Introduction

Phishing refers to a type of cyberattack that involves deceptive messages that are convincing and request passwords, money, or personal data. According to Regenscheid and Galluzzo (2023), phishing may occur via email, text messages, and even voice calls. According to the Federal Bureau of Investigation (2025), phishing and spoofing took third and fourth places in the list of the most frequently reported cyber crimes in 2024. Verizon (2024) also discovered that it takes less than 60 seconds before users succumb to phishing emails. These facts indicate that phishing is a human problem as well as a technical threat.

Analysis

The social sciences can be used to explain the success of phishing. Psychology demonstrates that fear, urgency, habit, and trust may compel an individual to a clicking frenzy. As Alomair et al. (2025) discovered, perceptual, social, psychological, behavioral, cultural, and organizational factors influence awareness of social engineering. Sociology suggests that the roles of the workplace, group pressure, and trust in authority may render the fake requests to be normal. Anthropology can also come in handy since culture, language, and mutual values influence the ways in which individuals perceive risk and authority. A phishing email does not always work because the message is very technical, but because it is compatible with the way humans behave.

Solutions

The most appropriate solution is a mixture of cybersecurity tools and human action. Email filtering, link scanning, account monitoring, and phishing-resistant multi-factor authentication should be considered technical measures. According to Regenscheid and Galluzzo (2023), phishing-resistant authentication aids in preventing attackers from stealing login secrets

by using fraudulent sites. Human-based measures must comprise brief training, easy reporting procedures, and practice emails that are feasible. According to Dawkins and Jacobs (2023), the NIST Phish Scale can be used to understand how difficult a phishing email is for individuals to detect, which can be used to design training. However, one of the issues that can happen with these solutions is the fatigue of workers, as excessive warnings or severe criticism may lead to the disregard of precautionary messages. Open and honest leader support and feedback may help remedy that issue.

Reflection

This demonstrates that phishing is not merely an issue with computers. It is also a social issue in a way that is influenced by trust, work culture, and day-to-day pressure. A multidisciplinary approach is needed to assist security teams in developing tools and policies that are consistent with actual human behavior.

Conclusion

Phishing is still harmful as it preys on systems and human intuition. The risk can be mitigated by stronger protection of logins and training, as well as implementing healthy workplace culture. The lesson is that cybersecurity is best achieved with a combination of technical knowledge and social science is the greatest.

References

Alomair, M., Issa, T., Nau, S. Z., & Abu Salih, B. (2025). The key factors that influence employees' awareness of social engineering: A systematic literature review. *Heliyon, 11*(16), e44012. https://doi.org/10.1016/j.heliyon.2025.e44012

Dawkins, S., & Jacobs, J. (2023). *NIST Phish Scale User Guide* (NIST Technical Note 2276). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.TN.2276

Federal Bureau of Investigation. (2025, April 23). *FBI releases annual internet crime report*. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Regenscheid, A., & Galluzzo, R. (2023, February 1). *Phishing resistance – Protecting the keys to your kingdom*. National Institute of Standards and Technology. https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

Verizon. (2024). *2024 data breach investigations report*. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf