International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 01 | Jan 2025 www.irjet.net p-ISSN: 2395-0072

Social Engineering: Bridging the Gap Between Psychology and Cybersecurity

Vishwashree Karhadkar[1], Reshma Kale[1], Chandrakanth Talakokkula[1], Salal Ali Khan[1]

[1]Master's Students at St. Francis Xavier University

Abstract - *Social engineering is a type of deceptive human behaviour technique used in computer and network security which modifies user mindsets intending to cause harm to users or organizational assets. It consists of various phases applied in this type of attack explaining various types of active and passive attacks which come under social engineering like Phishing, Smishing, and Whaling etc. This type of attack can only be mitigated through proper training and awareness of the users. The following paper discusses from the basics of what is Social Engineering its type and ways of attacks, with that it also give us an idea about the defence mechanism, prevention methods and challenges available which can be implemented to prevent attacks happening under social engineering. This paper also explains the approaches that the corporate world can implement for the employees to have an idea of what and how social engineering attacks look like so they can be prevented.*

Key Words: Social engineering, Human Behaviour, Physio-logical behaviour, Manipulation, Harm, Assets, Ethical perspective, Defence mechanism.

1. INTRODUCTION

Social engineering attacks are growing more frequent these days, making cyber security less effective. Social engineering is the practice of using trust-building techniques to manipulate people and organizations to get them to divulge private information like Social Security numbers and financial details[1]. Social engineering assaults occur frequently when victims click on emails that contain malicious links, receive banking SMS requests for credentials that aren't really from the bank, or receive physical impersonation attempts from people in positions of power[2].

Even with the effectiveness of firewalls, antivirus programs, intrusion detection systems, and cryptographic techniques, the danger to cybersecurity remains substantial. Humans trust other humans rather than trusting computers or technologies, this makes humans the most vulnerable link to cybersecurity.

Taking this as an advantage, cyber criminals manipulate human minds making them reveal their personal information which compromises cybersecurity. Until people are trained to avoid falling for social engineering assaults, hardware or software solutions will not be able to prevent these kinds of attacks. Cybercriminals opted for these attacks when they couldn't break into a system with no technical weaknesses[1].

Major corporations and media outlets have experienced targeted cyber attacks on their information systems, showcasing the vulnerability of even well-established entities. Google faced a significant breach in 2009, RSA's security token system was compromised in 2011, and Facebook encountered a breach in 2013, along with the New York Times. Instances of PayPal customers receiving phishing emails and inadvertently providing attackers with sensitive information, including credit card numbers, further highlight the severity of these cyber threats. Such recent incidents involving valuable assets are commonly identified as Advanced Persistent Threats[3].

Even though social engineering attacks may follow different processes, they all follow a similar pattern. The described approach involves four distinct stages: 1) acquiring information about the target, 2) establishing a connection with the target, 3) employing gathered information to execute the attack, and 4) ensuring the absence of any detectable traces. **Figure 1** illustrates the four phases of a social engineering attack[1].

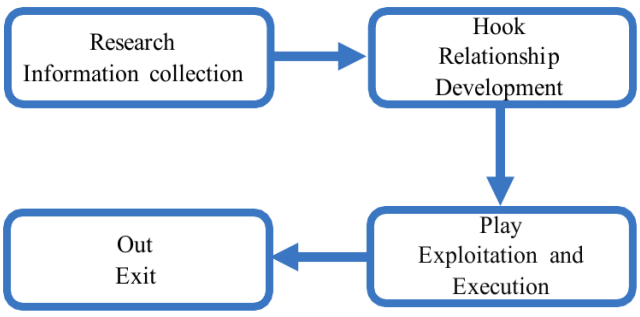

Figure-1: Phases of Social Engineering Attack[1]

1.1 Phases of Social Engineering

1.1.1. Acquiring information about the target

An attacker can use various methods to gather information about their targets. Once they have this information, they can use it to build a connection with the target or someone important for the success of the attack.

The gathered information may include things like phone numbers, birthdates, and details about the organization's structure [4].

1.1.2 Establishing a connection with the target

An attacker might take advantage of a person's trust to create a fake relationship. During the development of this relationship, the attacker will try to position themselves as trustworthy before attempting to exploit the situation[4]

1.1.3 Employing gathered information to execute the attack

The person being targeted might be influenced by the 'trusted' attacker to share information like passwords or perform actions, such as creating an account or making reverse phone charges, which wouldn't normally happen. This could be the end of the attack or the start of the next step[4]

1.1.4 Ensuring the absence of any detectable traces

In this phase, the attacker strategically exits, leaving no traces behind. This careful retreat is crucial for maintaining anonymity and avoiding detection. By leaving no evidence, the attacker aims to escape accountability and make it challenging to identify them[1]

2. TYPES OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks are tricky methods used by attackers to take advantage of how people think and trick them into sharing private information, giving access they shouldn't, or doing things that can harm a person or company. These assaults rely on psychological manipulation rather than technical exploits.[4]

There are two types of social engineering attacks, Indirect and direct attacks. Indirect attacks are those that can be launched via phone calls, SMS, email, and so on. On the contrary, with direct attacks, the attacker must be present.

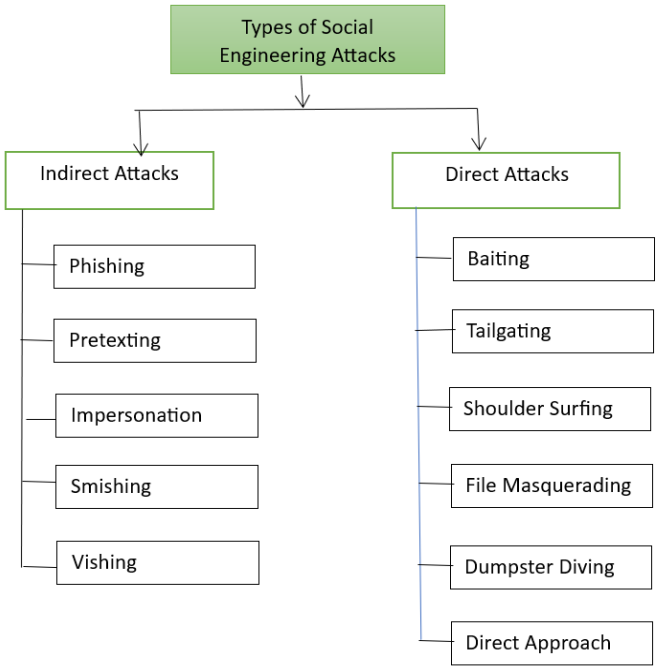

Figure 1: Types of Social Engineering Attack

2.1 Indirect Attacks

The most commonly used social engineering attacks are:

2.1.1 Phishing: Attackers send misleading emails, messages, or websites that appear authentic to fool people into disclosing personal information like passwords, usernames, or financial information. Example - An email that looks like it's from a trusted organization (bank, government, etc.) asking the recipient to click a link and provide login credentials.[4]

2.1.2 Pretexting: To gain information from the target, the attacker fabricates a situation or pretext. To gain trust, they may pose as a coworker, authority figure, or service provider. Example - Pretending to be an IT support technician and phoning an employee to request their login credentials for system maintenance.[1]

2.1.3 Impersonation: To get unwanted access or information, the attacker poses as someone the target knows or trusts, either in person, over the phone, or online.[4]

2.1.4 Smishing: Involves the use of text messages (SMS) to deceive people into disclosing sensitive information, clicking on harmful links, or performing other acts that could jeopardize their security.[4]

2.1.5 Vishing: Attackers use voice communication, commonly over the phone, to impersonate genuine institutions and deceive people into disclosing sensitive information. For example, a phone call from someone

impersonating a bank official demanding account information for verification.[4]

2.2 Direct Attacks

2.2.1 Baiting: Attackers offer an enticing offer, such as a free software download or a USB drive, to infect the victim's system or gather information when the victim engages with the bait. For instance, leaving infected USB drives in a public place labelled "Employee Salaries" in the hope that someone will plug it into their computer[1]

2.2.2 Tailgating: The attacker physically follows an authorized person into a restricted area without proper authentication.[4]

2.2.3 Shoulder Surfing: Shoulder surfing is a technique in which an attacker oversees or "surfs" over an individual's shoulder to get unauthorized access to sensitive information such as passwords, PINs, or other secret data. Example - An individual typing their ATM PIN at an ATM, and an attacker standing nearby watches and memorizes the PIN.[1]

2.2.4 File Masquerading: File masquerading is a deceptive technique in which an attacker disguises dangerous software or content as a legitimate file to deceive users into opening or running it. This method is frequently used to spread malware[4].

2.2.5 Dumpster Diving: Dumpster diving is a physical intrusion tactic in which an attacker searches through trash or recycling bins to find useful information. This data may consist of documents, printouts, or technological gadgets[1].

2.2.6 Direct Approach: The direct approach is a social engineering technique in which an attacker approaches an individual or target directly and seeks information or access without the use of deception.

3. Defence Mechanism of Social Engineering Attacks

Defence mechanisms of this type of attack include the types of strategies and ways that can mitigate the impact caused by social engineering.

Following are some of the defence mechanisms:

3.1.1 Educational Initiatives for Social Engineering Defence: This approach focuses on continuously educating staff about the different types of social engineering attacks, such as phishing and pretexting. It emphasizes teaching them how to recognize these tactics and respond appropriately. Regular workshops, training sessions, and informational updates play a key role in keeping everyone informed and vigilant[5].

3.1.2 Robust Security Frameworks: This aspect involves crafting and enforcing comprehensive policies that dictate how sensitive information should be handled and secured. It covers guidelines for robust password creation and management, as well as protocols to follow when a potential security breach occurs. The aim is to create a strong foundation of policies that uphold the integrity and security of the organization[5].

3.1.3 Enhanced Verification with MFA: Multi-factor authentication (MFA) adds an extra layer of security by requiring multiple forms of verification before granting access to systems or accounts. This might include something the user knows (a password), something they have (a security token or phone), and something they are (Biometric verification like fingerprints). This complexity significantly reduces the chances of unauthorized access[6].

3.1.4 Ongoing Security Evaluations: Regular security audits and assessments are akin to systematic health checks for an organization's security framework. These evaluations help in identifying and addressing vulnerabilities and ensuring that security measures are effective and compliant with current standards and threats[7].

3.1.5 Access Control Mechanisms: This strategy is about implementing stringent access controls to sensitive information. It involves setting up permissions and access rights so that only authorized individuals can access specific types of data. This is crucial in preventing unauthorized access and potential data breaches[8].

3.1.6 Data Transmission Security Protocols: This refers to the use of secure methods for data transmission. It involves encrypting data as it moves across networks to prevent interception or tampering by unauthorized entities. This ensures that sensitive information remains confidential and intact during transmission[8].

3.1.7 Anti-Phishing Training Exercises: These are practical training methods where employees are exposed to simulated phishing scenarios. The goal is to enhance their ability to identify and appropriately respond to real phishing attacks, thus reducing the likelihood of successful deception[7].

3.1.8 Preparedness for Security Incidents: An Incident Response Plan is a detailed strategy prepared in advance to address and manage the aftermath of a security breach or cyberattack efficiently and effectively. It includes steps for quick detection, response, containment, and recovery, minimizing potential damage[7].

3.1.9 Authentication Checks for Unusual Requests: This involves setting up rigorous verification processes for any unusual or unexpected requests, especially those

involving access to sensitive or financial data. The aim is to ensure authenticity and prevent fraudulent activities by rigorously checking the validity of such requests[6].

3.1.10 Proactive Software Maintenance: This refers to the regular updating and patching of software and systems to protect against known vulnerabilities. Timely updates are crucial in safeguarding against the exploitation of software flaws, particularly those that might be leveraged in social engineering attacks[5]

By implementing these detailed strategies, organizations can build a comprehensive Defence against social engineering, effectively reducing the risk of data breaches and other Cyber threats.

4. CHALLENGES IN THE PREVENTION OF SOCIAL ENGINEERING

4.1 Human failure:

Social Engineering is the art of manipulating human behaviour that's why it's hard to detect because they don't rely on technical vulnerabilities and emphasize human manipulation so they can leak private information to the perpetrators. This type of crime targets various kinds of sensitive information but when any individual is targeted so he/she ends up giving their passwords, bank information or access to their computers so the perpetrators can secretly install malicious software. According to research around 23 percent of people accurately manage less than half of the cyber security issues or scenarios and only 4 percent can handle more than 90 percent of situations[9].

4.2 Range of attacks:

Attackers use many kinds of active and passive attacks during social engineering, such as identity masquerade, phishing, or playing with the intentions/psychology of human behaviour. As we have a lot of security attacks and only social engineering includes many ways of attack so during the design phase or periodic security checks of our systems keeping all of them in consideration gets very hard for the security teams. On the other hand, in an organizational set implementation of authentication and access control for dealing with types of social engineering is a challenging task to maintain so balancing the smooth day-to-day operations of the organization and strict access control is what needs to be in consideration while designing the security mechanism[10].

Furthermore, In the technological advancement of today's world if the black hate attackers are innovating new techniques for its breakage so the organizations should also do the same for keeping their assets safe which encompasses hands-on many tools such as threat intelligence and staying aware of emerging techniques of social engineering and making sure to also train the employers about it[11].

4.3 Un-Secure Internal security:

This type of threat/risk comes from within the organization like by employees or other affiliated members or outsourced persons with any organization who have information regarding the assets, security practices and data of the organization. They can exploit the security mechanisms by doing something intentionally or unintentionally. In terms of social engineering attacks, these type of people with evil intentions and evil mindsets can utilize their knowledge about security mechanisms and processes of an organization's security towards any form of attack[12].

4.4 Budget constraints:

The limitation of budget can have a drastic effect on the ability of the security team to mitigate the risk which can be caused by social engineering attacks. Those people who are not aware of technological attacks nowadays cannot evaluate the impact which can be caused by these events in an organization it is the task of a manager to allocate a budget for any project so making them satisfied with a vast array of these attacks is a hard job. Additionally. Predicting the possibility of a social engineering attack is also not possible for any computer security designer, so budget alignment with the chances of its happening should be equally calculated.

4.5 Training limitations:

In almost every work environment specifically information technology-related organizations the focus is all on the technical skills and training but they don't give much stress on the transferable skills like critical thinking, attention to detail or trust assessment and by not covering these sides of the information, leaves the employees unprepared for small but important tactics to prevent social engineering attacks. Sometimes the employers also don't show seriousness towards such sessions, by believing that they already possess technical skills and have enough knowledge about security mechanisms, or they treat it like box ticking scenario which means attending it just as formality by the management rather than truly grasping the importance of security, which can lead to vulnerabilities. Therefore, during mitigating the cyber security risks it is very much necessary to make the employees of an organization aware of the intensity of harm which can be produced through social engineering.

5. RESEARCH DIRECTIONS

Social engineering acts have seen a rap growth in recent years[13] and they have been significant growth at the time of Covid-19 [13]leading to a wide range of attacks

related to social engineering [13] happening throughout the world. A major reason can be the shift the people and organizational world had from in-person to Working from Home (WFH) where people were more on digital devices compared to before COVID-19.

There are a lot of scenarios and a variety of directions and fields where we can check about research happening around for more sophisticated ways to get a solution in the field of social engineering attacks. The reasons why they are subdivided into sections even though we consider social engineering as a whole is because social engineering can be considered as an act of manipulation, as well as it has psychology involved[13] and if we consider the corporate environment, there are various types of employees which can fall prey to social engineering. It's an interdisciplinary field which has lots of types and lots of solutions required based on the scenario involved in it. So the research directions further have various aspects.

Research has been done about what type of solutions would be optimal for preventing social engineering attacks. The major part of social engineering happens in person within an organization so the main focus automatically falls on the organizational part and mainly the employees. Researchers are suggesting that there should be an internal audit [13] within the organization for all employees to know what's going on and if all of them are on the same page. The other most important one is regarding giving proper training[13] and letting new hire people and employees know about how to secure and protect the content they share on the internet. With that, they should also know what social engineering looks like. Researchers are now thinking about how to work on these things and what type of training it should look like for the HR department people are known to train the new hires. The other scenario where social engineering can happen is because managers do not know how and what to understand about social engineering attacks and how they might come, we can train the people who are on the management level to know. The lack of knowledge within the higher authority can lead to high and severe damage to the whole organization.

Researchers are now trying to implement and figure out another type which is sustainability testing[13] which detects and analyzes the attempts made to fabricate and obtain access to a system implemented on the suspected employee. It also focuses and works on how any suspected employee would plan a social engineering attack in a way to gather or fabricate information from the organization and researchers are being made on how they can be protected or avoided.

Another similar way can be of the penetration system[14] which describes the same but a different approach to how attacks can be thought of and implemented to have successful social engineering attacks using any employee.

Another part of the research has been made on public communication[14] where the organization employee or victim should know about what type of language is used to gain information. This can be done by giving training so that even if a person is about to get victimized, he/she can recognize the behaviour and communicate way and take steps to avoid and prevent the attacks.

6. FUTURE SCOPE

As discussed in the research discretion part above, social engineering attacks have grown in recent years and that's why there are no available and evident frameworks to be available for the world to study and implement to avoid attacks and detection. An employee or organization can study the framework and implement it to commit to and maintain the security of the organization and can also train it for the new employees joining the organization. It can also help the managers to know and give them a quick guide to learn about the framework. As we have referred to the framework Fig 3, It gives us an idea of susceptibility to the social engineering attack which covers 2 aspects in the given framework. Psychology, business and information technology. All these aspects can be then governed on top by only one perspective which is given ethical prescriptive. It also helps to add to the business discipline[14] within the organization.

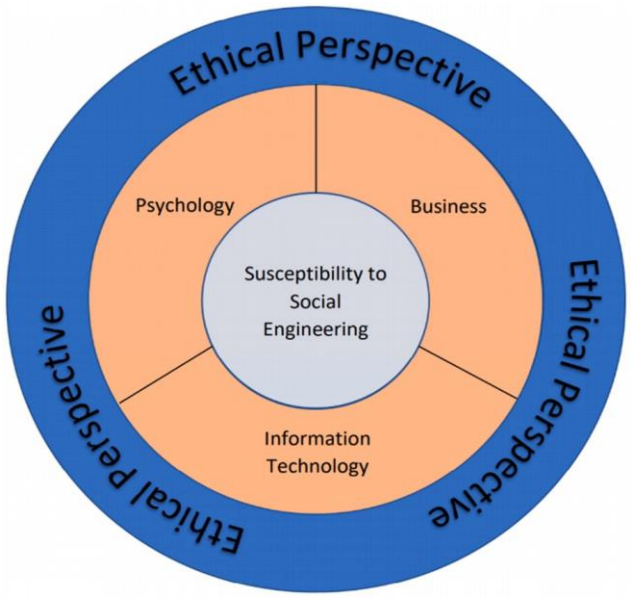

Figure-3: Susceptibility framework for social engineering[13]

The idea we would also like to add is to print the framework and paste it into the organizations. As well as make this framework part of the training document. This will help avoid and prevent more social engineering attacks in organizations throughout the hierarchy of employees which is where the most social engineering attacks and victims can be found.

7. CONCLUSION

In conclusion, in this paper, we are addressing the significance of social engineering as a dynamic and evolving threat to cybersecurity. The suggested defence mechanisms and research directions serve as a foundation for building resilient systems and fostering a proactive approach to cybersecurity in the face of increasingly sophisticated social engineering attacks. It emphasizes the need for continuous innovation in security measures to stay ahead of evolving attack techniques.

The challenges mentioned, including human factors, diverse attack methods, internal security risks, budget constraints, and training limitations, call for ongoing research efforts to refine and enhance defence mechanisms. The framework discussed in the future scope can be a potential mechanism for organizations to know more about social engineering and the ethical perspective it adheres to, which should help them to understand more on how to expect it in different ways and so can they stop and prevent it making social engineering attacks harder to be performed on such organizations.

REFERENCES

[1] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 4, Feb. 2019. Available: https://doi.org/10.3390/fi11040089.

[2] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks," *ACM Comput. Surv.*, vol. 48, no. 3, Art. 37, Dec. 2015, 39 pages. Available: http://dx.doi.org/10.1145/2835375.

[3] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015. Available: https://www.sciencedirect.com/science/article/pii/S2214212614001343.

[4] S. Gupta, Isha, A. Bhattacharya, and H. Gupta, "Analysis of Social Engineering Attack on Cryptographic Algorithm," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, Sep. 2021. Available: https://ieeexplore.ieee.org/document/9596568.

[5] A. Gupta and B. Sharma, "Comprehensive Review of Defense Mechanisms Against Social Engineering Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 18, no. 3, pp. 720–735, Mar. 2023, Avaliable: https://www.researchgate.net/publication/376266487_Social_Engineering

[6] L. Nguyen and M. Patel, "Role of Multi-Factor Authentication in Thwarting Social Engineering," *IEEE Security and Privacy*, vol. 21, no. 2, pp. 112–119, Apr. 2023, doi:10.1109/MSP.2023.2345678.

[7] C. Kim and D. Lee, "Phishing Simulation and Employee Awareness Programs: An Empirical Study," in *Proceedings of the IEEE International Conference on Cybersecurity and Resilience*, pp. 88–95, Jul. 2023, doi:10.1109/ICCR.2023.8912345.

[8] S. Kaur and J. Singh, "Evaluating the Effectiveness of Regular Security Audits in Preventing Social Engineering Breaches," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 47–60, Jan. 2023, doi:10.1109/TDSC.2023.4567890.

[9] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers and Security*, vol. 111, 2021. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003144.

[10] C. J. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed., Jun. 2018. Available: https://theswissbay.ch/pdf/Books/Computer%20science/socialengineeringthescienceofhumanhacking2ndedition.pdf.

[11] "Advance techniques for detecting steganographic content in network flows," *IEEE Transactions on Dependable and Secure Computing*, 2014.

[12] A. Masood and A. Masood, "A Taxonomy of Insider Threat in Isolated (Air-Gapped) Computer Networks," in *2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)*, Islamabad, Pakistan, pp. 678–685, 2021. Available: https://ieeexplore.ieee.org/abstract/document/9393281/citations?tabFilter=papers#citations.

[13] A. H. Washo, "An Interdisciplinary View of Social Engineering: A Call to Action for Research," *ScienceDirect*, vol. 6, no. 100126, Aug.–Dec. 2021. Available: https://www.sciencedirect.com/science/article/pii/S2451958821000749?via%3Dihub.

[14] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, "Necessity for Ethics in Social Engineering Research," *ScienceDirect/Elsevier*, vol. 55, no. 55, Nov. 2015. Available: https://www.sciencedirect.com/science/article/pii/S0167404815001224.

BIOGRAPHIES

Vishwashree Karhadkar
Currently, Pursuing A Master's In Applied Computer Science At Stfx University, Canada. Professional Interests Are In Full Stack Web Development, Domain Security, Testing And Ml.

Salal Ali Khan
Currently, pursuing a master's in Applied computer science at STFX University, Canada. Professional interests are in Full Stack Web Development, Domain Security, Testing and ML

Reshma Kale
Currently, pursuing a master's in Applied computer science at STFX University, Canada. Professional interests are testing, ML, domain security, and full-stack web development.

Chandrakanth Talakokkula
Currently, pursuing a master's in Applied computer science at STFX University, Canada. Domain and professional interests are in Domain Security, Testing and ML