Article Review #1: The Social Psychology of Reporting Phishing

Asher L. Embry

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

October 2, 2025

Article Review #1: The Social Psychology of Reporting Phishing

Introduction: Cybersecurity and Social Science

The chosen article for this review is “Information security culture and phishing-reporting model: structural equivalence across Germany, UK, and USA,” published in the *Journal of Cybersecurity*. This study explores the psychological factors that influence employees to report phishing emails, linking cybersecurity and social sciences. The concept of phishing is based on manipulating a user’s trust, emotions, and behavior using different psychological methods (Daudi, 2024). This article expands this connection by seeing how culture, a large part of psychology and sociology, shapes those behaviors. It also looks at how communication and individual responsibility contribute to a stronger cyber environment, showing that cybersecurity is a human subject as well as a technical subject.

Research Questions, Hypotheses, and Variables

The primary focus of this study is to understand how an organization's information security culture (ISC) influences an employee's decision to report phishing emails. The study also seeks to determine if their proposed model for this relationship is consistent across different national cultures (Germany, the UK, and the USA).

The study's hypotheses are not explicitly written as single sentences, but can be summarized into the following:

- A positive information security culture (characterized by supportive norms, clear communication, policy awareness, and security knowledge) will lead to more positive employee attitudes and a greater sense of responsibility towards security.

- Employees with more positive attitudes and a greater sense of responsibility will be more likely to report phishing emails.

The Independent Variables (IVs) are the components of the information security culture: awareness and understanding of IS policies, quality of IS-related communication, IS knowledge, and IS-supportive norms.

The Dependent Variable (DV) is the act of reporting phishing emails (Petrič & Just, 2025). Employee attitudes and their sense of responsibility can be considered mediating variables in this model.

Research Methods, Data, and Analysis

This study utilized a survey-based approach for quantitative results. The researchers collected data from employees in medium and large-sized organizations across Germany, the UK, and the USA (Petrič & Just, 2024). This method allows for the collection of a large dataset on attitudes, beliefs, and self-reported behaviors. The data was collected by asking respondents a question and rating a response statement from 1 (Never) to 5 (Very Frequently) based on their agreement with the statement.

Relation to Cybersecurity Concepts

This article relates to several key concepts in cybersecurity. The most obvious is social engineering, as phishing is a popular form of this concept. The study's focus on user education and attitude aligns with the principle of a defense-in-depth strategy, where human vigilance is a critical layer of protection (Fortinet, n.d.). Additionally, the concept of an information security culture is central to the growing understanding cybersecurity extends to people and policy rather than only technology.

Marginalized Groups: Challenges and Contributions

While this article does not focus on marginalized groups, its findings have implications that apply them. For example, individuals with less education, or those who are not as proficient in English may be more vulnerable to phishing attacks or not know how to properly report one. This shows the need for cybersecurity training and communication to be accessible to all employees regardless of their background. Marginalized groups might also be targeted by certain types of phishing scams related to immigration services or government benefits, making them more vulnerable outside of the workplace.

Conclusion: Contributions to Society

The overall contribution of this study to society is that it provides straightforward evidence for organizations to improve their resilience against phishing attacks. As Petrič and Just note, employees are more likely to report a phishing email when their organization has effective communications channels. By demonstrating this link between communication and a positive security culture, organizations are encouraged to invest in employee knowledge and engagement to strengthen their information security. This institutional shift can lead to better understanding of the importance of cybersecurity and a more secure digital landscape for everyone. The study also identifies the similarity of these psychological principles across western cultures, suggesting that the human factor remains a consistent factor in cybersecurity.

References

Daudi, M. (2024). Exploiting Human Trust in Cybersecurity: Which Trust Development Process Is Predominant in Phishing Attacks? *Applied Cybersecurity & Internet Governance, 3(2)*, 233-249. doi:https://doi.org/10.60097/ACIG/199452

Fortinet. (n.d.). *What Is Defense In Depth?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/defense-in-depth

Petrič, G., & Just, J. N. (2025). Information security culture and phishing-reporting model: structural equivalence across Germany, UK, and USA. *Journal of Cybersecurity, 11*(1). doi:https://doi.org/10.1093/cybsec/tyaf011