Article 1 review

Elizabeth Simpkins

2/16/2025

The risks of AI cybercrime and the need for cyber hygiene

AI, Cybersecurity, and the Social Sciences

The research article called *Investigating the intersection of AI and cybercrime: Risks, trends, and countermeasures* discusses AI, social science research and cyber awareness. It connects cybersecurity and the social sciences through the analysis of criminological theories such as the routine activity theory in relation to cyberspace and the advancement of technology due to AI. The article also includes an analysis of what AI tools hackers use and how people communicate through social media to discuss malicious usage. This research studies how AI is used maliciously over the internet, how public forums are used to converse about the malicious AI prompts, and how cyber hygiene can be improved in order to safeguard more people online.

Research Methods and data analysis used

This research used quantitative and qualitative research to understand AI's role in cybercrime. The quantitative research covers the data collected from what AI is giving out as far as information and what is collected from forums that cybercriminals use. The qualitative research is the solutions that have been collected through interview processes in order to help protect people online. The research team collected prompts across both the dark and clear web of malicious uses of AI prompts. They also recorded what generative AI sources were used, such as ChatGPT. The interview responses were focused on AI in relation to how it is used online, how cyber hygiene can be improved with it, and policies used for mitigation of its use in threats. The criminological theories were also applied to help create the questions for the interviews, in order to determine the best practices for anyone who uses the internet based on their online practices whether they have them or not. The usage of this data helped the team create a well-formed analysis of how AI is used across the internet, including media forums and prompt creations, as well as the experimental solutions for new cyber hygiene that can be implemented into businesses and people's lives in order to cope with this new increase in cyber threats.

Relating the research back to class presentations

The first two things that I thought of when I read this research article was the connection between criminology and cybersecurity and the usage of surveys in social science research that was discussed in the first week. This research conducted was based upon the analysis through the collection of prompts, forums, and surveys through face-to-face interviews. Another concept in the research that was covered in class is ethical neutrality. This can be seen in the discussion of whether AI should be used and whether it is ethical to implement and use it more when it could take jobs away. The research remains neutral because it focuses on both sides without agreeing to one or the other. They focus on the malicious use of AI and the benefits to using cyber hygiene. The last concept that I noticed in this research was cyber victimization which was discussed in week 5. Wider populations of people are being affected and fooled by AI-attacks such as "fraud, cyberattacks, and misinformation" (Shetty, Choi, & Park, 2024) spread like in campaigns for elections.

How AI threats and cyber hygiene relate to marginalized groups

The usage of AI in the development of malicious AI attacks can be a challenge and concern for people with very little cyber hygiene or AI knowledge. Marginalized groups, outside of the typical cybersecurity employees of men, can help add to the conversations of developing new policies and hygiene tactics to mitigate against attacks. Specific marginalized groups may be targeted in some of the attacks, however, particularly during elections, to try to sway their opinion when the election comes. This can occur when deepfake videos are created by AI to make false content online to try to get more votes for one party over the other.

Conclusion

AI in the wrong hands on the internet can create a lot of issues, but the implication in the right hands can create ease of work. The article examined the creation of prompts through AI and the usage of media to distribute these malicious prompts across the internet to anyone in the world. The interviews used in the analysis of this research helped develop a wider understanding of what the motivations behind AI-driven attacks are and the need for a focus on cyber hygiene. This research was meant to help society work with AI by understanding how to use it more, how it can be implemented into education, and the need for research into innovative cyber hygiene against AI cyber threats.

References

Shetty, S., Choi, K. & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime, 7*(2). DOI: https://doi.org/10.52306/2578-3289.1187