Article Review: "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures"

Juan David Restrepo Gomez

School of Cybersecurity, Old Dominion University

Matthew Umphlet

21 Jul 2024

1. How the Topic Relates to the Principles of the Social Sciences

This article help us understand how human psychology and behavior is affected by social engineering attacks. Social interactions, human emotions, are example of the connection of social science themes with cybersecurity as we can take measurements by studying the psychological outcomes from these interactions to improved cybersecurity in that matter.

2. The Study's Research Questions or Hypotheses

The primary research questions addressed in the article are: What psychological tactics are most commonly used in social engineering attacks, How do these tactics exploit human vulnerabilities to bypass technical security measures, What existing countermeasures can be effective against social engineering-based cyberattacks? And the hypotheses may include, Social engineering attacks are more successful when they exploit specific human psychological trait, and Current countermeasures are insufficient due to the unpredictable and personalized nature of social engineering attacks.

3. The Types of Research Methods Used

The types of research are comprehensive literature review and real-world case studies. The studies analyze multiple methods of attacks, like phishing and smishing, and assesses the efficacy of different countermeasures, including those based on machine learning. By analyzing empirical data from recent cybersecurity breaches, the research provides a detailed understanding of how psychological manipulation is employed in these attacks.

4.The Types of Data and Analysis Done

The types of data are quantitative and qualitative. Quantitative data provides us statistics of success rates of different types of social engineering attacks. Qualitative data provides us detailing cases of significant breaches, showing us the psychological principles exploited. The analysis compares different effective methods of cybersecurity to put it in practice.

5.How Concepts Discussed in Class Relate to the Article

A lot of concepts discussed in the class related to this article. For example, security awareness training that is very important for educating individuals about social engineering tactics is emphasized, reflecting the preventive measures discussed in class. Moreover, human error impacts on social engineering attacks by always highlight that is not the machines but always somebody behind it. And how training again is mentioned to improvise our flaws in cybersecurity.

6. How the Topic Relates to the Challenges, Concerns, and Contributions of Marginalized Groups

Although the article does not explicitly focus on marginalized groups, the implications of social engineering attacks can disproportionately affect these populations. For example, individuals from marginalized communities may have less access to cybersecurity literacy making them more vulnerable for social engineering attacks. Moreover, attackers can take advantage of these communities as they have less resources to put in place counter counter-measurements.

7. The Overall Contributions of the Studies to Society

The study makes great contributions in order to make a digital environment more secure by analyzing the psychological mechanisms behind these attacks, the research informs the development of more effective security training programs and policies. The insights gained can help improve public awareness of social engineering tactics, enhance the resilience of individuals and organizations against such attacks.

References

Siddiqi, M.A., Pak, W., & Siddiqi, M.A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences, 12*(12), 6042.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). A practical assessment of social engineering vulnerabilities. *Information Management & Computer Security, 17*(1), 22-34.