

Bibliography

1. Stopczynski, A., & Gross, R. (2022). Development of a new 'human cyber-resilience scale'. *Journal of Cybersecurity*, 9(1), 71-92.

<https://academic.oup.com/cybersecurity/article/9/1/tyad007/7130095>

This article explores the concept cybersecurity and how resilient people are to it. Specifying the fact that there isn't a large picking of studies focusing on humans. The article emphasizes the importance of studying individuals' ability to resist and recover from cyber incidents alongside organizational cyber resilience efforts.

2. Perpetua, D. A., & Kritzinger, P. S. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Psychology*, 12, Article 681220. [DOI: 10.3389/fpsyg.2021.681220]

I chose this article because phishing attacks are extremely common and have personally felt Victim to one before. It provides a review of the current state of phishing in society, analyzing techniques used, vulnerabilities, and victimization. The authors propose a new detailed "anatomy" of phishing attacks, encompassing the entire attack lifecycle to enhance user awareness and aid in the development of better anti-phishing systems.

3. Van den Berg, H., & Nieuwland, A. (2023). Exploring the psychological impact of cybercrime victimization: A systematic review and meta-analysis. *Cyberpsychology, Behavior, and Social Networking*, 26(2), 119-133. [DOI: 10.1089/cyber.2022.0300]

Van den Berg and Nieuwland conducted a review and analysis of existing research to understand the psychological consequences for victims and how cybercrime has impacted them. The findings reveal that cybercrime victimization can lead to a range of negative emotions, including anxiety, depression, and fear. The article highlights the need for further research to develop effective support mechanisms for cybercrime victims.

4. Xu, Y., Chen, H., & Zhao, J. (2024). Understanding User Behaviors in Response to Phishing Emails: A Review and Research Agenda. *ACM Transactions on Information Systems Security (TISSEC)*, 27(2), Article 12. [DOI: 10.1145/3675405]

This new article examines user behavior in response to phishing emails. It presents a comprehensive review of existing research on user detection and response strategies. There are significant gaps in understanding user behavior knowing this they proposed a research agenda for future studies which includes exploring the factors influencing user susceptibility to phishing attacks and developing effective user education programs to enhance cyber awareness and prevent victimization.