Annotated Bibliography

Ray Montes Jr.
25 June 2025

Ray, G., McDermott, C. D., & Nicho, M. (2024, December 19). *Cyberbullying on social media: Definitions, prevalence, and impact challenges | journal of cybersecurity | oxford academic*. Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/10/1/tyae026/7928395

When reading this article, it defines how common cyberbullying is and the effect it has on people, including young adults as a majority. The authors explain how there is no clear one definition towards the study and fight behind cyberbullying, but how bullying in general can be more corrupt than in person since in the realm of cyber, it spreads quickly and can happen at any time of the day. When understanding social media, this article is helpful for bullying and why it is tough to deal with and is a good source for anyone studying cyberbullying and online safety.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022, May 23). *Developing metrics to assess the effectiveness of Cybersecurity Awareness Program | Journal of Cybersecurity | Oxford academic*. Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603

Let's look at cyberbullying on social media and how it is defined, how common it is and the possible effects it has on others. It is explained that the definition varies widely since there are different takes on it. The authors point out three roles that people usually play and show how each affects the way cyberbullying spreads. The roles include those of active bullies, bystanders, and those that share content that is hurtful. This all reports that it is widespread and leads to much more serious impacts, and emotional distress and even depression, since this covers a large audience faster than you think and can happen at any given moment. The importance stressed is that of clearer role definitions and improved reporting systems to better understand and counteract cyberbullying effectively. This article overall is impactful as it totals up current research emphasizing what's missing in study policy and design. This is useful for papers about social media safety, online behavior, and young mental health.

Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2024, January 2). *Systematic literature review on Advanced persistent threat behaviors and its detection strategy | journal of cybersecurity | oxford academic*. Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/10/1/tyad023/7504935

In this article we look at how it reviews sophisticated and long-running attacks that are advanced persistent threats, but also how they are detected from 45 various studies from academia and industry. They used the PRISMA thorough approach in gathering and analyzing research highlighting that APTs spread laterally across systems by exploiting existing vulnerabilities. They point out that current detection methods miss plenty of risks since they don't combine behavioral tracking with vulnerability analysis. The authors propose a better approach using vulnerability scores, metrics on probability, and attack paths on visual maps to spot APTs earlier. This is helpful because it sums up a lot of information from research and shows short falls for methods and suggests practical improvements.

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021, October 7). *Cyberattacks, cyber threats, and attitudes toward cybersecurity policies | journal of cybersecurity | oxford academic*. Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745

This particular survey experiment of 1022 Israeli participants explore how lethal versus non-lethal cyberattacks change public support on government cybersecurity actions. Participants watched simulated news reports of cyberattacks targeting national infrastructure. Results showed when people saw lethal tactics (including death), they are more likely to support policies requiring government to alert citizens. When they hear about non-lethal attacks, they prefer stronger policy oversight instead. This highlights threat perception and how it plays a key role in molding attitudes about cybersecurity laws. Ultimately, it implies citizens may be willing to give up some civil liberties if they think the cyber threat is critical.