Social Engineering Final Report

Anna Waldron, Gwendylan Furiato, Alex Xiong

1. Abstract

SE is the weakest aspect in the domain of information security management since it goes beyond technological control and is based on human nature. Emotional nature of humans lends to the issue of knowing better but not doing better since SE takes advantage of exploiting human cognitive biases. Steps towards a solution means shifting the focus away from only considering technological cues which trigger attacks, and put a focus on the behavioral factors associated with SE attacks.

Social engineering attacks have two main categories: human-based Intrusions or the Interactions between the attacker and the victim who possesses valuable information, and technology-based Intrusions or the act of accessing confidential information by employing computer software programs such as pop-up windows, e-mail attachments, and websites, and so on. Some psychological aspects and emotional cues of SE attacks include alternative routes to persuasion which include a central route and a peripheral route. Central route to persuasion is when SE attackers persuade victims to provide wanted information without fabricating unreal scenarios. This direct route depends on logical thinking from the responders typically doesn't work. Peripheral route to persuasion is used to bypass logical argument and counterargument by triggering strong emotions such as fear or excitement to impede the victims ability to logically analyze the situation and respond properly. SE relies on theories of attitudes and beliefs that affect human interactions, such as the differences between the victim's perception of the SE attacker, and the SE attacker's perception of the victim. Techniques for persuasion and influence are used such as relying on peripheral routes to persuasion, which are effective in influencing the victim. Six common factors which constitute effective persuasions are authority, scarcity, liking and similarity, reciprocation, commitment and consistency, social proof.

SE attackers exploit psychological phenomena in order to recognize psychological and behavioral vulnerabilities of the victim. Diffusion of responsibility is used to make targeted victims believe that they are not solely responsible for their actions. It effectively targets the moral duty of the victim when the individual victim conceives that what he/she responds to is of vital importance to the company or its employees. Chance for ingratiation is used to make victims believe that compliance with a request will enhance their chances of receiving some benefit. It's effective when when using authority or the opposite sex. Trust relationship is used to establish trust relationships with intended victims through seemingly innocent conversations or email communications. Human nature is to trust others until they prove they are not trustworthy. It's effective when the victims can recognize the attacker's voice and are willing to converse with and assist the

attacker. Guilt and Sympathy are used by confiding with intended victims that they have failed to accomplish things and the attackers survival solely depends on the victims' assistance, otherwise significant consequences (normally sad or negative) will occur. It’s effective when the victims tend to avoid guilt.

To address the complexities of social engineering, this report explores all aspects of social engineering and its history to propose a policy outline for cyber security teams to adopt to address social engineering attack concerns. The policy states the following. All employees are aware of the security threats from social media platforms. Organizations must educate their employees to spread basic training and awareness. Employee responsibility, roles, and accountability are explicitly described to every employee. Understand Regulatory and legal requirements. Understand Expectations of stakeholders. Implement network security controls and monitor enterprise social media activity. Draft procedures and other instructions in the case of an organizational breach. Include an awareness program which includes the methods of SE attacks, previous SE case studies, types of personalities, and types of persuasion. Allow users to get hands-on experience by carrying out their own SE attacks on other groups of users in a simulated environment. Use a software application to scan for SE vulnerabilities by using employee information. If employees are deemed vulnerable, they will be sent basic training and educational content on SE attacks. Include use of a panic button. Include use of a USB Security test.

2. Introduction

For a long time, social engineers have used numerous cunning tactics to deceive people. The skill of getting access to buildings, systems, or data by abusing human psychology rather than breaking in or utilizing technical hacking techniques is almost as old as crime itself, and has been utilized in a variety of ways for decades. Social engineers strive to lure unwary users into clicking on dangerous links and/or handing over sensitive information by posing as a colleague, a trusted authority, or even a well-known app in the online and mobile eras. An attacker can use this to persuade users to forgo their typical security safeguards, allowing them access to sensitive information. Attackers might approach targets in a variety of ways, including via email, social media, internet adverts, or a single SMS. In 2020, the Federal Trade Commission (FDC) collected more than 2.8 million fraud reports, with phishing scams being the most widely reported category once again, followed by online sales and banking scams. One of the simplest ways to obtain sensitive information is through social engineering, especially if employees haven't been trained to recognize and oppose it. Unfortunately, employees are bound to make mistakes, but by providing regular and relevant hands-on social engineering policies and training, it can prevent the majority of attacks from succeeding. A framework guideline, a social engineering awareness training campaign, and machine learning techniques are all included in our proposed strategy to combat social engineering. Our proposed approach focuses on teaching and educating users to raise understanding of various

engineering attacks, as teaching and informing users is thought to be the most effective way of preventing social engineering assaults.

3. Related Work

3.1 Related Work Overview

Social engineering is a method used by attackers to deceive users in order to gain access to confidential information. As such, social engineering attacks rely on the human factor in order for such attack methods to succeed. Humans will always be the weakest link in cybersecurity, and no solution can completely defend against social engineering attacks.

Numerous different countermeasures have been developed and explored over time, but the occurring main point of focus in each of these methods is to educate and maintain basic training for users and employees. Countermeasures to social engineering have been explored in many different contexts, including the use of policies, awareness programs, and technical solutions. Each of these developed solutions were carefully analyzed and further researched in order to understand how to develop an effective solution against social engineering attacks.

3.2 Existing Framework Policies

The use of policies in an organization is important, as it outlines the expected behavior, responsibilities, and consequences of an employee's role. As such, a strong and well defined policy can ensure that employees perform their daily job functionalities in a safe and secure manner. In terms of social engineering attacks, policies can also successfully countermeasure against a social engineering attack by making what is expected of the employee clear. Employees should know what information is confidential and what is not in order to carry out their day to day roles safely.

Many policies are developed upon frameworks, which include various components that may influence different departments of an organization. Researchers proposed a policy framework called Social Engineering through Social Media (SESM) that mitigated social engineering attacks through social media by using previous IT frameworks to determine the components of the SESM policy framework (H. Wilcox et al., 2016). The SESM framework includes three components: people, process, and technology. The people component focuses on protecting protecting users from SE methods through social media while also detailing user responsibility while using these technologies. The Process component focuses on enterprise social media management and gives instructions on legal and regulatory requirements. The Technology component focuses on the management of technology for the use of social media and SE threats from social media.

While the SESM framework policy has not been put into effect nor has it been tested on an organization (H. Wilcox et al., 2016), the proposed framework

can be considered a starting point for future frameworks that can contribute to the development of policies against social engineering attacks. Varying organizations should include or combine additional components to the proposed framework to make sure that all departments and employees are secure against social engineering attacks. The proposed SESM framework policy influenced the solution described in this paper to recognize and incorporate the most important components needed to ensure that employees carry out their roles in a safe manner and to safeguard them from social engineering attacks.

3.3 Existing Awareness Programs

As stated previously, social engineering heavily relies on human nature and deception in order for social engineering attacks to succeed. It is strongly recommended that employees understand the tactics, be trained, and know other basic information of social engineering attacks to be able to protect themselves and others against social engineering attacks. To create an effective social engineering awareness program, organizations should implement their own social engineering workshops accordingly and perform them routinely to train and update their employees.

The 2019 National Science Foundation Cybersecurity Summit put in effort to implement their own social engineering awareness program to educate and train users (A. Rege et al., 2020). The workshop was developed into two halves; one half included a purely educational program, where participants would be educated on social engineering material. The content included previous social engineering case studies, personality types, attack methods, types of persuasion, and other basic social engineering material. The other half of the workshop involved a simulated environment where participants would be grouped up and then perform their own developed social engineering attacks on other groups of participants to complete a series of tasks. Such tasks involved peeking over a user's shoulder and viewing their phone, or attempting to use a user's phone in a fabricated emergency situation.

After completing the workshop, participants would fill out a short report that included their experience and feedback. Overall, the participants enjoyed the experience and deemed the content informative. The participants were also able to explicitly describe their social engineering attack methods, thus showcasing that they were able to apply the material that they had just learned and develop their own tactics. Based on the results of this awareness program, the solution described in this paper is heavily influenced by what kind of content, materials, and activities should be included.

3.4 Existing Technical Solutions

As far as creating well defined policies and performing educational workshops consistently goes, these countermeasures against social engineering can be considered somewhat inefficient and time consuming since they rely on communication and knowledge being passed down throughout an organization.

WIth the use of vulnerability scanners, organizations and cybersecurity teams can efficiently scan networks and other computer systems to identify any vulnerabilities. Additionally, machine learning technologies can also be used to efficiently identify vulnerabilities by analyzing data sets and other information. Both of these technologies can be especially useful in identifying existing social engineering vulnerabilities through employee data, thus cutting down time and effort in determining the required amount of training.

Researchers have developed a software application that effectively uses both of these technologies in identifying social engineering vulnerabilities by scanning employee information as well as testing and training them against social engineering attack methods (L. Astakhova et al., 2020). Employee social engineering training results and other personal information is first recorded and stored for further scanning. Vulnerability scanning is then performed on employee data and their training results. Machine learning technology is then used to create a phishing email test using employee information and other gathered data from their social media in an attempt to have the employee enter their information. If the employee entered their information in the phishing email test or were deemed vulnerable to social engineering attacks, the software application would send them educational material and other training against social engineering, and store these results for further scanning as well.

Even though the software application was never tested on participants (L. Astakhova et al., 2020), the method was still developed with the purpose to countermeasure against social engineering attacks. The technological implementation of vulnerability scanners and machine learning technologies greatly improved efficiency and time in training users as well as identifying vulnerabilities. However, the use of gathering employee information from social media can be considered questionable, and as such alternative methods to gather employee information to draft up different social engineering tests should be further researched. The software application's implementation and purpose serves as inspiration to this research project into how to improve time and efficiency in training and educating users on social engineering attacks.

3.5 Research Work Contribution

In this research project, each of these developed methods were analyzed to identify what previous components were necessary and important to include in an effective solution against social engineering. Similar to the related works presented, the focus of our solution is to develop an effective countermeasure against social engineering but combine all three methods in a clear and direct proposal. As such, we hope that our solution stands as a starting point for future development against social engineering attacks.

4. Solution

4.1 Problem Overview

Social engineering attacks have become more prevalent and advanced in recent years, especially with many organizations switching to remote work from home jobs in the COVID-19 pandemic. Humans will always be the weakest link in a cybersecurity system, and this is only exacerbated when they are working remotely from their homes. The aftermath of a social engineering attack can lead to further attacks to compromise a user's data or systems, such as ransomware or malware attacks. The rising threat of social engineering and the effects they have on organizations leads us to ask and research on what are some of the most effective ways to mitigate social engineering attacks.

4.2 Solution Implementation and Details

The discussed problem and questions lead us to focus on some of the most effective mitigation strategies against social engineering. As such, the majority of our research work is qualitative and research based. IEEE articles and other scholarly based works were analyzed and selected based on the effectiveness or purpose the results presented. Different social engineering mitigation methods were also identified and researched to further explore other methods as much as possible. Deciding on what was important and what was not needed in our proposed solution was also conducted, and our solution was carefully developed over time. Once research was finished, a proposed mitigation solution against social engineering was drafted that combined all of the strongest and most important aspects from each developed method.

4.3 Solution Discussion

By conducting research on mitigation methods against social engineering, we were able to identify some of the most effective strategies and develop a solution that incorporated some of the most important aspects that would serve as a countermeasure against social engineering attacks. The core aspect of our solution focuses on educating and training users on social engineering, different tactics, and the consequences, as well as cutting down training and communication in an efficient way. Thus, we believe that our proposed solution should serve as an effective mitigation strategy against social engineering attacks.

5. Experimental and/or Theoretical Results

5.1 Results Overview

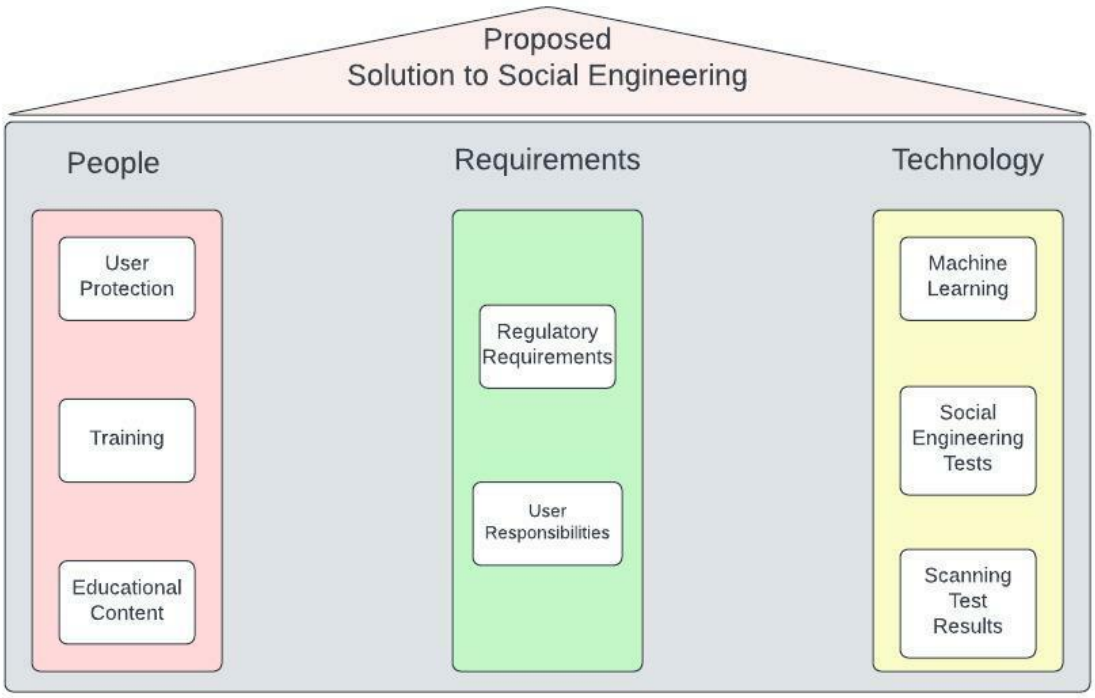
The results of this research was based on qualitative research as well as comparing the developed results of IEEE articles and other scholarly papers. The purpose and how effective each result greatly impacted on our proposed solution, as they were incorporated into the design of our method. Framework policy components, training and awareness programs, and other technological solutions were all incorporated and developed into our proposed solution against social engineering due to their effective methods.

5.2 Results Details

Our proposed solution against social engineering incorporates various aspects and components from a framework policy, a social engineering training and awareness program, and machine learning methods. The main focus of our proposed solution is to train and educate users to spread awareness of social engineering attacks, as training and educating users is considered the most effective way of mitigating a social engineering attack. The results from the social engineering workshop at the 2019 National Science Foundation Cybersecurity Summit further influenced this aspect, as most of the participants deemed the workshop material as educational and informative (A. Rege et al., 2020). Thus, providing training and educational content for users is an integral part of our proposed solution and is included in our solution's People section.

The framework policy's overall design and structure also heavily influenced our proposed solution. The People component focuses on protecting users from social engineering attacks as well as informing them of their responsibilities and potential consequences in a social engineering attack (H. Wilcox et al., 2016). Thus, the expected behavior of the user in a social engineering attack as well as being provided education content was included in our proposed solution's Requirements section to further ensure that the user is protected. The Process component's focus on regulatory requirements (H. Wilcox et al., 2016) is also included in our Requirements section, as performing consistent social engineering training and tests helps to update the user on social engineering attacks.

Finally, technological methods such as machine learning are also implemented in our proposed solution's Technology section. Machine learning methods were used in scanning for social engineering vulnerabilities, specifically in constructing phishing scam tests and sending educational content to users based on their test results (L. Astakhova et al., 2020). The inclusion of machine learning methods helps to reduce time and effort in training users, as verbal communication can be time consuming.



LucidChart Link

5.3 Results Discussion

The result of our proposed solution aims to provide a basis on what is needed to develop a strong method against social engineering. Some components can be considered unnecessary, such as the inclusion of machine learning, but the aspect of efficiency and creating social engineering tests should still be considered. As social engineering relies heavily on the human factor, the result of our proposed solution focuses entirely on informing and training users of social engineering, thus aligning on what we focused on solving. The implementation of our proposed solution includes important aspects and components from other developed solutions that presented positive results or had the purpose of mitigating social engineering attacks, thus showing that our proposed solution is effective. However, this proposed solution and other mitigation strategies against social engineering should be further researched and experimented on to provide results. The addition of more components to our solution should also be considered for diverse and varying organizations, as it may not completely cover every employee. As such, our proposed solution should be considered as a starting point for future research.

6. Conclusions

Social engineering is still a prevalent threat to many organizations, and attackers will only continue advancing their methods. Thus, it is critical that users

and employees are aware of social engineering attacks and are updated consistently about current social engineering threats. In order to mitigate social engineering attacks, our proposed solution focuses on informing users, outlining their responsibilities, and trains them against social engineering tactics. However, this proposed solution must be put in practice in the future and output results in order to test the full effectiveness against social engineering attacks. The lack of real testing on participants would greatly improve the design of our proposed solutions with feedback and experience. Thus, we hope that our proposed solution will be further developed and researched to defend against future social engineering attacks.

7. References

A. Rege, T. Nguyen and R. Bleiman, "A social engineering awareness and training workshop for STEM students and practitioners," 2020 IEEE Integrated STEM Education Conference (ISEC), 2020, pp. 1-6, doi: 10.1109/ISEC49744.2020.9280596.

H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 2016, pp. 1039-1044, doi: 10.1109/ICIEA.2016.7603735.

L. Astakhova and I. Medvedev, "Scanning the Resilience of an Organization Employees to Social Engineering Attacks Using Machine Learning Technologies," 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2020, pp. 606-610, doi: 10.1109/USBEREIT48449.2020.9117746.

Premerger Notification Office, and DPIP and CTO. “New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021.” *Federal Trade Commission*, 22 Feb. 2022, https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

Luo, Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. Information Resources Management Journal, 24(3), 1–8. https://doi.org/10.4018/irmj.2011070101

Roberts, P. (2017, November 9). BadNews: Mobile attackers pivot to malicious ads. The Security Ledger with Paul F. Roberts. Retrieved May 4, 2022, from https://securityledger.com/2013/04/badnews-mobile-attackers-pivot-to-malicious-ads/

“How to Disrupt Attacks Caused by Social Engineering.” *Microsoft Security Blog*,

20 Mar. 2019, https://www.microsoft.com/security/blog/2018/01/10/how-to-disrupt-attacks-caused-by-social-engineering/.

Klimburg-Witjes, N., & Wentland, A. (2021, February 10). Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses. Retrieved from Science, Technology, & Human Values: https://journals-sagepub-com.offcampus.lib.washington.edu/doi/full/10.1177/0162243921992844

Mouton, F., Leenen, L., & Venter, H. (2016, June). Social engineering attack examples, templates and scenarios. Retrieved from ScienceDirect: https://www-sciencedirect-com.offcampus.lib.washington.edu/science/article/pii/S0167404816300268