Journal of Research and Innovation in Technology, Commerce and Management
Vol. 2 Issue 8, August 2025, pp. 2850-2852
ISSN: 3049-3129(Online)

Social Engineering and the Psychology of Cybercrime: A Review

Pragati Shukla
Student: School of Computer Applications, Lovely Professional University, Jalandhar,Punjab

Cite as: Pragati Shukla. (2025). Social Engineering and the Psychology of Cybercrime: A Review. Journal of Research and Innovation in Technology, Commerce and Management, Vol. 2(Issue 8), 2850–2852. https://doi.org/10.5281/zenodo.17043364

DOI: https://doi.org/10.5281/zenodo.17043364

Abstract

In today's digital era, cybercrime has evolved beyond technical hacking into a psychological battlefield. Social engineering involves manipulating human emotions such as trust, fear, urgency, and curiosity to trick individuals into revealing sensitive information or performing unsafe actions. This paper reviews six research studies that explore the nature, methods, and impacts of social engineering in cybercrime. It presents a critical discussion on the psychology behind these attacks, the role of artificial intelligence, and the strategies that can be adopted to counteract them. The findings emphasize the urgent need for public awareness, psychological training, legal reform, and technological innovation to safeguard against such manipulative threats.

Keywords

Social Engineering, Cybercrime, Phishing, Human Psychology, Online Scams, Cybersecurity, Artificial Intelligence

Introduction

Social engineering is a form of cybercrime where the attacker deceives people instead of attacking software or systems. These attackers use psychological manipulation — such as creating urgency, building trust, or imitating authority — to make victims give away sensitive information like passwords, bank details, or personal data.

Unlike traditional cyberattacks that rely on code, social engineering exploits the human mind, making it a deeply personal and dangerous threat. This review explores how social engineering works, analyzes its psychological dimensions, and examines findings from six recent and relevant research papers.

Literature Review:

Paper 1: "Social Engineering and Cyber Security" (2017)

This paper focuses on the emotional triggers attackers use to deceive people — such as urgency or fear. It discusses methods like phishing, baiting, and pretexting. The study highlights the

limitations of purely technical defenses and stresses the importance of educating users about social engineering tactics.

Paper 2: "The Concept of Social Engineering and Cybercrime in the Digital Age" (2023)

This recent thesis categorizes different social engineering attacks and uses real-life examples to show how emotions like curiosity and respect for authority are exploited. It argues that improving digital literacy and awareness can significantly reduce the chances of people falling victim to these scams.

Paper 3: "Social Engineering and Crime Prevention in Cyberspace" (2009)

An earlier but still relevant work, this study divides social engineering into two types — semantic (language-based) and syntactic (system-based). It underlines the role of government policies and public education in preventing such crimes.

Paper 4: "The Impact of Social Engineering on Cybercrime: Psychological Aspects, Attack Techniques, and Mitigation Strategies" (2023)

This research explores how attackers exploit emotions like greed or anxiety to disrupt rational decision-making. It also evaluates the effectiveness of cybersecurity awareness campaigns and user training programs in building resistance against manipulation

Paper 5: "Social Engineering and Its Role in the Rise of Cybercrime"

This paper provides a broad view of how social engineering has contributed to the overall rise in cybercrime. It identifies phishing as the most common method and shows how attackers adapt their strategies over time to stay ahead of detection technologies.

Paper 6: "Artificial Intelligence's Impact on Social Engineering Attacks" (2022)

This paper introduces the concept of AI-enhanced social engineering. It describes how AI can be used to create hyper-realistic fake voices, emails, and videos — making it even harder to detect scams. The paper warns that without combining human vigilance with smart technology, these new threats will be harder to manage.

Discussion:

Across all six studies, a consistent message emerges: social engineering is successful not because of technical loopholes, but because of human psychological vulnerabilities. Emotions like fear, urgency, curiosity, and trust are powerful tools used by attackers. Phishing remains the most commonly used method, but newer, AI-driven techniques such as deepfakes and voice cloning are on the rise.

The papers agree that simply improving technical security will not solve the problem. People need to be trained not only in what to look out for but also in how to manage emotional responses when faced with suspicious messages. There is also a clear call for better digital laws and legal frameworks that can adapt to these emerging threats. Some papers

recommend the integration of behavioral psychology into digital education, and others highlight the need for collaborative solutions between governments, educators, and cybersecurity experts.

Conclusion

Social engineering is a growing challenge in the world of cybercrime because it targets the human mind — the most unpredictable part of any security system. The reviewed studies show that education, awareness, and behavior-focused training can help build resilience. Legal systems need to adapt quickly, and new technology — especially AI — must be used responsibly to detect and respond to evolving social engineering threats. In conclusion, a balanced approach that combines psychological understanding, user education, and legal action is key to combating the rise of social engineering in cybercrime.

References:

1. Breda, F., Barbosa, H., Morais, T. (2017). Social Engineering and Cyber Security. ResearchGate.
2. The Concept of Social Engineering and Cybercrime in the Digital Age. (2023). Opus.Govst.edu.
3. Chantler, A., Broadhurst, R. (2009). Social Engineering and Crime Prevention in Cyberspace. ResearchGate.
4. The Impact of Social Engineering on Cybercrime: Psychological Aspects, Attack Techniques, and Mitigation Strategies. (2023). Irshad Journals.
5. Social Engineering and Its Role in the Rise of Cybercrime. Core.ac.uk.
6. Artificial Intelligence's Impact on Social Engineering Attacks. (2022). Opus.Govst.edu.