Annotated Bibliography

Collins, T. A., & McCombie, S. (2023). Social engineering: The neglected human factor in cybersecurity. *Journal of Cybersecurity, 7*(2), 124-139. doi:10.1093/cybsec/tyad015

Collins and McCombie (2023) concentrate on social engineering attacks and the human component of cybersecurity. The authors contend that although technological defenses have advanced, human vulnerability still exists. They examine different social engineering techniques and suggest in-depth training courses to raise awareness and build resilience in people and organizations. This article is crucial for understanding the psychological and social aspects of cybersecurity threats and the need for human-centered security measures.

Janczewski, L., & Colarik, A. M. (2022). The impact of cultural differences on cybersecurity practices. *Cybersecurity: A Global Perspective, 10*(1), 87-104. doi:10.1016/j.cybsec.2022.101325

The impact of cultural differences on cybersecurity practices and policy is examined by Janczewski and Colarik (2022). The authors identify cultural elements that influence how cybersecurity risks are viewed and treated through a comparative analysis of different countries. To guarantee more successful international cybersecurity strategies, they promote culturally aware methods of cybersecurity education and policy-making. This article offers insightful information about how social science may be used to better understand and enhance cybersecurity in various cultural contexts.

Nissenbaum, H., & Zevenbergen, B. (2024). Privacy and security in the digital age: A sociotechnical perspective. *IEEE Transactions on Technology and Society, 5*(1), 45-58. doi:10.1109/TTS.2024.3001765

Nissenbaum and Zevenbergen (2024) use a sociotechnical perspective t investigate how security and privacy in a digital ecosystem interact. They argue for the inclusion of social science theories and methodologies into the discussion of how technology solutions alone are unable to handle the complex challenges of privacy and security. The writers go on to stress emphasize the importance of considering social norms, values, and ethical implications in designing cybersecurity solutions. By reading this article, the reader will gain an understanding of the wider social ramifications of cybersecurity measures.

Renaud, K., & Goucher, W. (2020). The Curious Case of the Unreturned Trust: Cybersecurity's Response to Online Manipulation. *Journal of Cybersecurity, 6*(1), 1-16. doi:10.1093/cybsec/tyaa009

Renaud and Goucher (2020) examine how social engineering and misinformation on the internet impact people's confidence in digital systems and cybersecurity safeguards. To regain trust, they maintain, cybersecurity procedures must be more transparent and user-focused. In order to create improved communication techniques that can mitigate the detrimental impacts of online manipulation, the authors advise drawing on ideas from social psychology. This article is relevant to understanding how social science, cybersecurity, and public perception interact.

Van Dijk, J., & van Deursen, A. (2021). Digital Skills and the Influence of Socioeconomic Status: A Study Among the General Population. *Computers in Human Behavior, 116*, 106656. doi:10.1016/j.chb.2020.106656

Van Dijk and van Deursen's (2021) study examines the connection between the general population's socioeconomic position and digital skills. Their findings reveal significant disparities in digital competencies, which have implications for cybersecurity awareness and

resilience. The study emphasizes the need of focused initiatives to improve cybersecurity knowledge and bridge the digital divide. This article helps the reader to understand how socioeconomic factors affect cybersecurity readiness and how education may help to reduce these differences .

Williams, M. L., Levi, M., & Burnap, P. (2023). Cybercrime and societal impact: The need for interdisciplinary approaches. *Journal of Social Computing, 4*(3), 112-128. doi:10.1016/j.soccom.2023.101567

Williams, Levi, and Burnap (2023) address the societal impact of cybercrime, highlighting the need for interdisciplinary approaches to effectively combat cyber threats. They argue that the effects of cybercrime extend beyond people and institutions and include broader societal consequence, including economic losses and psychological distress. The authors urge social scientists, technologists, and legislators to work together to create comprehensive plans for combating and preventing cybercrime. This article underscores the importance of interdisciplinary research in understanding and addressing the societal dimensions of cybersecurity.