Sebastian Stovall
11-10-23

Article Review #2: Understanding Artificial Intelligence and Cybercrime

Sebastian Stovall
11-10-23

About the article

The article, "Understanding the use of Artificial Intelligence in Cybercrime" touches on two papers written by students discussing how people have taken advantage of artificial intelligence to commit crimes. It is broken up into two sections based off the two different studies that make up the article.

Study 1

The first study involves the researcher using interview methods to gain knowledge on cybercrime in the metaverse from "policy, academic, and industry experts" to gain an understanding on why criminals commit crimes in the metaverse and what are the best ways to mitigate these acts. The article states that this information was used to "identify themes in the expert testimonies on the topics of deepfake crime in the metaverse." (Understanding the Use of Artificial Intelligence in Cybercrime). The study continues to mention principles such Routine activities theory as a framework to consider why people commit cybercrimes in the metaverse. The author comes to the conclusion that "proper guardianship" is an effective way to mitigate these cybercrimes. The study can also be related to the social principle of Relativism. The author acknowledges the relative relationship between kids and technology, as it continues to be integrated more into society, and therefore, resolves to have them be guarding more carefully when used technology rather than be stripped of it. The study can be further used as a way to help parents understand the importance of monitoring their children's internet use as the Metaverse becomes a bigger part of society.

Study 2

The second study looks into how people have used GPT Large Language modeling to find people who are vulnerable to social engineering attacks. The author uses the LLM to

"stimulate target vulnerabilities" along with the "Big Five Personality Traits model to categorize human personality traits".(. By doing such, the author can find the conclusions that the cybercriminals come to. The author comes to the conclusion that those who possess traits like naivety, carelessness, and impulsivity are more susceptible to attacks. The second study can be related to the theory of relativism in a similar was as the first study. The study acknowledges the relationship between certain personality traits and susceptibility to social engineering attacks. This study also plays into the principle of social norms and cybersecurity. It is important to note the fact that most people don't have cybersecurity in the forefront of their mind, and this causes them to neglect and find themselves vulnerable to these kinds of attacks. This research is important to take note of as it is key that we identify these traits in individuals and put special emphasis on the importance of avoiding social engineering attacks to these individuals.

Conclusion

Both studies in the articles serve a key purpose in today's society, as we must continue to try to understand why and how cybercriminals commit the crimes that they do in order to find the best way to combat these practices. The first study is crucial with today's victims of cybercrimes largely being younger people in today's generation. Both studies and summarized well in the article and provide a new and interesting take on the new ways cybercriminals are taking advantage of resources to commit crimes.