Social Engineering Attacks: Detection and Prevention Techniques

Ryan Seidel, Christopher Corkill, Zac Castaneda, Allison Adams

College of Engineering, Texas A&M University - Corpus Christi

COSC-3301-001: Cyber Security

Dr. Mahboobeh Haghparast

October 30, 2022

Overview

It has often been said that humans are “the weakest link in the information security chain” (Mittal, 2016). Human behavior is often unpredictable and inconsistent: a sampling of traits that make for successful social engineering attacks, although they make for the downfall and exploitation of a user.

The following paper will provide an overview of social engineering and a description of some typical attack genres, helpful prevention measures, as well as risk mitigation techniques after an attack has occurred.

What is social engineering?

Social engineering is an umbrella term in cybersecurity, given to mean any strategy relying on human interaction that a threat agent may use, in order to gain access to a system or network. Moreover, social engineering involves “influencing and manipulating persons to reveal sensitive information or granting access to restricted areas” (Uebelacker, 2014). In a social engineering attack, there must be some component of human interaction. The measure of success of a social engineering attack depends on the assailant’s ability to persuade a victim into carrying out a desired action, for instance, such as providing personal information like a password or social security number.

Why is Social Engineering so Effective?

“Authority, urgency, and intimidation are [...] only some of the human weaknesses in a social engineer’s exploitation kit” (Bakhshi, 2017). Despite the presence of social security systems like antivirus software, firewalls, or intrusion detection systems, social engineering attacks are prevalent and pose a great threat. “The revolution of information sharing and communication techniques in order to maximize efficiency in the work process is one of the main reasons for people and organizations falling prey to cyberattacks” (Aldawood et. al, 2020).

Authority

An attacker may impose an air of *authority* onto a user. Uebelacker (2014) states that “[...] there are two types of authority: One based on expertise and one relying on the hierarchical position in an organization or society”. This is proven true in our day to day experiences- we respect and follow people with roles of status, like doctors, lawyers and scientists. Authority tends to intimidate the victim so as to produce a certain action; in a social engineering attack, a feigned authority figure will be better able to get others to comply with their requests. An attacker could manifest as your supervisor, or somebody higher up in the organization.

Urgency

Many attackers will fabricate a sense of *urgency* in their attacks. Specifically, the attacker is striving to generate a scenario where the victim has little to no time to react rationally. Any time you may have received an email where the tone is in distress, this is a smoking gun that is a social engineering attack. Legitimate communication between entities should not incite panic- for example, the IT help desk at a university should not be sending alarmed emails that you must change your password within twenty-four hours notice, or else your account “will be purged from the system”! These scams use [...] urgency to stimulate increased information processing, short circuiting the targeted user's mental resources, thus preventing them from detecting deception" (Naidoo, 2015).

Intimidation

Intimidation is "a type of bullying attack, based in coercion and power to intimidate victims through fear, and thus, obtain information. It is a high effectiveness technique" (Bravo-Torres et al., 2017). There is typically some sort of consequence that bullies the victim into complying. For example, take a circumstance where a "supervisor" at your company sends you an email claiming that some important files were corrupted, and you must now send corrected versions of those corrupted files ASAP- or else the company will lose an important client. This tactic usually utilizes many tools at once; in this case, urgency and authority. By posing as an authority figure who is attentive and upset, the attacker successfully makes the victim uneasy, causing a lessened sense of caution and the divulgence of sensitive data.

Why choose social engineering?

Think of yourself in the shoes of an attacker. Faced with two strategies of gaining entry into a system, which would you prefer? Using complicated hacking expertise and brute force, or taking advantage of the trust of people to breach a system? Most attackers would choose the second option, as psychologically manipulative tactics such as phishing, scareware and ransomware are much more feasible for an attacker to carry out. Fortunately for potential victims (and unfortunately for attackers) cyber defense technologies have become highly viable and capable of protecting against foreign entities. Thus, if there is an opportunity to opt out of attempting to circumvent advanced security measures and still achieve the same end goal (gaining access to a system) an attacker will choose the latter.

Categorization and Description of Types of Attacks

Social engineering attacks are definitely something that every user should watch out for. This is because we as users are the most vulnerable to these kinds of attacks. Some of the more common attacks that can occur are as follows:

Phishing

Phishing attacks are gaining confidential information through fake websites and emails. These attacks often take place through an ad claiming a winning prize, fake offers or deals, and antivirus downloads. These include places for the victims to include secure personal information, for example: authentication information such as birthdays, childhood pets or maiden names, as well as any other confidential personal information. This information is used to bypass security questions on other, high-stakes accounts, such as online banking. Phishing can be broken up into five different categories:

Spear Phishing

Spear phishing is one of the five categories of phishing. Spear phishing is attacking a specific person using information found online. These attacks involve impersonation of the victim on sites and accounts. Due to the nature of this attack it is often left undetected.

Whaling Phishing

Whaling phishing is another of the five categories of phishing. Whaling phishing follows the same steps as spear but rather they target higher ups in companies.

Vishing Phishing

Vishing phishing is a form of phishing where the attacker gains information via a phone call or vocal information. This is often taken from fake bank calls or false warranty claims.

Business Email Compromise Phishing

Business email compromise phishing is using emails from businesses to gain information of higher ups. They take old schedules, past emails, and payments to gather the needed information.

Interactive Voice Response Phishing

Interactive voice response phishing is using pre recorded statements to give off the illusion of a professional business to gain information from the victims.

Baiting

Baiting attacks are a type of phishing attack where attackers create fake links to prizes. These are often links sent to emails entailing messages of “Click here to win!”. When the victim clicks the link it allows viruses to enter the computer and gain information. Baiting attacks can also include USB or similar devices placed in public areas where there is a high percentage of people. The attacker relies on a bystander to pick a said device and plug it into their personal computer. Once plugged in it reacts the same way as the link and steals confidential information via viruses.

Scareware

Scareware attacks are where the attacker relies on fear motivation to gain confidential information. These attacks present themselves as ads claiming you have viruses, or can show themselves as malicious emails. These attacks claim that in order to get rid of the problem listed, you need to download this app, or go to this website, where from there they get your information.

Tailgating

Tailgating attacks are when the attacker gains access to an otherwise unauthorized area, by following them, possibly stating “they forgot their ID or key.” Another way that they may gain access is by asking for the user's phone and downloading malware.

Ransomware

Ransomware attacks are attacks where information is already gained. After the attacker gets information most likely gained from a previously stated attack they then use it to exploit the victim, stating a hundred different things from “If you don’t send me (a certain amount of money) then I will share this to all your friends and family.” to “I know that your username is (this) and your password is (this) so if you don’t send me (a certain amount of money) I will (use this information in some way that extors the victim).” The FBI stated that losses due to ransomware attacks were about $1 billion in 2016 (Saylor Academy).

Prevention Techniques

Defending against social engineering is no small job. Given the multitude of social engineering tactics, prevention and defense needs to take a multi-layered approach that includes creating a security culture within the organization, encouraging the reporting of security breach attempts and suspicious activity, and sensitizing workplace personnel by increasing their ability to detect signs of social engineering activities (Salahdine & Kaabouch, 2019). Aldawood and Skinner (2020) categorize defenses against social engineering into human based and technology-based approaches. Human based approaches include increasing worker awareness, training, auditing and monitoring, and managing access to systems. Technology-based approaches include the use of biometrics, scanning and filtering software, and intrusion detection). Given that social engineering attacks rely on a combination of human decision making and capabilities of technology, it makes sense that defense against such tactics should involve improving user awareness of social engineering threats along with making technical improvements to protect user devices (Koyun & Janabi, 2017).

Social engineering attack strategies often depend on weaknesses of employees. Such strategies often rely on automatic social influence strategies such as reciprocity, reactance, authority, liking, commitment and consistency, and conformity (Workman, 2007; Cialdini, 2001). Given the nature of Social Engineering tactics, the most important and impactful approach to dealing with social engineering is increasing security awareness of all system users (Saleem & Hammoudeh, 2018; Bhusal, 2021). Training employees how to identify and properly handle threats can go a long way in improving security. Given, however, that human judgment is far from perfect, technology-based solutions (use of sensors, artificial intelligence, biometrics, etc.) should always supplement human mitigation techniques (Salahdine & Kaabouch, 2019).

Identifying an organization's susceptibility to attack can assist with the prevention of attacks (Klimburg-Witjes & Wentland, 2021; Salahdine & Kaabouch, 2019). Hiring professionals who can attempt a false attack on a company's system is one way to identify weak points in cybersecurity. Given that cybersecurity is an ongoing process that needs constant renegotiation, frequent risk assessment improves the ability of companies to identify new threats to counter them by revising policy and employing reactionary measures developed by cybersecurity specialists.

Given the extent of the problem, Odey, Eleyan, & Eleyan (2021) suggest that there is a need to make cybercrime laws stricter and that penalties be increased on those committing cybercrime activities such as social engineering. By increasing deterrents to committing cybercrime, enhancing worker''s ability to detect and deal with threats, and employing technological advances in security, companies can maintain a reasonable defense against social engineering attacks and limit the damage resulting from them.

Mitigation Techniques

As time goes on, it is apparent that social engineering attacks are becoming more common, and the perpetrators are becoming more advanced with their methods; which in turn produces a successful harvest and exploitation of data. The entity desiring to safeguard data must enact mitigation techniques to minimize the impacts of exploiting employee vulnerabilities. While human-based attacks are challenging to detect, often due to intruder uniqueness, many mitigation techniques help reduce the impact on individuals, employees, and corporations. Mitigation aims to defend the data that was preserved after an assault on a corporate system or individual, and is typically the last line of defense after prevention systems have failed or succumbed to breach. Minimizing data loss as much as possible is the top priority once an attack occurs.

Developers and programmers are becoming more aware of social engineering threats and producing more resilient products with quality security standards. Because new code is constructed well, loopholes are not as abundant as they used to be and are becoming more challenging for attackers to penetrate, often resulting in less data being lost and stolen. Mitigation techniques are typically based on sound decisions made by a knowledgeable human being and are used to determine whether a particular action is malignant or genuine. The first approach is enforcing auditing and policy in which various security procedures and regulations are implemented to aid detection. Auditing goes hand in hand with a guideline and is a defense strategy that regulates how employees react during an intrusion. The last approach implements education and awareness to discipline employees for preparedness to ensure the security policies and auditing are correctly carried out and followed.

Additionally, after an attack is carried out, several technology-based mitigation instruments may be activated by an entity as an accessory to safeguarding data. One is sensor-based systems that use detecting elements to identify authorized personnel and authentication segments. This technique can utilize adaptive artificial intelligence systems to learn from and respond to a situation. While sensor-based technology is instrumental in detecting phishing and analyzing communications automatically, it is only considered a layer of security and should be in addition to other techniques. On the other hand, biometric-based systems can identify authorized entities from unauthorized entities using unique patterns like fingerprints, facial recognition, iris design, and vocal recordings. Effectively, biometric tests must be conducted on malicious users, thus making it less efficient.

Ransomware assaults, in which criminals hold data hostage by encrypting it and demanding payment to unlock the information, have become increasingly prevalent. These kinds of attacks, as mentioned previously, often target individuals rather than data from a corporation's network or database, often making the attack difficult to detect. Several layers are to be considered when implementing the security policy.

To start, a company's security staff should eliminate all vulnerabilities to prevent hackers from entering the system, spreading ransomware, and stealing sensitive data. In addition to the elimination of exposures, the security staff should regularly back up the data and should safeguard these backups from being harvested or destroyed by an attack and develop a response to attacks while regularly checking its effectiveness.

Secondly, early ransomware detection allows the user to stop or minimize its damage since quick detection allows containment and fast action while the violation is already being conducted. Use of special software can be integrated into an intrusion detection system to be utilized to limit an attack's distribution and effect over an extensive network or database. The containment step strives to restrict an attack from spreading beyond its first detected devices. This step is chiefly based on an endpoint protection system able to deprive the life of the attack and its network linkage, resulting in disconnection from the attacker and prevention of file encryption by the intruder. The eradication component entails the destruction of infected files once the ransomware attack is locked down. It performs by eradicating the attack from the network and replacing infected machines and devices instead of cleaning them to prevent reinfection from hidden malicious files on the devices.

The final step is finding ways to recover lost or damaged files and relocate the uninfected data onto fresh hardware. Once the previously infiltrated system and hardware are replaced, it is vital to perform new backups of the recovered data and store the backup files in a safe location inaccessible to intruders.

Conclusion

Overall, there is an expansive catalog of potential social engineering attacks that exploit typical human nature. After an overview of social engineering attacks, a delineation of some typical attack genres, helpful prevention measures, and finally risk mitigation techniques, this paper hopes to have imparted a considerable level of security competency to the reader.

References

Academy, S. (n.d.). An overview of social engineering: Ransomware attacks. Saylor Academy. Retrieved October 29, 2022, from http://learn.saylor.org/mod/book/view.php?id=29612&chapterid=5162

Aldawood, H. and Skinner, G. (2020). An Advanced Taxonomy for Social Engineering Attacks. *International Journal of Computer Applications, 177,* 1-11. doi: 10.5120/ijca2020919744

Bakhshi, T. (2017). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. *13th International Conference on Emerging Technologies*, 1-6, doi: 10.1109/ICET.2017.8281653

Bhusal, C.S. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security, 12,* 104-114. https://doi.org/10.4236/jis.2021.121005

Cialdini, R. B. (2001). Influence: Science and Practice. Boston, MA: Allyn & Bacon.

Bravo-Torres, J. F., Gallegos-Segovia, P. L., Jara-Saltos, J. D., Larios-Rosillo, V. M., Vintimilla-Tapia, P.E., and Yuquilima-Albarado, I. F. (2017). Social engineering as an attack vector for ransomware. *Conference on Electrical, Electronics Engineering, Information and Communication Technologies,* 1-6, doi: 10.1109/CHILECON.2017.8229528

Klimburg-Witjes, N. and Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology, & Human Values, 46*, 1316-1339. https://doi.org/10.1177/0162243921992844

Koyun, A. and Al Janabi, E. (2017). Social Engineering Attacks. *Journal of Multidisciplinary Engineering Science and Technology, 4*, 7533-7538. www.jmest.org/JMESTN42352270

Mittal, Sandeep. (2016). Understanding the Human Dimension of Cyber Security. *Indian Journal of Criminology & Criminalistics, 34,* 0970 – 4345. https://ssrn.com/abstract=2975924

Naidoo, R. (2015). Analyzing urgency and trust cues exploited in phishing scam designs. *Academic Conferences International Limited.* https://manowar.tamucc.edu/login?url=https://www.proquest.com/conference-papers-proceedings/analysing-urgency-trust-cues-exploited-phishing/docview/1781336050/se-2

Odey, N., Eleyan, A., & Eleyan, D. (2021). A Survey of Social Engineering Attacks: Detection and Prevention Tools. *Journal of Theoretical and Applied Information Technology, 99*, 4375-4386. http://www.jatit.org/volumes/Vol99No18/17Vol99No18.pdf

Salahdine, F. and Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*, 1-17. https://doi.org/10.3390/fi11040089

Saleem, J., and Hammoudeh, M. (2018). Defense Methods Against Social Engineering Attacks. In: Daimi, K. (eds) Computer and Network Security Essentials. Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_35

Uebelacker, S., and Quiel, S. (2014). The Social Engineering Personality Framework. *Workshop on Socio-Technical Aspects in Security and Trust*, 24-30, doi: 10.1109/STAST.2014.12

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security, 16*, 315 – 331. https://doi.org/10.1080/10658980701788165