The Role of Human Factors in Phishing Attacks: A Behavioral Cybersecurity Study

[Cybersecurity]

Sailaja Midde
X24112666
Programme Code – Research in Computing CA1
National College of Ireland

Research Problem Background

Phishing keeps being a leading cyberattack method by fooling people through suspicious emails and websites that aim to grab private details. Although devices and systems are now stronger, ignoring security advice is still a big problem in organisations. Not all phishing attacks are due to technical problems; the majority are successful due to people being fooled by social engineering acts (Desolda *et al*., 2021). It explores the mental and social aspects that influence people's decisions while using the internet. Cognitive biases, pressure, low awareness, and trusting people in authority are some reasons why people are prone to phishing attacks (Nina *et al*., 2024). It has been shown through research that tight deadlines can result in users rather quickly accessing unknown links. Because many people can work from home now, their security responsibilities at home have grown. However, it is not common for real-world studies to look closely at this kind of behavior carefully (Mutlutürk *et al., 20*24). The purpose of this study is to shed light on how the way people act at work affects their chances of being phished.

Research Question

- How do cognitive biases (eg, authority bias and urgency) affect the chances of a person falling victim to phishing attacks?
- To what extent does stress and multitasking make a person more vulnerable to phishing in a work context?
- Does previous cybersecurity training lower refresh a working professional's vulnerability to phishing?
- To what extent do demographics (eg, age, digital literacy, and job role) correlate with phishing vulnerability?

Justification

This question is generalizable and important, because most cybersecurity breaches involve some error on the part of the user, especially with phishing attacks. Exploring the behavioral aspects gives us more context around the notion of why we are susceptible to responses to user psychology, even if there are positive technical solutions. Furthermore, the study will fill a gap in research by exploring phishing through the lens of psychological theory (Marin *et al*., 2023). This will be straightforward because it can be pursued with a number of methodologies and associated tools such as surveys, simulations, and questionnaire approaches which all reflect behavioral dimensions. The three variables being examined - bias, stress, and training - are all also directly measurable. It is of community interest in a greater context for improving training and awareness campaigns that can reduce incidents of security in the cyber context (Wei, 2024). The research will be undertaken ethically - informed consent and anonymity will be preserved as part of the data collection and analysing process. Implications for the findings from the research will be extensive and include possible benefits to IT departments, schools, and policy-makers looking to raise the bar of cyber resiliency.

Specific Items to be Addressed

Item #1: Cognitive Biases and Decisions

This involves exploring cognitive biases such as authority bias, urgency effect, and familiarity that drive users' clicks on phishing links.

Item #2: Psychological State and Environment

Looking into how users' level of stress, workload, and tendency to multitask increase or decrease their level of vulnerability to phishing in the workplace.

Item #3: Training and Awareness

Investigating if past cybersecurity training or phishing awareness programs reduce users' susceptibility to phishing.

Item #4: Demographic and Professional Factors

Assessing how factors such as age, profession, and digital literacy relate to users' susceptibility to phishing.

BIBLIOGRAPHY

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F., 2021. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), pp.1-35.

Nina, P.N., Nina, P.N., Géza, K.B., Malatyinszki, S. and Szilárd, M., 2024. The Human Factor of Information Security: Phishing in Cybercrime.

Mutlutürk, M., Wynn, M.G. and Metin, B., 2024. Phishing and the Human Factor: Insights from a Bibliometric Analysis. *Information*, *15*(643).

Marin, I.A., Burda, P., Zannone, N. and Allodi, L., 2023, April. The influence of human factors on the intention to report phishing emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-18).

Wei, W., 2024. *Operational Variations in State-Owned Hotels and International Branded Hotels in China: A Qualitative Analysis of Practitioners' Perspectives and Implications* (Doctoral dissertation, University of South Florida).