My New Understanding of the Use of Artificial Intelligence in Cybercrime

Kaleb Yonas
2/12/2024

After reading Understanding the Use of Artificial Intelligence in Cybercrime by Katalin Part, Thomas Dearden, and Sinyong Choi. I have learned how AI is being used for cybercrimes. The article I read talked about the relation of artificial intelligence and cybercrime. It shed light on how criminals use AI for their cyber crimes. The article also pulls from two articles that are from the International Journal of Cybersecurity Intelligence and Cybercrime. The articles are Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks, a case study by Mohammad Asfour and Juan Carlos Murillo, and Victimization by Deepfake in the Metaverse: Building a Practical Management Framework by Julia Stavola and Kyung-Shick Choi.

The first study was centered around victimization by deepfake in the metaverse. Julia Stavola and Kyung-Shick Choi explored how personal cyber victimization in the metaverse can be analyzed to deep fake crime, and they proposed a practical management framework to solve it. Using eight semi-structured interviews with experts from policy, academia, and industry in South Korea, Julia Stavola and Kyung-Shick Choi were able to conduct thematic analysis to identify key themes when personal cyber victimization in the metaverse was linked to deep fake crime. Through their study they learned that deepfake crimes are usually targeted towards the younger population fueled with the motivation of financial gain or sexual gratification Stavola, J., & Choi, K. (2023). This shows that we need to improve our criminal justice processes, digital law enforcement , and our psychological support for victims that have combated this rising threat.

The second study was centered around harnessing large language models for social engineering attacks. Mohammad Asfour and Juan Carlos Murillo explored how large language models like Chat-gpt can be used for cyber attacks like phishing. Mohammad Asfour and Juan Carlos Murillo were able to learn that traits like naivety, carelessness, and impulsivity correlate with a higher chance of being a victim of these attacks Asfour, M., & Murillo, J. C. (2023). Using this information we can implement cybersecurity frameworks that aid and safeguard such potential victims of such attacks.

Technology is not going to stop improving, so it is important for us to learn about these new threats so we can implement ways to protect ourselves against them. The article I read taught me a lot about how AI is being used for cyber crimes. This article also connected the relation of technology and criminology. This is important because both these practices shape and will keep shaping our field of cybersecurity and cybercrime.

References:

Parti, K. , Dearden, T. & Choi, S. (2023). Understanding the Use of Artificial Intelligence in Cybercrime. International Journal of Cybersecurity Intelligence & Cybercrime: 6(2), . DOI: https://doi.org/10.52306/ 2578-3289.1170

Asfour, M. & Murillo, J. C. (2023). Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks: A Case Study. International Journal of Cybersecurity Intelligence & Cybercrime: 6(2), 21-49. DOI: https://doi.org/10.52306/2578-3289.1172

Stavola, J. & Choi, K. (2023). Victimization by Deepfake in the Metaverse: Building a Practical Management Framework. International Journal of Cybersecurity Intelligence & Cybercrime: 6(2), . DOI: https://doi.org/10.52306/2578-3289.1171

The Article

https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1170&context=ijcic