CSIM

Analyzing Techniques of Social Engineering Attacks in Emotional Factors and finding their Recovering Strategies

Pinaki Sahu [1]

[1]International Center for AI and Cyber Security Research and Innovations (CCRI), Asia University, Taiwan,
0000pinaki1234.kv@gmail.com

ABSTRACT

In the world of cyber-attacks, social engineering attacks are becoming terrifying amongst them. The evolution of these attacks aims at a particular individual or organization by finding different ways to acquire the confidential and sensitive data which involves security numbers, records or database and passwords. Social engineering is becoming one of the most challenging for data security which misuses human trust and access their credentials. We delve into types of social engineering attacks, how to classify emotion factors attack, recovery strategies and their prevention procedure.

KEYWORDS Social Engineering, Cyber-attacks, Emotional Factor, Recovery

1. Introduction

In this interconnected digital world, social engineering attack technique are getting popular these days which are executed by cyber-attackers. These attacks are not just opportunistic tricks, they are cleverly planned operations that take advantage of the vulnerability of human nature. The majority of Indians often lacked access to 4G internet and social media platforms until 2016. After Reliance introduced free 4G internet access [1], a significant number of social media accounts were created, giving hackers the chance to conduct unethical attacks on people. Cybercriminals craft their social engineering attacks by targeting individuals and attempting to exploit or threaten them into disclosing confidential personal information. In some cases, the victim doesn't take any action after the cyber-attack because social engineering attacks are successful due to the human emotions like trust, greed, fear, curiosity involved in it [2]. We'll look into the devious tactics used by cybercriminals to carry out these attacks in section. It's similar to studying a magician's tricks, like if you understand how the trick works, it's much more difficult to be fooled. This article aims to expose the attacker's stuff as well as techniques to keep you safe with these attacks. We'll discuss smart strategies and advice to help you and your business avoid falling victim to these clever scams. We won't stop there, though. We are aware that sometimes these attackers manage to breach even the greatest defenses. Because of this, we'll also discuss what to do if you ever fall victim to one of these traps.

2. Related Works

Pethers and Bello investigated on cyber sextortion, which utilizes threats to expose graphic content in order to influence victims. The research looks into how design signals and attention manipulation influence cyber sextortion via social engineering and phishing attack [3]. Arif KOYUN and Al provided a thorough overview of social engineering assaults by addressing its phases, types, methodologies, skills, and strategies for detection and avoidance [4]. "Learn Social Engineering," Ozkaya's book, delves into the art of human hacking. It discusses many techniques and ethical considerations for manipulating human behavior in the context of cybersecurity awareness and prevention. Readers can anticipate insights into social engineering tactics employed by both malevolent actors and security professionals [5]. Yang et al. present a real-time defense system against Web Social Engineering Attacks (WSEAs) during web browsing. They approach the difficulty of identifying and banning WSEAs indirectly

before users engage with dangerous information, focusing on aspects such as transparent overlays and user click tracking, known as Social Engineering Ads (SE-ads) [6]. Jinsol Yoo and Youngho Cho presented an Intelligent Chatbot Security Assistant (ICSA) developed to detect the progress phase of SNS phishing assaults. They use Text-CNN-based attack phase classifiers and AI Chatbot technologies to build on existing social engineering attack cycles [7]. According to Saleem and Hammoudeh, it is critical to protect against social engineering attacks, which can cause social, economic, or reputational harm. They talked about common mitigation measures that people and organizations can use to defend themselves from potentially disastrous attacks [8].

3. Understanding Social Engineering

Social engineering is a crafty and manipulative strategy used by evil persons to get sensitive information such as passwords, addresses, and bank account information by exploiting human vulnerabilities. These attacks are extremely successful and harmful because they prey on our inherent human weaknesses, such as trust, emotions, and behavioral patterns, rather than software vulnerabilities[10]. Although it’s a less technological approach, social engineering is nevertheless a big threat that can cause huge damage to the victims. Criminals frequently use social engineering because it is easier to exploit human trust than complex hacking tactics [9]. For instance, suppose your friend is in emotional distress and needs help paying medical bills immediately, and he provides you the payment details via social media such as Facebook. However, after paying your friend (who you know), you realized that you had sent money to the wrong individual. This is known as a social engineering impersonation attack. You will understand more about these attacks after understanding the social engineering phases in the next section.

10 years back, Yahoo! became the target of one of the most cyber-attacks of the century. During this hack, attackers have been reported to have penetrated Yahoo!'s servers, compromising the account information of a whopping 500 million users. This breach was particularly concerning because the attackers used a technique known as social engineering to bypass the strong layers of security technologies and procedures in place to protect this vast amount of user data. The FBI's statement that social engineering was used in this attack on Yahoo!, an IT giant with significant investments in cybersecurity, highlights the potency of social engineering [5].

3.1. Phases of social engineering

We learned from the last example that it was an impersonation social engineering attack. So, you may be wondering how this attack was carried out. The hacker could impersonate your friend. A hacker can steal your friend's identity, take their profile picture and cover photo, and use their identity to ask for money. So, this type of social engineering attack is in four stages. First is preparation stage, where attack gather information of your friend, second stage is interaction stage where during which the attacker will interact with friends of your friend who are similar to you and win over their trust. The third stage is exploitation, where attacker can ask money from the victim and ended up giving money and last stage is clearing of track, the attacker deactivates the social media and disappear (Fig1).

The steps involeved in a social engineering life cycle are as follows(fig1):

• Preparation: After choosing a target, the attacker would do an extensive investigation to learn as much as they can about the person before developing their attack strategy.

•Interact: The attacker will go closer to the target and try to build rapport by making a connection and earning their trust.

•Exploit: Once a connection has been established, the attacker will use a variety of strategies to force or influence the victim in an effort to gain the required information.

•Clear of Track: After collecting the required information or accomplishing the objective, the attacker will stop contact with the victim to prevent detection, then move on to choose a new target.

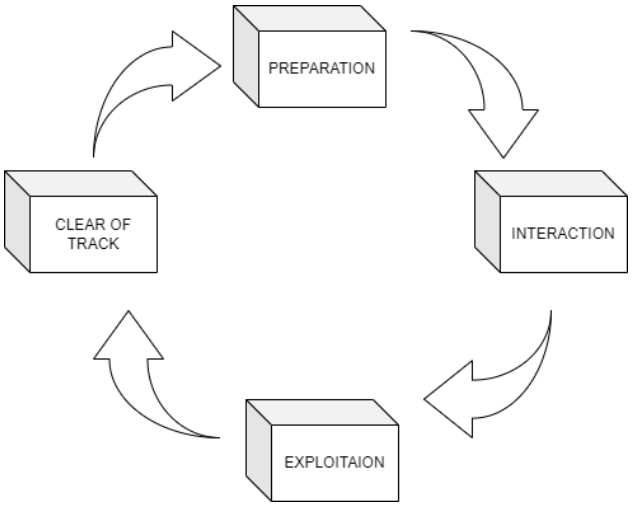

Fig1: Social Engineering attack life cycle

Most social engineering scams rely heavily on direct communication between the attacker and the target. Instead of using brute force tactics to crack the data, the attacker will attempt to convince the victim to compromise themselves.

3.2 Attack Classification

Social engineering attacks can be classified into two categories: Social-based or computer-based as illustrated in Fig2[9]

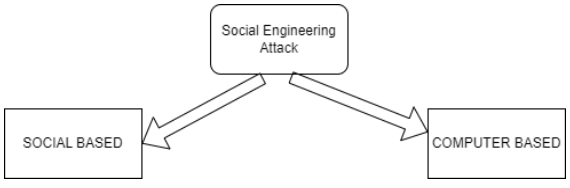

Fig2:Social Engineering Attack classification

Social-based attacks are carried out in person by the attacker interacting with the victim in order to collect the needed information. As a result, they can only influence a limited number of victims. To obtain information from targets, computer-based attacks use devices such as PCs or mobile phones. They can attack a large number of people in a matter of seconds.

3.3 Focus on Social-Based Attacks

Some attacks involving social engineering rely heavily on victim psychology and emotions in order to succeed. These attacks are very sneaky and frequently very effective since they depend on people's support and trust.

From above example from the phases of social engineering, impersonation have been used. In this engineering the emotion factors were trust, helpfulness and empathy exploited in this attack. Likewise other emotions like greed, fear, curiosity and social proof Fig.3.

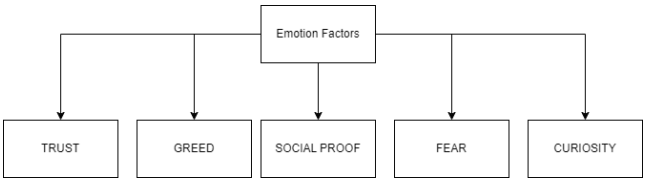

Fig3: Emotions Factor Classification

4.Analysis of Emotional Factor Attacks

Human nature is primarily characterized by emotions, and cybercriminals have gotten better at using these emotions to their advantage in social engineering techniques. These emotional factor attacks take advantage of people's emotions by manipulating their circumstances and leading them to act in ways that compromise their security.
1.Trust: Attackers take advantage of trust which is a crucial element of human relationships by posing as reliable organizations or people. Victims may reveal critical information or follow instructions blindly because they think they are communicating with a trustworthy source, friend, or family. The example which was shown in 3.1, it was trust factor which uses impersonation attack[2].
2.Greed: Greed is frequently a factor in social engineering attacks involving investments. Scammers may advertise fake investment opportunities that guarantee huge profits. Victims may willingly reveal personal and financial

information or spend money in fraudulent schemes because they are motivated by the possibility of instant gain. Some people may laugh at the mails but some of them think that it's a genuine scheme and they end up losing money because the lack of awareness of the attack.

3.Fear: Fear is a strong emotion that can be effectively manipulated in social engineering attacks. Attackers frequently build up terrifying scenarios, such as threatening legal action, account cancellations, or the loss of personal information. Fear-induced victims could quickly agree with requests without confirming the validity of the danger.

In certain cases, cyber-sextortion adds another element of fear by tricking the victim into believing they are a potential partner and gathering personal data about them, including images and videos, in order to later use them as a financial tool [3].

4.Curiosity: Another emotion that cybercriminals frequently prey upon is curiosity. They might create messages or scenarios that spark someone's interest and encourage them to click on harmful links or download dangerous files. People are more prone to take risks without thinking about the consequences after their interest is awakened. Some of the social engineering-ADs are used by attackers to attract the victims to click in [6].

5.Social Proof: People often copy the actions, decisions, or behaviors of others due to the psychological phenomena, based on the idea that if many people are interested in or have already engaged in a particular activity or scheme, it must be worth their attention and trust. Suppose if hacker shows you the evidence that 10 people from your area are subscribed to the scheme then you are more likely to subscribe to scheme.

These where the few emotional factors that leverages social engineering attacks.

5.Recovering Strategies and Prevention Procedure

It can be difficult to recover from emotional factor social engineering attacks, but with the correct techniques and preventative measures, people and organizations can able to mitigate the effects of such attacks and better defend themselves [8].

1.Trust: If you realized that you've been victim of a trust-based social engineering attack then take quick action. Check whether the profile is real or not, confirm with your friends and family to send the money or not. Change your passwords, safeguard your accounts, and notify the appropriate authorities of the event. Even if they seem to come from reputable sources, be wary of unwanted messages or demands. Check the legitimacy of requests before disclosing private information.

2.Greed: If you have been the victim of greed attack, stop communicating with the scammer right now, report the incident to the law enforcement agency, and keep an eye on your financial accounts for any unusual activity. Being aware of the offers that guarantee profits or make unrealistic financial promises, take a step back and seek guidance from your family or financial advisors.

3.Fear: This emotional factor has done the most of cyber-attacks successful. Verify the claims and threats made by the attackers before completing their demand. Report the incident to the concerned authority for cross verification. Have a level suspicion in your mind when you are facing this situation or threat. Seek guidance from reliable sources.

Concerning cyber -sextortion, its critical to be composure when you suspect you're a victim. Resisting the urge to fulfill the attacker's demand. Preserve the evidence related to the attack such as messages, email or screenshots. Report the incident to the cyber-cell or law enforcement agency. Terminate all contact with the attacker. To stop further harassment, block their email, phone number, or social media accounts.

4.Curiosity: Disconnect from the source and refrain from further involvement if you've fallen victim to attacks motivated by curiosity. If you downloaded questionable files, scan your device

for malware and file a report about the occurrence. Train yourself to be cautious when encountering intriguing messages or links. Avoid clicking on unknown or suspicious links and only interact with trusted sources.SE-Ads are the dangerous clickable ads which comes during watching movies from illegal websites. For avoiding or detecting real time virus from the website: Trident defense system that aims to detect and block generic WSEAs in real time [12-14].

Change passwords for your email, social media, and any other online accounts that may have been compromised. Enable two-factor authentication for added security. Turn on two-factor authentication (2FA) for your accounts whenever it is possible. This provides an extra layer of security by requiring an additional verification step. Stay informed about common cyber threats, including cyber-sextortion. Awareness is a powerful tool in preventing victimization. Make regular backups of your critical data and files in a safe location. You can recover your data in the event of an attack without giving in to financial demands.

6.Conclusion

In the digital age, social engineering attacks have grown to be a serious problem since they target people and organizations by preying on human weaknesses. They fool people by appealing to emotions including trust, greed, fear, curiosity, and social proof. It is essential to understand the stages of these attacks because they include planning, interacting, exploiting, and leaving no trace. These attacks, which concentrate on manipulating victims' emotions, can be either human- or computer-based. While greed leads people into fraudulent schemes, trust is exploited by appearing to be trustworthy sources. Victims are pushed into clicking hazardous links out of curiosity and fear is used to threaten legal consequences.

Recovery from social engineering attacks involving the emotional factor is difficult, but it requires quick action and reporting. Vigilance, confirmation, two-factor authentication, and data backups are all part of prevention. In this ever-changing surroundings, knowledge and awareness are essential for defense.

7.References

1. Kalyani, P. (2016). An empirical study on Reliance JIO effect, Competitor's reaction and customer perception on the JIO's pre-launch offer. Journal of management engineering and information technology, 3(5), 18-36.
2. Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks.
3. Pethers, B., & Bello, A. (2023). Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. Future Internet, 15(1), 29.
4. Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4(6), 7533-7538.
5. Ozkaya, E. (2018). Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd5.
6. Yang, Z., Allen, J., Landen, M., Perdisci, R., & Lee, W. (2023). TRIDENT: Towards Detecting and Mitigating Web-based Social Engineering Attacks. In 32st USENIX Security Symposium, USENIX Security (Vol. 2023, pp. 1681-1698).
7. Yoo, J., & Cho, Y. (2022). ICSA: Intelligent chatbot security assistant using Text-CNN and multi-phase real-time defense against SNS phishing attacks. Expert Systems with Applications, 207, 117893.
8. Saleem, J., & Hammoudeh, M. (2018). Defense methods against social engineering attacks. Computer and network security essentials, 603-618
9. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.
10. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social

engineering attacks on social networks. Procedia Computer Science, 198, 656-661.
11. Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.
12. Mishra, A., Gupta, N., & Gupta, B. B. (2021). Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommunication systems, 77(1), 47-62.
13. Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.
14. Wang, T., Pan, Z., Hu, G., Duan, Y., & Pan, Y. (2022). Understanding universal adversarial attack and defense on graph. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-21.