Unpredictability of Phishing Scams Article Review

Charlotte Lacy

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

September 26, 2025

Principles of Social Sciences

In the article, "The unpredictability of phishing susceptibility: results from a repeated measures experiment," the study shows many relations to the principles of the social sciences. It displayed ethical neutrality by receiving consent and avoiding harmful or intrusive phishing emails. The authors also gained approval from a governmental ethics board. This article on phishing demonstrates skepticism because the authors challenge past assumptions that persuasion techniques are strong predictors of if individuals will fall for them. However, later in the article, it was concluded that persuasion and personalization techniques, such as adding a personal salutation and greeting to a specific person, have a much weaker effect than once thought. Objectivity was maintained in this experiment by measuring the behavior of people's interactions with phishing emails instead of asking if they think they would click on it. This removes bias and the risk of faulty results.

Analysis of Experiment

The research question posed was, 'What email characteristics most influence susceptibility to phishing?' In this experiment, there were three main hypotheses created: the scam represented in the email, the number of adaptations added to personalize the email to the recipient, and the number of influence techniques added to the email (Sommestad & Karlzén, 2024). The independent variables include the scam type, number of adaptations, and number of influence techniques. The dependent variables include whether participants clicked a phishing link and whether the participants executed malicious code. To test these hypotheses, a multilevel model was used as one level fits in with the variance of susceptibility to the scam of the deceptive email and the other level fits with the other two hypotheses; the number of adaptations

and influence techniques. One of the research methods used is field experiments with fake phishing emails sent to real employees in Swedish organizations. Another research method is repeated measures which is shown by participants receiving numerous phishing emails across 16 months. The data collected was binary outcomes, such as if the links in the emails were clicked or not, or if the malicious code was executed or not. To analyze this data, the authors used logistic regression, a statistical method suited for binary data, as it predicts the likelihood of an event.

Relating to the Real World

In module 2, there are concepts of research studies and the purpose of them. Since this is a research article, I was able to gain a better understanding of why research in these fields is important. The topic of this article, phishing, relates to the marginalized groups because of less access to security training so they may be more likely to be scammed as well as the language barriers that may confuse them to fall into these scams.

Conclusion

Overall, this study concludes that phishing susceptibility is much harder to predict than imagined and that security training should emphasize recognizing the scams themselves rather than personalization tricks. It contributes to society by reframing how phishing is understood by the general public as well as future researchers.

References

Sommestad, T., & Karlzén, H. (2024). The unpredictability of phishing susceptibility: results from a repeated measures experiment Open Access . *Journal of Cybersecurity*, *Volume 10*(1). https://doi.org/https://doi.org/10.1093/cybsec/tyae021

Link: https://academic.oup.com/cybersecurity/article/10/1/tyae021/7900092?searchresult=1