Social Engineering and Online Scam Psychology

Posted on July 22, 2024

Introduction

New and modern technologies in the world of advancements play a big role in shaping the way people interact with each other through digital platforms which results in individuals' shifting their thinking patterns, internalizing their feelings while communicating, and consuming new information. The world of the internet has created an atmosphere where individuals get scammed and frauds that affect the lives and mental health of the people offline (Guadagno et al., 2009). Therefore, researchers and technology experts have developed the field of Cyberpsychology to mitigate the negative impacts the online or internet world is posing to people. Cyberpsychology and cybersecurity are proven to be effective solutions to various unintended problems rising due to online technology as this field offers a scientific study of the mind and behavior that focuses on the psychological aspects in the context of their interaction with online technology (Maalem Lahcen et al., 2020). It is a significant area of study as technology has impacted several spheres of human life including the psychological sphere in the context of its interaction with the human mind and behavior and their links with technology.

Over the past few years, social engineering has seen an increase in popularity as an attack method used by cybercriminals to obtain information, steal credentials, or take over control of a computer or network. It exploits human psychology by using psychological techniques to trick people into revealing confidential information such as credit card or password details, thus enabling attackers to take control of a victim's account or device. This method of attack exploits a human's vulnerabilities by using psychological methods to persuade a victim into divulging personal or sensitive information (Gulenko, 2013). Social engineering attacks are an emerging threat to companies and individuals, especially in the digital age where individuals often make decisions based on recommendations and data without examining their sources. People unwittingly fall for social engineering attacks not always realizing that they are actually being defrauded. This affects the individuals socially, financially, and mentally and they can experience horrible consequences of being a victim of fraud (Wang et al., 2021). However, these types of attacks can be reduced by training individuals on how to recognize these attacks and developing a more rigorous security protocol. This paper explores the prevalence of social engineering, and social engineering attack used in the typical IT Communications company, and evaluate the consequences, and findings of the scenario. Finally, this paper recommends a psychology-based awareness approach to mitigate the dire consequences of such attacks by promoting an awareness of social engineering attacks.

Anatomy of the Attack

This Vishing and Smishing scam in an IT Communications company followed four significant phases that include reconnaissance, engagement, exploitation, and closure.

The Reconnaissance Phase

This phase entails the collection of the data that was needed to design, implement, and execute the later stages of interaction for the successful engagement with the victim of the scam (Arabia-Obedoza et al., 2020). During the reconnaissance stage, a social engineer would be more equipped to collect facts and information about the victim that later serve as the basis to manipulate or exploit the victim. The scam could involve a caller or text message sender pretending to be an IT department employee or representative of the company claiming that there was a security threat and that they needed the target's login credentials or personal information to fix the issue (Haber and Haber, 2020). During the reconnaissance stage of this type of scam, the attacker might gather information about the company's IT infrastructure and the employees' roles and responsibilities through publicly available sources such as social media profiles or the company website in the targeted department (Yeboah-Boateng and Amanor, 2014). In this scenario, the social engineer used social engineering tactics such as researching the target's personal information from public databases or social media platforms to create a sense of familiarity with the target (Handoko et al., 2015). This information allowed the social engineer to create a vivid picture of the victim that helped him present himself as the right person for the victim.

Engagement

During the engagement phase of the scam, the social engineer used social engineering tactics to gain the target's trust in order to convince the victim that he was a legitimate representative of the company. The scammer might also create a sense of urgency by emphasizing the severity of the supposed security threat and encouraging the target to take immediate action to act quickly to avoid serious consequences (Yasin et al., 2021). He might also use flattery or other psychological manipulation techniques to make the victim feel important and valued which could make the target more likely to comply with the scammer's requests (Handoko and Putri, 2019). This would lead the target to let his guard down and provide the requested information without verifying that the caller or text sender could be a scammer.

Exploitation

In the previous stage where social engineer engaged with the target while asking for personal information such as name, phone, email address, passwords, address, and banking information. The

fraudster then exploited the information they gained to obtain access to the company's network and the target's confidential information for extending further access to the victim's data (Ferreira et al., 2015). This would lead to the fraudster stealing data from the IT Communications company's network and running attacks against the company's computer system to steal financial data. Once the scammer had access to the target's data, he would use it to steal the target's identity and also exploit this information to steal other people's data and money in the company (Parthy and Rajendran, 2019).

Closure

This last phase entails the attacker's want and needs to create a strong impression of legitimacy and credibility by building trust with the target via "questioning" the victim to uncover any other potential weaknesses or threats to further complicate the issue. This would make the target panic as this strategy is the ultimate goal of the fraudsters to make their target panic into handing over personal or work-related information for a quick fix to the issue (Atkins and Huang, 2013). When the phase of collection of data and facts would be completed, the attacker used the data to compromise the security of the target's systems with malicious codes that could disrupt the target's business and financial operations in the closure phase. This would result in serious harm to the individual targeted in the scam, the organization, and society overall (Justin and Anastasios, 2018).

Impact Analysis

Investigating the scenario, it is confirmed that the purpose of the scam was to steal the information of an employee serving in an IT Communications company who was told that the information was required to log back in and fix the problem. This resulted in the attacker accessing the company's resources and potentially causing harm to the individual target as well as other people and the company's finances. The scammer used this type of Vishing and Smishing scam to try to collect payment from the victim for fixing the supposed issue by manipulating the target psychologically into handing over all the facts and information (Montañez et al., 2020). Moreover, the impacts of a Vishing and Smishing scam in an IT Communications company would be severe leading to financial losses, compromised sensitive information, and damage to the company's reputation as well. The financial losses could occur due to theft of funds or damage to IT infrastructure caused by the scam. The financial losses incurred due to such scams included direct loss associated with unauthorized access to company accounts and systems as well as indirect costs such as loss of productivity due to downtime and the cost of investigating and resolving the issue (Drew and Cross, 2013).

In addition to the direct financial losses and compromised information, such scams could also cause a loss of customer trust and result in regulatory fines and legal repercussions for the company if the corporation is found to have failed to adequately protect its customers' or employees' information. Vishing and Smishing scams in this scenario can also compromise sensitive information such as the

target's data and the company's network including personal and financial information, confidential company data, and intellectual property (Montañez et al., 2020). This would result in legal liabilities, damage to the company's reputation, and loss of competitive advantage. Furthermore, these scams definitely violated and damaged the reputation of the IT company by eroding customers' and employees' trust and confidence in the company's security practices. The impact analysis of the Vishing and Smishing scam in an IT Communications company also include the potential legal and regulatory consequences as the company may face lawsuits for failing to protect sensitive and confidential information (Washo, 2021).

Recommended Approach

The psychology-based awareness approach devised to mitigate the impacts of Vishing and Phishing scams in the IT Communications company should specifically focus on changing attitudes and behavior. These types of scams become more sophisticated and aggressive in nature, therefore, the need for a tailored awareness approach is more pressing than ever before. The psychology-based awareness approach "Vishing Security Awareness Project" recommended for the scam is based on the key principle of creating awareness regarding cybersecurity risks. To create awareness among IT Communications employees, the company should utilize the principles of socialization and exposure by engaging the employees in continuous communication on cybersecurity awareness (Zulkurnain et al., 2015).

This approach is devised to help the IT Communications company increase security awareness and the adoption of cybersecurity measures to reduce the risk of cyber-attacks among its employees. Additionally, this approach aims to improve the overall cybersecurity posture of the IT company and strengthen its ability to protect its employees' and customers' identities and information (Alsulami et al., 2021). After the recent Vishing and Smishing scam, the targeted IT company needs to devise a practical approach along with the recommended psychology-based approach to raise awareness of security threats and to positively impact business continuity. In addition to this, the IT Communications company should include regular training and education sessions on how to identify Vishing and Smishing scams or social engineering tactics in order to protect itself from fraud or online scams (Campbell, 2019).

Conclusion

Today, cybercriminals are increasingly using tactics such as Social Engineering, Vishing, Phishing, and Smishing to steal money from organizations and individuals. These techniques rely on psychological persuasion, designed to make targets fall victim to the attack. The present study investigated a scenario where a social engineer used sophisticated psychologically persuasive techniques to trick the target into handing over his personal and confidential banking details. The fraudster targeted both the individual and the IT Communications Company but the scam was particularly designed to exploit

the vulnerabilities of the individual target. Therefore, a psychology-based approach to scam risk mitigation was recommended to recognize, detect, and prevent social engineering attacks. The approach recommended is to increase the accuracy of detection of the Vishing and Smishing scams in the IT Communications company so that social engineering tactics can be stopped and prevented.

References

Alsulami, M.H., Alharbi, F.D., Almutairi, H.M., Almutairi, B.S., Alotaibi, M.M., Alanzi, M.E., Alotaibi, K.G., Alharthi, S.S., 2021. Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia. Information 12, 208.

Arabia-Obedoza, M.R., Rodriguez, G., Johnston, A., Salahdine, F., Kaabouch, N., 2020. Social engineering attacks a reconnaissance synthesis analysis, in: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, pp. 0843–0848.

Atkins, B., Huang, W., 2013. A study of social engineering in online frauds. Open J. Soc. Sci. 1, 23.

Campbell, C.C., 2019. Solutions for counteracting human deception in social engineering attacks. Inf. Technol. People 32, 1130–1152.

Drew, J.M., Cross, C., 2013. Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. J. Financ. Serv. Mark. 18, 188–198.

Ferreira, A., Coventry, L., Lenzini, G., 2015. Principles of persuasion in social engineering and their use in phishing, in: Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3. Springer, pp. 36–47.

Guadagno, R.E., Cialdini, R.B., Amichai-Hamburger, Y., 2009. The social net: The social psychology of the Internet. Oxford University Press: New York, NY, USA.

Gulenko, I., 2013. Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Inf. Manag. Comput. Secur. 21, 91–101.

Haber, M.J., Haber, M.J., 2020. Privilege escalation. Privileged Attack Vectors Build. Eff. Cyber-Def. Strateg. Prot. Organ. 99–116.

Handoko, H., Putri, D., 2019. Threat language: Cognitive exploitation in social engineering, in: Proceedings of the First International Conference on Social Sciences, Humanities, Economics and Law, September 5-6 2018, Padang, Indonesia.

Handoko, H., Putri, D.A.W., Sastra, G., Revita, I., 2015. The language of social engineering: From persuasion to deception. Lang. Civiliz. 136–142.

Justin, S., Anastasios, A., 2018. Social engineering as a threat to societies: The cambridge analytica case. Real Clear Def.

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., Kumar, M., 2020. Review and insight on the behavioral aspects of cybersecurity. Cybersecurity 3, 1–18.

Montañez, R., Golob, E., Xu, S., 2020. Human cognition through the lens of social engineering cyberattacks. Front. Psychol. 11, 1755.

Parthy, P.P., Rajendran, G., 2019. Identification and prevention of social engineering attacks on an enterprise, in: 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–5.

Wang, Z., Zhu, H., Sun, L., 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access 9, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

Washo, A.H., 2021. An interdisciplinary view of social engineering: A call to action for research. Comput. Hum. Behav. Rep. 4, 100126.

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., Wei, Z., 2021. Understanding and deciphering of social engineering attack scenarios. Secur. Priv. 4, e161.

Yeboah-Boateng, E.O., Amanor, P.M., 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 5, 297–307.

Zulkurnain, A.U., Hamidy, A., Husain, A.B., Chizari, H., 2015. Social engineering attack mitigation. Int. J. Math. Comput. Sci. 1, 188–198.