Christian Demopoulos

CYSE 201S

November 6th, 2023

Article Review #2

The Prevalence of Social Engineering

Social engineering is a massive problem in modern society and affects people daily. The biggest victims in social engineering attacks are the people who are unaware. However, this is why social engineering relies on human error. Social engineering is not just as simple as following someone into a secure but could be falsifying digital signatures in emails or redirecting someone to a very fake website. Self-awareness is the half-battle, and being ready to respond is the second step. Throughout this article, we will discover how easily people are susceptible to social engineering attacks and how to respond moving forward.

To assess the risk of social engineering, a study was conducted where 138 participants were exposed to fake emails or phishing attacks. “The study explored the influence of scam type, cybercrime awareness, gender, IT competence, and perceived Internet safety on susceptibility to email scams.” (Broadhurst et al., 2019). Sadly, technology is not the culprit leading to social engineering attacks; it is human error. Human judgment has become so bad that hackers now have a monopoly. Email has been the springboard for several phishing attacks and is a popular method. These emails are popular and personalized to their victims to appear real.

"Spearphishing is contextual, with emails often containing specific information that would be familiar or important to specific recipients." (Broadhurst et al., 2019).

The ANU conducted a study to find the factors influencing cybercrime among ANU students. The school tested the following hypotheses: "H1: Scam susceptibility increases with email tailoring. H2: Scam susceptibility varies with cybercrime awareness. H3: Females exhibit higher scam susceptibility than males. H4: Lower IT competence is associated with higher scam susceptibility. H5: Feeling safe on the internet may increase susceptibility" (Broadhurst et al., 2019). The school determined who was more susceptible by creating conditions. There were two condition groups, "Hunter" and "Passive. The "Hunter" condition group received regular warnings to avoid cyber-based attacks. The "Passive" condition group received no warnings. After this was decided, the school would send phishing emails with links to a fake login page to the student portal hosted on a local server. The school found that "The most successful attack related to an urgent email sent during the exam period about the participants' final exam timetable" (Broadhurst et al., 2019). Awareness campaigns did not help, as the "Hunters" remained just as vulnerable to social engineering attacks.

While it is true the study did not support all five proposed hypotheses, new information came to light. A certain demographic was exposed to more risk than others. The study found that "the most susceptible to social engineering attacks were international students and first-year students." (Broadhurst et al., 2019). New students coming to college are at high risk of experiencing cybercrime. This set up a terrible platform for newcomers to college. In the future, this may push students away from cyber-related activities due to the increased risk.

This study showed us many things. For starters, ANU needs enhanced cybersecurity awareness to combat cybercrime. Second, the school needs to fund tailored cybersecurity training for its students. Leaving the student population in its current state will put students at unnecessary risk. Lastly, the school needs to do a better job of educating its new students. New students are the riskiest and need extra care to prevent severe cyber offenses.

In conclusion, the research on the hazards associated with phishing and cybercrime, although not conclusively verifying its first assumptions, provided insightful information on the intricate realm of online security. Targeting cybercrime education, improving cybersecurity awareness, and customizing cybersecurity training are just a few ways the study can benefit society. Together, these efforts lessen cybercrime's harm to both people and businesses. Emphasizing the complex nature of cyber risks, the study shows that email customizing, awareness prompts, and gender do not consistently correspond with fraud vulnerability. It also emphasizes how crucial it is to recognize the distinct qualities of scam content—like relevancy and urgency—that may heighten susceptibility. As we move forward, we must continue researching cybercrime preventative strategies. With social engineering techniques constantly changing, failing to do this could have devastating effects on society.

References

Broadhurst, Roderic; Skinner, Katie; Sifniotis, Nicholas; Matamoros-Macias, Bryan; and Ipsen, Yuguang (2019) *Phishing and Cybercrime Risks in a University Student Community*, International Journal of Cybersecurity Intelligence & Cybercrime: 2(1), 4-23. https://www.doi.org/10.52306/02010219RZEX445