Amanda Sandoval

21 April 2026

Professor Yalpi

Social Engineering Attacks

Humans play a vital role in the cybersecurity world; our behaviors and biases allow other individuals to break security protocols. Lack of human awareness of social engineering attacks has allowed these attackers to conduct these attacks leading to severe consequences. As humans play a huge role on social engineering attacks, the psychological perspective also attacks the decision-making of humans. Analyzing these different aspects of the human mind and behaviors to understand but also provide mitigations for social engineering attacks. Throughout this case study I will address how social engineering attacks impact human factors and discuss solutions to help mitigate and resolve these issues.

A big weakness in cybersecurity is lack of knowledge and awareness on attacks. For example, phishing attacks is a very common attack that reels an individual in by providing false advertisement to receive personal information. In most cases we as individuals don't analyze the advertisement as a threat because it looks familiar to the eye. However, if humans were to be educated on the clues that show how these emails or websites are fake it could prevent so many people from these attacks. I believe by creating an interactive awareness guide that instructs those working in the cybersecurity field about how to detect these meniscal threats and allow them to pass this information to those who need as well. By increasing security protocols, it "allows humans to recognize potential threats and reduce the likelihood of creating or allowing

security issues such as human error to occur" (Jen 2025). Another issue in cybersecurity is possible insider threats. A valuable prevention to minimize this type of threat is conducting psychological profiling. By conducting this it "enhances risk assessments by providing detailed behavioral analysis, assessing threats, and employing predictive profiling" (Jun 2025). This goes to show how important the psychological aspect of social engineering attacks is, many attackers will manipulate individuals to conduct their work to cover their tracks.

It's important to understand that cybersecurity isn't just technical issues, but the main risk is humans and their behaviors. Humans are the ones who are building these complex systems and maintaining them which can lead to it being compromised or lack security safety. Attackers tend to watch and apply social science tactics to distract and attack humans. I believe enforcing proper and effective policies designed by a sociological standard can help mitigate these attacks. Having a multidisciplinary approach to these issues allows security teams to create not only a technical defense but also incorporate behavioral methods into a strategic plan for better security. This approach also allows typical noninteractive training to become interactive and valuable training to ensure quality instruction.

In conclusion, cybersecurity doesn't just revolve around technology but includes social science perspectives and begins with human behavior. Incorporating behavioral strategies from prior threats and attacks lowers the probability of it happening again. By enforcing psychological and sociological policies it strengthens the security protocols.

References:

Jun, D. T. J., Rafsanjani, A. S., Aslam, S., & Behjati, M. (2025, December 15). *Human Factors i n Information Security: A Quantitative Study with Technical Solutions to Prevent Social Enginee ring Attacks*. ACM Digital Library.https://dl.acm.org/doi/full/10.1145/3767320#sec-4