? Definition + Protection Tips.” *Norton*, 21 Sept. 2023, us.norton.com/blog/emerging-threats/what-is-social-engineering. Accessed 2 Dec 2023

“What Is Social Engineering - the Human Element in the Technology Scam| Cybersecurity | CompTIA.” *CompTIA.org*, [www.comptia.org/content/articles/what-is-social-engineering](http://www.comptia.org/content/articles/what-is-social-engineering). Accessed 2 Dec 2023