Annotated Bibliography

Johnson, M., & Patel, S. (2023). The role of trust in cybersecurity behavior: An empirical study of online banking users. *Journal of Cybersecurity, 9*(2), 130–148. https://doi.org/10.1093/cybsec/tyad020
This article investigates the connection between online banking platform trust and user cybersecurity practices like password management and phishing awareness. The authors used survey data from 500 participants to demonstrate that higher institutional trust correlates with both risky and positive cybersecurity behaviors, revealing a complex relationship where trust can sometimes reduce vigilance. The study's findings are credible because it employs exacting quantitative methods and was published in a respectable, peer-reviewed journal. The authors talk about the ramifications for cybersecurity education that strikes a balance between promoting trust and necessary security measures. This source offers insightful information about the social psychology of cybersecurity behavior and the intricate relationship between trust and decisions about digital security.

Gómez, L., & Ramirez, T. (2022). Cyberbullying in social media: Social determinants and intervention strategies. *International Journal of Cyber Criminology, 16*(1), 55–73. https://www.cybercrimejournal.com/IJCCv16n1p055.pdf
On well-known social media platforms, Gómez and Ramirez look into the social elements that contribute to teen cyberbullying. Important factors like peer pressure, family dynamics, and socioeconomic status are identified by their mixed-methods study. They recommend multi-level intervention tactics that involve schools, families, and legislators. The paper, which has undergone peer review, provides a solid integration of social science theory with practical cybersecurity concerns. The qualitative interviews give the quantitative results more context. Because it provides important insights into the social context of cyber victimization and prevention, this article is relevant to research on the human and social aspects of cybersecurity.

Nguyen, H., & Tran, D. (2021). Organizational cybersecurity culture: Effects on employee security compliance in the healthcare sector. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(2), 89–102. https://vc.bridgew.edu/ijcic/vol5/iss2/7
Nguyen and Tran investigate how healthcare workers' adherence to cybersecurity is impacted by organizational culture. According to their survey, a positive security culture that is marked by open communication and leadership support significantly improves employees' adherence to security protocols. Reliability is ensured by the peer-reviewed journal article's extensive sample drawn from several hospitals. It highlights how crucial social and organizational elements are to cybersecurity risk management. Research on the institutional and social elements influencing cybersecurity behaviors, particularly in vital industries like healthcare, can benefit from this source.

Zhao, Y., & Li, X. (2023). Privacy concerns and information-sharing behavior on social networking sites: A cross-cultural study. *Journal of Cybersecurity, 9*(3), 210–225. https://doi.org/10.1093/cybsec/tyad030
In a cross-cultural study, Zhao and Li examine how privacy concerns affect users' willingness to

share information on social networking sites. The study compares users in China and the US and reveals significant differences influenced by cultural values surrounding privacy and trust. This article, which was published in a peer-reviewed, high-impact journal, combines cultural psychology and cybersecurity research. Its comparative approach enhances its ability to comprehend how global social factors impact cybersecurity. For studies looking at how culture affects cybersecurity attitudes and behaviors in a connected digital world, this source is extremely pertinent.