Phishing Attacks and Human Error in Cybersecurity

Dorian Jones

CYSE201S

Old Dominion University

4/15/2026

Phishing attacks remain one of the most common and effective cybersecurity threats, largely due to human error rather than technological failure. These attacks involve deceptive emails, messages, or websites designed to trick individuals into revealing sensitive information such as passwords, financial data, or personal details. While organizations invest heavily in technical defenses, attackers often exploit human psychology, making phishing a critical issue that combines both technological and social dimensions.

From a social science perspective, phishing attacks rely heavily on psychological manipulation. Attackers use tactics such as urgency, authority, and fear to influence user behavior. For example, an email that appears to come from a trusted organization and warns of account suspension can trigger panic, causing individuals to act quickly without verifying authenticity. Concepts from psychology, such as cognitive bias and decision-making under stress, help explain why even well-trained users fall victim to these scams. Sociological factors, including workplace culture and communication norms, also play a role, as employees may feel pressured to respond quickly to perceived authority figures.

To effectively combat phishing, organizations must adopt a multidisciplinary approach that combines technical solutions with social science insights. Technical measures include email filtering systems, multi-factor authentication, and threat detection tools. However, these must be supported by user-focused strategies such as regular security awareness training, simulated phishing exercises, and clear reporting procedures. Training programs should be designed using behavioral science principles, focusing on habit formation and repeated exposure rather than one-time instruction.

Despite these strategies, several barriers can hinder implementation. Employees may experience training fatigue, ignore security policies, or lack motivation to follow best practices.

Additionally, organizations may prioritize productivity over security, leading to shortcuts in behavior. To overcome these challenges, companies should create a security-focused culture that encourages accountability and continuous learning. Incentives, engaging training methods, and leadership support can significantly improve user compliance.

In conclusion, phishing attacks highlight the importance of addressing both technological vulnerabilities and human behavior in cybersecurity. By integrating insights from psychology and sociology with technical defenses, organizations can better understand and mitigate the risks associated with human error. This interdisciplinary approach not only strengthens security but also promotes a more resilient and informed workforce.

References

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

Verizon. (2023). *Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/