Madison Baughman

Professor Yalpi

CYSE 201s

6 February 2024

Article Review #1 on Understanding the Use of Artificial Intelligence in Cybercrime

**Introduction**

This article seeks to expand the reader's understanding of artificial intelligence in cybercrime through specific case studies and analysis of AI's implications in today's world. Studies in both metaverse deepfakes and human vulnerabilities in social engineering attacks are examined. By looking at different examples of artificial intelligence in cybercrime a more comprehensive understanding can be reached.

**Principles of Social Sciences**

Several principles of social science can be applied to this article. The analysis of more than one study relates to relativism and having connections throughout a system. A change in one area of artificial intelligence can affect another. Ethical neutrality is considered when collecting data for analysis. Protecting individual rights is a first priority in any study conducted. Lastly, objectivity is important to keep in mind to study fact and not opinion. Conducting research to come to new conclusions about developing technology.

**Study on Metaverse Deepfakes**

The first study reviews victimization by deepfake in the metaverse. The study sought to identify likely offenders by conducting eight interviews with industry experts in South Korea (Parti et al., 2023). The study found that these crimes were likely to be committed by people in their twenties motivated by financial gain or sexual gratification (Parti et al., 2023). It was

concluded that criminal procedures and police enforcement needed to be established to mitigate the risks associated with the metaverse.

**Study on Human Responses to Social Engineering Attacks**

The second study focuses on human responses to social engineering attacks and using AI as a tool to research it. The study aimed to identify certain vulnerabilities or human traits susceptible to social engineering (Parti et al., 2023). GPT was used to simulate target responses to social engineering. It was found that people with naivety, carelessness, and impulsivity were most susceptible (Parti et al., 2023). This study can be applied to employee training and being able to target and address certain vulnerable traits.

**Relating to the Real World**

In class we have discussed conducting survey research and field studies, as well as psychology and human factors. All of which are relevant to this study, especially when it comes to collecting data and evaluating human vulnerabilities. AI can often take advantage of people with vulnerabilities. Especially when learning a new language, it's difficult to discern between what's human or computer generated.

**Conclusion**

It cannot be understated the importance of having a comprehensive understanding of technology and its implications. Research must be conducted to evaluate the benefits and consequences. By evaluating studies in different areas of artificial intelligence, we can make sound connections to real world implications of its effects. Better criminal justice policies can be developed on these connections and analyses.

# References

Parti, K., Dearden, T., & Choi, S. (2023, August 30). *Understanding the Use of Artificial Intelligence in Cybercrime*. International Journal of Cybersecurity Intelligence & Cybercrime. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1170&context=ijcic