REVIEW ON SOCIAL ENGINEERING ATTACKS AND DEFENSE MECHANISMS

Aanchal Kushwaha, Pramod Singh[1], Dr. Akhilesh A. Waoo[1]

[1] AKS University, SATNA, MP, India

Corresponding Author
Akhilesh A. Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.1887

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Social engineering attacks involve manipulating individuals to disclose sensitive information, compromise security, or perform actions that may not be in their best interest. These attacks exploit psychological and social aspects rather than relying on technical vulnerabilities. Techniques include phishing, pretexting, baiting, and quid pro quo, targeting human susceptibility to persuasion for malicious purposes. Understanding and awareness are crucial in mitigating the risks associated with social engineering attacks.

Keywords: Social Engineering Attacks, Phishing, Baiting, and Pretexting, Defence Mechanism.

1. INTRODUCTION

Social networks face constant and increasing challenges due to social engineering attacks [15]. Human interaction and social engineering attacks are the most powerful attacks because they threaten all systems and networks. They cannot be banned from expanding software or hardware keys as long as individuals are not taught to stop these attacks [1][17]. Today some social platforms like metadata and Twitter have become the largest and most important source of information, data exchange, and online service by its rapid growth. The social network gives full support to find new friends through the exchange of data and thus a new source of information is added to our knowledge [3].

2. SOCIAL ENGINEERING ATTACK

Social engineering attacks are one of the most dangerous and greatest threats and concerns facing cyber security. Through social engineering, it can obtain confidential and sensitive information, and it can be used for such as blackmailing the victim or commercial purposes sold on the black market. Social engineering attacks differ in terms of purpose, target, and reason, they have a common pattern with fixed or approved stages for attackers [11]. The social engineering process has two categories of existing models or frameworks. Firstly, there is a conceptual model. This is

How to cite this article (APA): Kushwaha, A., Singh, A.K.P., and Woo, A.A (2024). Review on Social Engineering Attacks and Defense Mechanisms. *ShodhKosh: Journal of Visual and Performing Arts, 5*(5), 362–368. doi: 10.29121/shodhkosh.v5.i5.2024.1887

grounded on the social engineering attack keys entities [10]. Social engineering attacks are comprised of four phases figure shown in [Fig1].

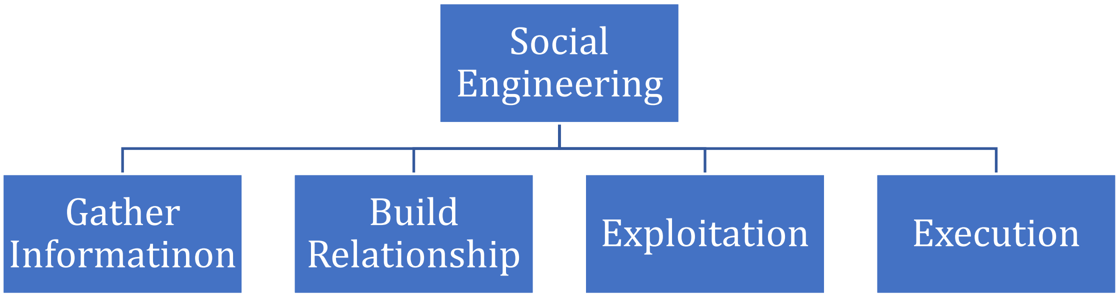

Figure-1: Social Engineering Attack

1.1. Types of Social Engineering Attacks

Social engineering attacks are on the rise in modern networks and pose a significant cybersecurity threat. These attacks focus on manipulating people and organizations to reveal important and sensitive information to cybercriminals. Regardless of the strength of firewalls, encryption methods, intrusion detection systems, or anti-virus software, social engineering can compromise network security. Humans are inherently more trusting of other humans than of technology, making them the most vulnerable part of the security chain. Through psychological manipulation, these attacks can lead individuals to disclose confidential data or violate security protocols [19].

Social engineering attacks pose the greatest cybersecurity threat today, as they manipulate individuals into revealing sensitive information. While these attacks can be detected, they cannot be entirely prevented. Cybercriminals exploit victims to obtain valuable data, which may be sold on the dark web or used for specific purposes. With the rise of Big Data, attackers leverage large datasets to profit by packaging and selling the information in bulk on today's markets [20].

i. **Human-Based Social Engineering Attack -** Social engineering is the psychosomatic influence of people to perform an action or obtain sensitive information like personal data, sensitive information, and confidential information [12].

ii. **Computer-Based Social Engineering Attack -** Social engineering is carried out with the help of computers. The invader uses the procedures to launch more creative, sophisticated, and destructive attacks, such as using a computer or cell phone to enable the attackers to access the information [15].

iii. **Technical-Based Social Engineering Attack-**Technical-based attacks are conducted through the Internet via social networks and online service websites and they collect information such as passwords, credit card details, and emails [1].

iv. **Physical-Based Social Engineering Attack -** Physical-based attacks refer to physical action achieved by the attacker to accumulate evidence almost the target [15].

v. **Social-Based Social Engineering Attack -** Social-based attacks are done by connections with the target to composition on their sensibility and feelings [5].

2.2 Attack Description

Cyberattacks and the risks associated with wireless communication technology have become significant challenges for many government agencies and private businesses globally. As the modern world is increasingly dependent on electronic technology, protecting this information from cyber threats is a complex issue.

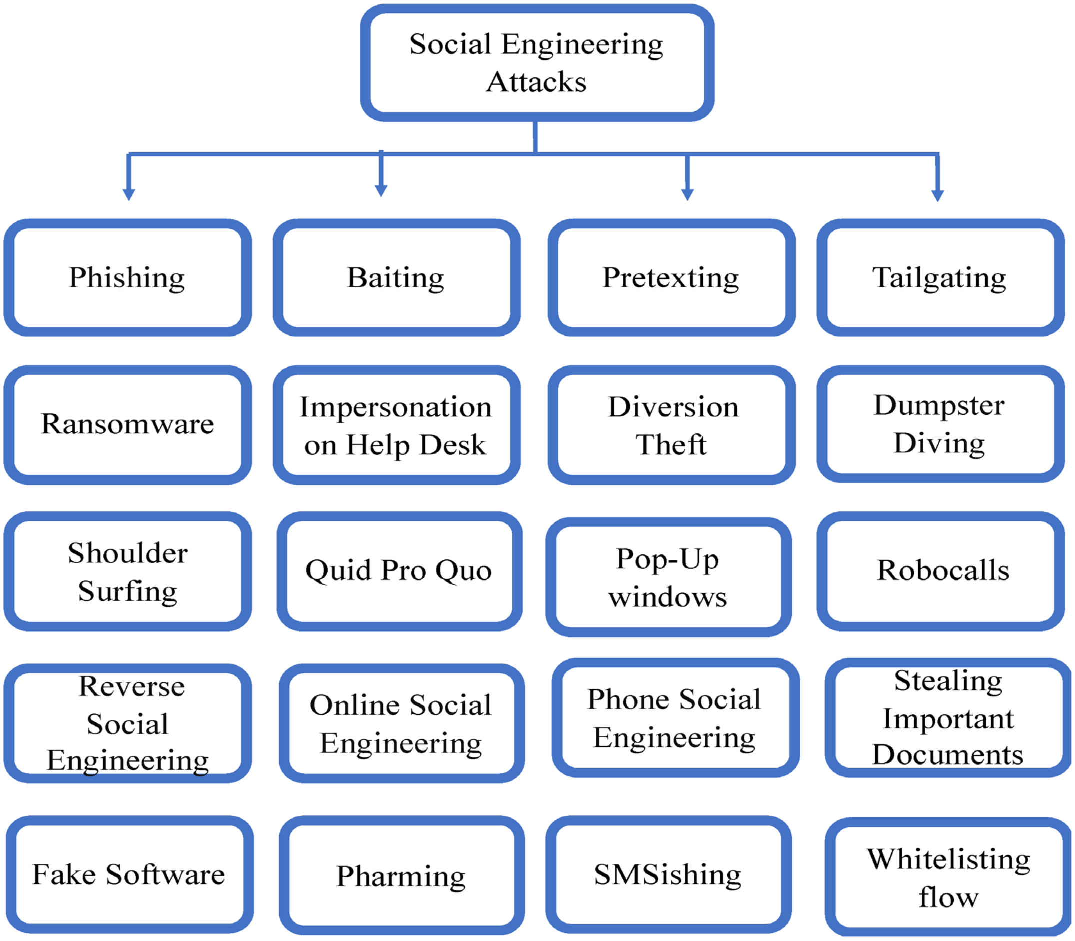

Figure 2: Social Engineering Attack

Cyberattacks aim to inflict financial damage on businesses and may also serve political or military purposes. These threats can include computer viruses, knowledge gaps, data distribution services (DDS), and other attack vectors [21].

2.2.1. Phishing Attack

Phishing is a type of cyber-attack where attackers trick individuals into providing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity. This is often completed over deceiving websites, emails, and messages, aiming to exploit the recipient's truss and prompt them to reveal confidential information [7] figure shown as [fig2].

2.2.2. Pretexting Attack

Creating a false pretext (fake identity) or scenario to obtain information, often through impersonation or building a fake sense of trust [1].

2.2.3. Baiting Attack

Baiting uses a simple method by utilizing members of the organization who have a high curiosity about something. Offering something enticing, like a free download, to lure individuals into taking action that compromises security [8].

2.2.4. Tailgating Attack

Tailgating is a very common type of physical social engineering attacks around the world. Physically following someone into a secure area without proper authorization, taking advantage of trust in a shared environment [4].

2.2.5. Quid Pro Quo Attack

Quid Pro Quo is an attack that reciprocity from a free service or product. Offering a service or benefit in exchange for sensitive information, exploiting the victim's desire for gain [4].

2.2.6. Dumpster Diving Attack

Dumpster diving is the practice of sifting through the trash of private individuals or companies to find discarded items that include sensitive information that can be used to compromise a system or a specific user account [2].

2.2.7. Watering Hole attack

A watering hole describes a targeted attack where the attackers compromise a website that is to be of interest to the chosen victim [4].

2.2.8. Shoulder Surfing Attack

Shoulder surfing refers to expending straight observation methods to acquire data such as looking over someone's shoulder at their keyboards or screen. This technique takes benefit of mortal nature, ignorant of the nearby circumstances when cooperating with contact or important information [4].

2.2.9 Reverse Social Engineering Attack

Attackers create conditions where the victim will fall into the reverse social engineering trap. Attackers make victims of fundamental problems in the organization. Then Attackers come to the target straight or incidentally to offer help [4].

2.2.10. Pop-Up Windows Attack

The window that appears on the user's screen informs him that he has lost his network connection, which requires him to enter the username and password to reconnect so that there are previously installed hidden programs intended to collect this information and redirect it to the attacker [15].

2.2.11. Diversion Theft Attack

This attack uses courier companies to insert malware into a computer or system sent and used by a company [15].

2.2.12. Phone/Email Scam Attack

In this type of attack, the attacker uses the phone or email to influence and deceive the victim to search for money or information or to gain access to the victim's computer [15].

2.2.13. Fake Software Attack

Fake software attacks, also called fake websites, are based on fake websites that make victims believe they are known and trusted software or websites. The target passes real login info into the fake website, which provides the invader the victim's authorization to use genuine websites, like online bank account entree[1].

2.2.14. Robocalls Attack

Robocall attacks have recently appeared as substantial calls coming from computers to victims with well-known phone numbers. It targets cell phones, residential, and work phones [1].

2.2.15 Impersonation on Help Desk Attack

The attacker imagines to be somebody with rights or a company employee and demands from the help desk for information or services.

3. PROCESS OF SOCIAL ENGINEERING ATTACK

Social engineering attacks involve manipulating individuals to gain unauthorized access to information or systems [9, 18].

i. **Target Selection –** Identifying specific individuals or departments within an organization as potential targets [13].

ii. **Planning –** Collection of information about the target, which may be individuals, organizations, or systems. Utilizing online sources, social media, or public records to gather details [6].
iii. **Building Trust -** Establishing rapport and gaining the trust of the target through manipulation or impersonation [14].
iv. **Delivery of the Attack –** Deploying various social engineering tactics such as phishing emails, phone calls, or human interactions [9].
v. **Maintaining Access –** If successful, maintaining the gained access covertly [6].
vi. **Covering Tracks –** Erasing traces of the social engineering attack to avoid detection [5].

4. MITIGATION TECHNIQUE

In this paper, there has been a discussion on the social engineering terminology, how social engineering operates which is by manipulating psychological principles or human traits to exploit their victim, the motivation of conducting social engineering attacks such as financial gain, politics, personal interest and revenge and also the type of social engineering attack [16].

Human-based mitigation is a type of detection that involves human intervention in detecting and preventing social engineering. Human-based mitigation is more towards the judgment of human-based to define whether the actions that they come upon are associated with social engineering attacks. Two approaches can be classified in human in human-based mitigation which are the strategy and auditing method and also the training, education, and awareness approach. In these approaches, several works have been studied to moderate social engineering attacks by human supervisory.

Technology-based modification technique is another way that has been investigated in detecting and avoiding social engineering attacks. Several categories can represent this method.

5. CHALLENGE AND FUTURE DIRECTION

Future directions in defense involve advanced awareness training, AI-driven threat detection, and stricter authentication measures to mitigate risks. Constant vigilance and adaptive security strategies are crucial to stay ahead of emerging social engineering threats. Human-based techniques are limited by human subjective decisions. Technology-based systems can be also inadequate as the technical weaknesses may be abused [1].

The evolving landscape of technology poses challenges for combating social engineering attacks. Increasingly sophisticated tactics, such as spear-phishing and pretexting, exploit human psychology.

6. PREVENTION

Social engineering attacks pose challenges and risks to the security of all networks, and it is difficult to confront and overcome them because they depend on exploiting preventing, and protecting against these attacks is extremely important to all computer and mobile phone users [15].

Table 1: Prevention of Social Engineering Attacks

Type	Prevention
Phishing Attack	Educate yourself and develop your technology knowledge permanently to be able to properly deal with such attacks. Don't click on an email or instant message. Always make sure you are using the official website.
Baiting Attack	Beware of clicking on the links that you receive via unknown messages because they often contain harmful programs and files.
Pretexting Attack	Ensure that individuals and employees are constantly trained and educated about the pretexting attacks and how to deal with them. Use the spam filter to filter email messages.
Quid Pro Quo	Make sure to change the password for your account frequently. Never disclose any personal information related to your account.

Tailgating Attack	Always verify the identity of any suspicious person and verify his data to see if he has the right to authorized access in that area or not. Make sure to log computer or other device when you are away from them.
Ransomware Attack	Take care to make backup copies of all data Using two-factor authentication to make your account more secure.
Shoulder Surfing	Not to enter credit card details or account passwords when they are in a public place and use strong passwords so that it is difficult for fraudsters to remember them if they see them.
Dumpster Diving	Shredding or burning printed copies of confidential data or information before disposing of them in trash bins so that an attacker cannot shift through the rubbish and collect confidential information such as username and password.

7. CONCLUSION

In this paper, social engineering attacks humans and manipulates the human mind to gain sensitive information or take specific actions. Social engineering attacks are a thoughtful danger to individuals and societies, and they can occur through various channels such as email, phone, or social media. To defend against these attacks, organizations should educate employees about social engineering risks, implement robust security policies, conduct regular training, and use technology like multi-factor authentication, vigilance, skepticism, and awareness of social engineering threats.

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCE

Salahdine, F.: Kaabouch, N., (2019), "Social Engineering Attacks: A Survey", Future Internet 2019; 11(4),89, https://

Heartfield, R.; Loukas, G. (2015), "A taxonomy of attacks and survey of defense mechanisms for semantic social engineering attacks", ACM Computing Survey; pp 1-39,

Koyun, A.; Janabi AI E., (2017), "Social engineering attacks", Journal of Multidisciplinary Engineering Science and Technology; Volume, 4 issue.

Syafitri, W.; Shukur, Z.; Umi Asma'Mokhtar; Sulaiman, R.; Muhammad Azwan Ibrahim, (2022), "Social engineering attacks prevention: A systematic literature review", IEEE Pages 39325-39343. https://doi.org/10.1109/ACCESS.2022.3162594

Junger, M.; Montoya, L.; Overink, FJ., (2017), "Priming and arming are not effective in preventing social engineering attacks", computers in human behavior; Elsevier

Saleem, J.; Hammoudeh, M., (2018), "Defense method against social engineering attacks" Computer and network security essentials; pp 603-618.

Abeer, F.; AL-Otaibi; ES AIsuwat. (2020), "A study on social engineering attacks: Phishing attacks", International Journal of Recent Advances in Multidisciplinary Research; pp 6374-6380.

Krombholz, K.; Hober, H.; Weippl E., (2015), "Advanced social engineering attacks", Journal of information security and Application; pages 113-122, https://doi.org/10.1016/j.jisa.2014.09.005

Li, T.; Song, C.; Pang, Q., (2023), "Defending against social engineering attack: A security pattern-based analysis framework", IET Information Security; pages 703-726, https://doi.org/10.1049/ise2.12125.

Rita, M.; Obedoza, A.; Rodriguez, G.; Johnston, A.; Salahdine, F.; Kaabouch, N., (2020)," Social engineering attacks a reconnaissance synthesis analysis", IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference.

Beckers, K.; Krautsevich, L.; Yautsiukhin, A., (2014)," Analysis of social engineering threats with attack graphs", International workshop on data Privacy Management, Quantitative Aspects in Security Assurance, Autonomous, and Spontaneous Security; pp 216-232.

Costantio, G., La Marra, A., Martinelli, F, Matteucci, CANDY, I., (2018), "A social engineering attack to leak information from an infotainment system", Proceeding of the IEEE Vehicular Technology Conference; Porto, Portugal, 3, pp. 1-5.

Foozy, CFM.; Ahmad, R.; Abdollah, MF.; Yusof, R., (2011), "Generic taxonomy of social engineering attack and defense mechanism for handheld computer study", icact.org.

Wang, Z.; Zhu, H.; Sun, L., (2021), "Social engineering in cybersecurity: Effect mechanism, human vulnerabilities, and attack method", Springer; IEEE Access, ieeexplore.ieee.org.

Tulkrm, P. (2021), "A Survey of Social Engineering Attacks: Detection and Prevention Tools", Journal of Theoretical and Applied Information Technology.

Zulkumain, AU.; Hamidy, A.; Husain, AB.; Chizari, H. (2015), "Social Engineering Attack Mitigation", International Journal of Mathematics and Computational Science; pp 188-198.

Jain, JK., Waoo, AA., Chauhan, D, (2022), "A Literature Review on Machine Learning for Cyber Security Issues", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 8, Issue 6 Page Number: 374-385, ISSN: 2456-3307 (www.ijsrcseit.com). https://doi.org/10.32628/CSEIT228654

Pramod Singh, Bharat Mishra, P. K. Rai, "Study and Analysis of Different Database Threats and Basic Access Control Models", INTERNATIONAL JOURNAL OF APPLIED RESEARCH AND TECHNOLOGY, IJART- Vol-2, Issue-3, June 2017, ISSN 2519-5115.

Salahdine, F., & Kaabouch, N. (2019)., "Social Engineering Attacks: A Surve", Future Internet, 11(4), 89.

Atwell, C.; Blasi, T.; Hayajneh, T. (2016)," Reverse TCP and social engineering attacks in the era of big data", IEEE International Conference of Intelligent Data and Security, New York, NY, USA, 9–10 April 2016; pp. 1–6.

Li, Y., & Liu, Q. (2021), "A comprehensive review study of cyber-attacks and cyber security", Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126.