Social engineering, like phishing attacks, stands for a major cybersecurity threat that exploits human behaviors rather than their technical vulnerabilities. In this journal cybercriminals rely on mind reading manipulation to trick people into revealing their information. Phishing attacks often copy real life organizations trying to use emails or messages to create fear or curiosity. Even though defenses like firewalls and encryption exist, human factors are still the weakest link in cybersecurity systems. This highlights the importance of cyber technology and social behavior, making it a case for social science analysis.

Using the psychological perspective of a cybersecurity professional, phishing exploits mental biases such as urgency, trust, and authority. People more likely work with requests that appear to come from authoritative sources because they can trust those due to it being protected. Social norms can also influence behavior, like employees may hesitate to question suspicious requests from their bosses. Cultural factors can also affect how people interpret communication, impacting susceptibility to attacks. This article highlights that cybersecurity is not only about technical problems but it is also a human centered issue that requires understanding the behavior and decision making process.

Working solutions must integrate both the social approaches and technical. Organizations should improve their multi factor authentications, email filtering systems, and they should keep monitoring their systems to reduce technical vulnerabilities. Even though behavioral training programs should teach people about phishing tactics using real world situations. Encouraging the workplace culture that helps people ask questions and suspicious communications can also help reduce the risk of cyber attacks happening. Many people underestimate their vulnerability, leading to low engagement in security practices. To get over these challenges some organizations can adopt interactive training to educate people about these issues in the real world. Leadership support and clear communications are also essential for fostering a security conscious culture.

This case study demonstrates the importance of social sciences into cybersecurity. Technical issues alone can’t fully fix threats that exploit human behavior. By using psychology, sociology, and anthropology, organizations have a better understanding of why individuals become victims to cyberattacks and design more effective defenses. The interdisciplinary approach shows that cybersecurity is not just about protecting systems but also about understanding people. This is a great perspective in addressing evolving threats in the digital society.

Social engineering attacks show the critical role of human factors in cybersecurity. Adding technical safeguard with social science insights leads to more effective solutions. As cyber threats continue to grow, the interdisciplinary approaches will remain important in strengthening organizational security and individuals.

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9