Article Review #2: Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions

Student Name: Morgan Brown

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Quinn

Date: April 7th, 2026

Introduction/BLUF

BLUF: Demographic characteristics and prior experience significantly influence phishing susceptibility, and training can reduce vulnerability to social engineering attacks.

The article "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions" examines how factors such as age, gender, technical knowledge, and previous exposure to phishing affect individuals' likelihood of falling for phishing emails. It also evaluates the effectiveness of training interventions in reducing susceptibility. The study applies social science principles to real-world online behavior, highlighting how human factors, not just technology, shape cybersecurity outcomes.

Relation/Connection to Social Science Principles

The article incorporates social science principles by exploring how human behavior, demographic factors, and prior experiences influence an individual's likelihood of falling for phishing attacks. It emphasizes that behavior is shaped by differences among individuals (such as age, gender, and technical background), as well as perceptions of risk and the situational context in which decisions are made (such as the appearance and credibility of phishing emails). The study also reflects the predictability of behavior, the importance of learning and experience (with training shown to reduce susceptibility), and the interaction between cognitive processes and social influences as users evaluate potentially deceptive messages. Furthermore, it relies on empirical methods to observe and measure these behavioral patterns in a controlled setting. Overall, the article uses social science principles to explain why some individuals are more vulnerable to social engineering attacks than others.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: What demographic and experiential factors influence an individual's susceptibility to phishing attacks, and can training reduce that susceptibility?
- Hypothesis: The study is based on the following expectations:
  - H1: Certain demographic groups (such as differences in age and gender) will show varying levels of phishing susceptibility.
  - H2: Individuals with more technical knowledge or prior experience with phishing will be less likely to fall for phishing attacks.
  - H3: Security training or interventions will decrease the likelihood of users responding to phishing emails.
- Independent Variable: Age, Gender, Education Level, Technical Experience, and Prior Phishing Knowledge (training or awareness).
- Dependent Variable: Phishing susceptibility (measured by whether participants clicked on phishing links, submitted sensitive information, or failed to identify phishing attempts).

Types of Research Methods used

This was a quantitative study that focused on measurable behavior and statistical analysis rather than qualitative interviews or open-ended responses. Data was collected through a simulated phishing experiment in which participants were exposed to different types of phishing emails and asked to respond as they normally would. The independent variables (i.e., age, gender, technical experience, and prior training) were recorded for each participant, and the dependent variables were participants' actual behaviors, including whether they clicked on links

or submitted sensitive information. The participants included a diverse group of users with varying levels of computer experience, and the authors ensured that the analysis accurately reflected differences across demographic and experiential factors.

Types of Data Analysis used

The authors used statistical methods to analyze data from the simulated phishing experiment. They used logistic regression and correlation analyses to explore the relationship between demographic and experiential factors (independent variables) and participants' phishing susceptibility. Additionally, reliability analyses were conducted to ensure consistency in how participant behaviors were measured across different phishing scenarios, and comparisons between groups were performed to evaluate the impact of training interventions on reducing vulnerability.

Connections to other Course Concepts

The study "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions" connects closely with what I've learned about the social aspects of cybersecurity. In our course, we explored social engineering as a process that manipulates human behavior through stages like information gathering, relationship building, exploitation, and execution. This article highlighted how factors such as age, gender, and prior experience can shape how individuals respond to these social manipulations, emphasizing that vulnerability is not purely technical but strongly behavioral.

What I found particularly interesting is how training and awareness can change user behavior, essentially interrupting the social tactics that cybercriminals rely on. It made me think

about the overlap I mentioned in my discussion board post: if cybercriminals use social strategies to succeed, understanding those same behaviors can help professionals anticipate and prevent attacks. For example, someone who is naturally trusting might be more likely to click a phishing link, but exposure to training encourages them to pause, verify, and avoid falling victim.

Overall, this study strengthens my grasp of how social dynamics play a role in cybersecurity. It shows that human behavior is both a potential vulnerability and a key defense, providing a concrete example of how the social engineering principles we discuss in class are applied in real-world scenarios.

Connections to the Concerns or Contributions of Marginalized Groups

An important consideration from this study for marginalized groups is that demographic factors like age, gender, and access to technology can influence phishing susceptibility in different ways. Individuals from communities with limited access to cybersecurity education or workplace training may be at greater risk of falling for social engineering attacks. While the study does not specifically examine these populations, it highlights the need for tailored cybersecurity programs that consider diverse backgrounds and experiences. Providing accessible training and awareness initiatives for marginalized groups could help reduce vulnerabilities and ensure that protections are more equitable across different segments of the population. This is particularly important because falling victim to phishing and social engineering can lead to serious consequences, including financial loss, identity theft, and compromised personal information, which may disproportionately affect marginalized communities.

Overall societal contributions of the study/Conclusion

In conclusion, this study highlights how factors like age, gender, technical experience, and prior training shape people's vulnerability to phishing attacks. It underscores that cybersecurity is not just a technical challenge but also a behavioral one, where awareness and proper guidance can make a meaningful difference in reducing risk. By applying social science principles to real-world behaviors, the research provides valuable insights for designing effective training programs and interventions that help people recognize and respond to social engineering threats, ultimately contributing to safer online environments for all users.

Reference

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 373–382. https://doi.org/10.1145/1753326.1753383