## Introduction

The article I will be reviewing is called “Investigating the intersection of AI and Cybercrime: Risks, Trends, and countermeasures.” The article aims to identify what are the new technology and AI tools cybercriminals use like malwares, social engineering, etc.

## Relationship to social science principles

I feel that the article relates to the economic aspect of social science being that some of the attacks the criminals use is very damaging to companies and its important to see what are to cost of damages the criminal cost the company. Also, what would be the prevention cost of obtaining tools to protect their company from future threats. Another relationship would be criminology as the definition of criminology is the study of criminal activity, motives, etc. Studying instances with AI.

## Research questions of hypotheses

With the information from the article, some questions and hypotheses that arose while reading were how does the media play a part in spreading AI-facilitated crime? Also, how are companies spreading awareness to prevent employees from falling for cybercriminals traps. How effective are companies current treat preventions?

## Research Methods

This study uses both quantitative and qualitative data to answer the questions on AI and cybercrime. The quantitative methods focus on identifying malicious AI prompts and forums, while the qualitative methods give insights to legal solutions and other methods to gain answers.

## Types of data and analysis

The data contained a multitude of information collected from various online websites and also getting various information from experts in cybercrime, cybersecurity, and criminal justice. They used this information to determine trends and pattens to cybercrime to deter it.

## Relationship to PowerPoint concepts

Something that stands out when discussing this article that relates to the PowerPoint is the routine activities theory. The theory is a concept which explains why crime happens. To be more specific, it focuses on why offender make the choices they make when committing crime. So for this article, it would be more focused on why criminals commit cybercrime, what did they see in going for the cyber side rather than physical, or what makes cybercrime more popular than other acts of crime.

## Challenges, concerns, and contributions of marginalized groups

Something I feel is a challenge in this article is going into better detail about the groups of people who are educated on cybercrime and who aren’t. I feel the results would’ve been a bit different if they showed the differences between the two.

## Conclusion

Overall, this article touches on the importances on spreading awareness of cybercrime and AI having a part in it. Its important for people to understand the consequences of not having the proper knowledge of cybercrime. Not only cybercrime, but AI being that although AI is a helpful tool for everyone, it still can pose a threat if used incorrectly.

## 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

##