International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.018 ISSN: 2581-4621

CYBER ATTACKS AND HUMAN PSYCHOLOGY: THE ROLE OF SOCIAL ENGINEERING

N. Hiranmai
Assistant Professor1, Mechanical Engineering Department, G. Narayanamma Institute of Technology and Science
Email ID: hiranmai@gnits.ac.in

Abstract
While software vulnerabilities are falling and cyber security is coming of age as the technology advances, individuals are more vulnerable than ever. Today, social as opposed to technological penetration attempts rank among the most well-liked and effective; indeed, they are so effective that they are a central component in the majority of cyberattacks. The art of exploiting human frailties to gain a nefarious goal goes by the name of social engineering. Information security experts violate security controls to access confidential information, especially by taking advantage of individuals' trust nature. To initiate a more focused attack, cybercriminals compel their victims to compromise security procedures at the cost of personal information. Most of the time, victims are tricked into unknowingly infecting and demolishing the system. Beyond revealing a simple supplementary technological method to carry out effective exploits, this research is exploring typical social engineering methods exploited by attackers. Cybercrime attackers are inventing cyberattacks to become increasingly difficult to recognize due to continuously strong and complicated cybersecurity measures [1].
The application of social engineering of criminals as a method to attack the human factor in an enterprise's security system has been the focus of recent research. To bypass technical safety measures for malicious purposes, psychological attacks exploit particular human traits and psychology. As it is comparatively simpler to breach an individual than to find a security system vulnerability, social engineering is emerging as a common method used to breach individuals and organizations. Because cyberattacks based on social engineering do not have patterns or methods of executing an attack, they are very hard to prevent, making them very effective, efficient, easy, and stealthy means to breach any firm [2]. A better understanding of the attack strategy is essential in order to thwart such attacks. Therefore, the methods that are used in order to conduct social engineering-driven cyberattacks are analyzed in-depth in this study.
Keywords: Cyber-security, cyberattack, psychology, social engineering.

I. Introduction
Human psychology is exploited by social engineering cyberattacks to trick people into revealing sensitive information or taking actions that weaken security. Social engineering attacks are especially malicious because they attack human mental vulnerabilities, not technical vulnerabilities, and hence pose a serious threatinthe world of cybersecurity[3].

II. Literature Review
There have been various studies examining the psychological foundations of social engineering attacks. Cialdini (2001) named fundamental persuasion strategies including reciprocity, authority, and social proof that are manipulated by attackers to trick victims[4]. Mitnick and Simon (2002) showed the importance of deception and exploitation of trust in cyberattacks. Later research by Hadnagy (2018) illustrates the utilization of emotional manipulation, specifically fear and a sense of urgency, in phishing and other frauds.

DOI:10.46647/ijetms.2025.v09si01.018 ISSN: 2581-4621

Cognitive bias studies have also extended these findings. Tversky and Kahneman (1974) established the groundwork of heuristics in decision-making and why individuals are prone to fallacious methods. Sheng et al. (2010) research into phishing susceptibility proved that less security-conscious users are vulnerable to deception as a result of confirmation bias and habitual online behavior.

Besides, empirical evidence of social engineering defense emphasizes the importance of security awareness training and user education. Althobaiti and Abdullah (2021) argue that continuous training programs are effective in reducing the risk of social engineering attacks. In addition, advances in artificial intelligence, as discussed by Gupta et al. (2022), provide solution prospects for phishing detection through automation and behavioral anomaly detection.

Even with such advancements, successful counter-measures against social engineering attacks are still a challenge. It is indicated by studies that attackers continue to adapt their approach in a bid to leverage new communication technology and emerging trends. There should therefore be ongoing research in a bid to develop defense methods and stronger security policies[5].

III. Psychological Mechanisms of Social Engineering Attacks

Social engineering attacks exploit many of the psychological approaches and human weaknesses. The main mechanisms are persuasion, social influence, trust and deception, and emotional manipulation. They use cognitive biases, personality and habits, and exploit them to gain their goals. Success is usually based on attackers manipulating victims' emotions and decision-making.

Persuasion Techniques

Attackers employ persuasion techniques to get victims to perform actions that undermine security. Some common techniques are reciprocity, commitment and consistency, authority, social proof, liking, and scarcity. These psychological triggers drive decision-making and make people act contrary to their better judgment.

Social Influence and Trust Manipulation

Humans are prone to trusting others, and therefore, they are vulnerable to social engineering attacks. Attackers usually pretend to be authority figures, colleagues, or trusted organizations in order to be credible. Trust-based attacks like pretexting and impersonation take advantage of this nature to trick victims into divulging sensitive information.

Deception and Emotional Manipulation

Emotional manipulation is central to social engineering. Attackers use fear, urgency, greed, curiosity, and empathy to make victims respond impulsively to situations. Phishing emails, for instance, use a sense of urgency to compel victims to click on malicious links or provide confidential information [6].

IV. Cognitive Biases Used in Social Engineering

Authority Bias

Individuals have a tendency to obey requests made by authority figures without questioning. Attackers take advantage of this by posing as executives, IT staff, or police officers in order to bully victims into cooperation.

Confirmation Bias

Victims will be more likely to believe information that is consistent with what they already know. Attackers use this by writing messages that fit anticipated storylines, so the scam will sound more authentic.

Routine Behaviors and Predictability

Human routines and habits render them predictable targets. Attacker analysis of these routines informs the design of attacks that are routine and reliable. Repeated phishing emails, for example, become effective once they mimic regular correspondence[7].

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.018 ISSN: 2581-4621

Popular Social Engineering Attack Types

One of the most common social engineering attacks is phishing. Phishing is the act of sending spoof messages, email addresses, or websites to deceive consumers into revealing confidential information, like credit card numbers, usernames, or passwords.

Pretexting is the process of creating a false pretext to gather information from a victim. To gain authenticity and get sensitive information, attackers pretend to be officials, vendors, or colleagues.

The Quid Pro Quo and Baiting Quid pro quo attacks offer a service or advantage in return for information, while baiting employs free goods, like malicious downloads or infected USB drives, to entice victims [8].

Impersonation and Tailgating If a predator purposefully comes into a banned region by sitting with an accredited person, that is called tailgating.

V. Mitigation Strategies and Defense Mechanisms

Security Awareness TrainingIt is important to educate employees and people on social engineering techniques. Phishing attempts, suspicious requests, and identity verification should be emphasized during training.

Multi-Factor Authentication (MFA)MFA makes it more difficult for attackers to take advantage of stolen credentials.

Verification and Reporting ProtocolsOrganizations must have strict verification processes in place and urge the reporting of suspicious activity to deter successful social engineering attacks.

Technical SafeguardsEmail filters, endpoint security software, and network monitoring tools can detect and prevent social engineering attempts prior to reaching the victim.

Human Vulnerabilities

Success of social engineering attacks hinges heavily on human weaknesses. These include certain behaviors, personality types, emotional responses, and areas of knowledge and cognitive gaps. Due to the fact that it is easier for the attacker to exploit one's psychology than to bypass technical obstacles, the human factor is at times described as the weakest link in cybersecurity [9].

Challenges in Defense

Even with increased cybersecurity, it is still difficult to defend against social engineering attacks. Existing defense mechanisms have not maximally exploited the psychological elements used by the attackers, resulting in minimal success in blocking the attacks. The absence of defined patterns in social engineering methods also makes it hard to develop efficient counter measures.

Prevention and Mitigation Strategies

It is critical to have in-depth knowledge about attack techniques and human vulnerabilities to counter social engineering attacks. The measures entail building machine learning-based detection approaches, strengthening security awareness training, and promoting collective cybersecurity responsibility. Furthermore, leveraging psychological insight in cybersecurity protocols can assist in establishing more potent protections [10].

VI. Conclusion

Social engineering attacks are particularly dangerous because they target individuals' psychological vulnerabilities. To develop effective countermeasures, one must understand the techniques and vulnerabilities behind such attacks. In the future, research should attempt to bridge the gap between cybersecurity practice and psychological[15] knowledge to make individuals and organizations more resistant to such attacks[11].

Social engineering attacks are especially destructive since they use psychological manipulation as opposed to technical exploits. Both individuals and groups can implement better defense systems by learning about how cognitive biases, emotional manipulation, trust exploitation, and persuasion mechanisms[12] work. To minimize the threats resulting from social engineering attacks, an amalgamation of technical solutions, legislative enforcement, and education is needed [14].

DOI:10.46647/ijetms.2025.v09si01.018 ISSN: 2581-4621

VII. Reference

[1] Murtaza Ahmed Siddiqi, Wooguil Pak and MoquddamA.Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures", Appl. Sci. 2022, 12, 6042
[2] Wenke Lee, Bo Rotoloni, "Emerging cyber threats, trends and technologies", Technical report, Institute for Information Security and Privacy, 2016.
[3] "Internet organized crime threat assessment", Technical report, Europol, 2016.
[4] James Comey, "Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security", FBI, July 2016.
[5] "Internet security threat report", Technical report, vol. 21, Symantec, April 2016.
[6] Nahal Sarbjit, Ma Beijia, Tran Felix, "Global cybersecurity primer", Technical report, Bank of America Merrill Lynch, 2015.
[7] Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.
[8] Ketha, S.; Srinivasan, S.; Ravi, V.; Soman, K.P. Deep Learning Approach for Intelligent Named Entity Recognition of Cyber Security. In Proceedings of the the 5th International Symposium on Signal Processing and Intelligent Recognition Systems (SIRS'19), Trivandrum, India, 18–21 December 2019.
[9] Huang,Y.; Huang, L.; Zhu, Q. Reinforcement learning for feedback-enabled cyber resilience. Annu. Rev. Control 2022, 23, 273–295. [CrossRef]
[10] Bland, J.A.; Petty, M.D.; Whitaker, T.S.; Maxwell, K.P.; Cantrell, W.A. Machine learning cyberattack and defense strategies. Comput. Secur. 2020, 92, 101738. [CrossRef]
[11] Rawindaran, N.; Jayal, A.; Prakash, E.; Hewage, C. Cost benefits of using machine learning features in NIDS for cyber security in UKsmall mediumenterprises (SME). Future Internet 2021, 13, 186. [CrossRef]
[12] Sallouma, S.; Gaber, T.; Vadera, S.; Shaalan, K. Phishing email detection using natural language processing techniques: A literature survey. Procedia Comput. Sci. 2021, 189, 19–28. [CrossRef]
[13] Fang, Y.; Zhang, C.; Huang, C.; Liu, L.; Yang, Y. Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism. IEEE Access 2019, 7, 56329–56340. [CrossRef]
[14] Gutierrez, C.N.; Kim, T.; Corte, R.D.; Avery, J.; Goldwasser, D.; Cinque, M.; Bagchi, S. Learning from the ones that got away: Detecting new forms of phishing attacks. IEEE Trans. Dependable Secure Comput. 2018, 15, 988–1001. [CrossRef]
[15] Repke, T.; Krestel, R. Bringing back structure to free text email conversations with recurrent neural networks. In Proceedings of the European Conference on Information Retrieval (ECIR), Grenoble, France, 25–29 March 2018.