Article Name:

Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation

Relation to Social Science Principles

This article directly relates to social science principles with human behavior shaping the reason phishing attacks work. Social structures and human relationships are the only reason phishing and smishing attacks still work, they exploit the users trust by posing as trusted colleague or boss then luring the user into clicking a link or downloading a file. Workplace dynamics also play a huge role in the effectiveness of phishing attacks. Small companies where the CEO may legitimately need someone to pay for something out of their own pocket then they will pay the person back are highly susceptible to those types of phishing attacks. Another key factor could be a new employee or low trust work environment fostering a higher likelihood of successful phishing attacks.

Research Questions and Hypotheses

The main research question is: What individual and organizational factors predict whether employees fall for phishing attacks in a real-world setting?

The authors were trying to determine whether individual traits like tenure, satisfaction, and loyalty would correlate with how susceptible someone is to phishing attacks. The study aimed to find these behavior patterns to better inform and explain why some employees are more vulnerable than others.

Research Methods

The study used a naturalistic field experiment combined with a survey to determine its findings. Participants were actual employees in an organization who were unknowingly subjected to the phishing attack. Afterward the employees were surveyed to determine things like job satisfaction and organizational commitment. This approach allowed for the most accurate results on how those surveyed factors affect an employee's susceptibility to being phished.

Data and Analysis

Data like click rates on phishing emails and employee responses to survey questions were compared and contrasted to determine the susceptibility of certain employee groups. Employees that are newer or who lack job satisfaction and those who lack organizational loyalty were significantly more likely to click a phishing link.

Connection to Class Concepts

This study connects multiple class concepts like social engineering and trust in other colleagues and organizations. Behavioral science, determining why humans are always the weakest link in cybersecurity incidents. It also touched on organizational psychology and how that plays a role in your susceptibility to phishing attacks.

Relevance to Marginalized Groups

Phishing attacks disproportionately affect new or less tech inclined employees. New employees may lack the familiarity with certain coworkers or organizational norms that may lead them to trust even egregious phishing attacks. Less tech savvy employees may also get exposed more frequently because they don’t know or understand the techniques being used on them and are less likely to look for the warning signs of a phishing email.

Overall Contribution to Society

I think this study does a super good job explaining the ways social engineering and phishing attacks can plague an organization of any size. I think this study is also a good resource for which individuals in your organization may need more training to help them make the proper decision when faced with a phishing attack. It also shows that some people, especially those who lack organizational trust will always fall (either purposefully or not) for phishing attacks. I believe this article is one of the strongest examples of applied interdisciplinary sciences combining cybersecurity and psychology to help the business of society protection from these malicious actors.

References

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security, 131*, 103313. https://doi.org/10.1016/j.cose.2023.103313