Article Review #1: Who Will Take the Bait? Phishing Susceptibility in a Municipal Organization

Student Name: Josiah Lynch

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 2/20/26

Introduction/BLUF

Cybercrime is growing exponentially and increasingly targeting individuals through social engineering attacks called phishing, which basically exploits basic human behavior rather than hacking the system itself. Understanding why some individuals are more susceptible to phishing is important for improving cybersecurity strategies. The article "*Who Will Take the Bait? Using an Embedded Experimental Design to Assess Phishing Susceptibility in a Municipal Organization"* studies how employees respond to phishing attempts in a real world organizational setting. One of the main findings of this study is that phishing susceptibility is influenced by individual and organizational factors and not just technical systems, proving the importance of human behavior in cybersecurity.

Relation to Social Science Principles

This article connects to social science principles like criminology and sociology. The study focuses on how human behavior, social roles, and everyday work routines affect cybercrime victimization. Instead of blaming the individuals, it shows how the environment people are in and the situations they are placed in can increase or decrease their risk of victimization, which fits with social science ideas about behavior being shaped by context.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

Research Question: Which factors influence employee likelihood to phishing attacks within a municipal organization?

Hypotheses: The author suggests that phishing susceptibility varies based on individual characteristics, exposure to training, and features of phishing emails.

Independent Variables : Employee characteristics such as age, job role, exposure to cybersecurity training, and phishing email characteristics.

Dependent Variable : Phishing susceptibility, measured by whether employees clicked on or interacted with simulated phishing emails.

Types of Research Methods used

The study uses a quantitative research method with an embedded experimental design. The employees in their organization were sent simulated phishing emails without any prior notices. By doing this approach it allows the researchers to observe authentic behavior.

Types of Data Analysis used

The behavioral data from the phishing simulations were analyzed using statistical methods. According to the author, they compared response rates across different employee groups to figure out a pattern in the phishing susceptibility and assess which factors increased or decreased risk.

Connections to other Course Concepts

The study connects to course concepts like victimization, routine activities, and risk exposure. Employees' everyday work routines create a lot of opportunities for phishing attacks, particularly when awareness and security measures are limited. The article strengthens the ideas discussed in class that cybersecurity problems are often human centered rather than just technical.

Connections to the Concerns or contributions of Marginalized Groups

The findings have implications for marginalized groups, mainly people who struggle with digital literacy or lack of training in cybersecurity. Employees in non technical roles may face higher risk of phishing victimization, showing how inequality can reach into digital environments.

Overall societal contributions of the study/Conclusion

In general, this study contributes to society by demonstrating that phishing is influenced by social and organizational factors. The evidence supports the need for improved cybersecurity education and targeted training programs instead of relying mainly on technical defense like Windows Security, Mcafee, and Norton. By applying social science perspectives to cybersecurity, the study adds to the understanding of how human behavior affects cybercrime prevention.

Reference

Spithoven, R. (2024). Who will take the bait? Using an embedded, experimental design to assess phishing susceptibility in a municipal organization. Journal of Cybersecurity

Article Link: [https://academic.oup.com/cybersecurity/article/10/1/tyae010/7695673]