Article Review #2 - Understanding Artificial Intelligence in Cybercrime

Adan Romero

4/10/2025

CYSE 201S

Article 2

Instructor Diwakar Yalpi

Introduction

As technology advances, crime is also evolving. Criminals are finding new ways to commit offenses using tools like artificial intelligence (AI). The following article by Choi, Dearden, and Parti (2024) discuss how Artificial Intelligence is being utilized by cybercriminals to automate phishing campaigns and create deep fakes. It is further discussed that there's still not enough research on how it's being misused.

How topic relates to social science principles

The topic of AI use in cybercrime relates to social science principles because it explores human behavior and technology. Social sciences study how people make decisions, respond to risks, and adapt to changes. This research looks at how criminals misuse technology (like AI) for harmful purposes. Also the human behavior aspect, involves understanding motivations behind cybercrime. Overall, technology and human behavior are some concerns of social sciences.

Research questions/hypotheses

While reading a research question I felt that was valid was: what ways can AI-related cyber crimes be addressed through social science-based frameworks. Different fields require different frameworks. Choi, Dearden, and Parti (2024) discuss how the framework will look different depending on the sector.

Types of research methods used

Exploratory research is often conducted in newer fields to gain a better understanding of issues. Its primary goals are to scope a problem, make hypotheses, and deeper investigation. Exploratory research is used when studying a new topic to understand it better. For example, if people are unhappy with government policies during a recession, exploratory research can help identify the main issues. This helps decide if more in-depth research is needed to address the problem.

Types of data and analysis done

The research during this study uses collected data and gathered opinions from experts on how people use AI prompts for cybercrime. They study how large language models (LLMs) can be manipulated into creating more complex phishing emails. Language models, like GPT-based systems, can be manipulated by cybercriminals, by creating prompts that work around safety guidelines.

How topic relates to the challenges, concerns, and contributions of marginalized groups

The use of AI in cybercrime can have a significant impact on marginalized groups, who are often more vulnerable to digital threats because of limited access to resources and security. These communities are more likely to fall victim to AI phishing scams or deep fakes. Especially when they target sensitive areas like immigration, financial aid, or healthcare—areas that affect marginalized populations significantly.

Describes the overall societal contributions of the study

This study contributes to society by increasing awareness of how artificial intelligence, particularly large language models, can be misused in cybercrime. This can include creating more convincing phishing emails. By identifying these risks the research helps inform the public about potential threats and the need for stronger digital security measures. This study aims to promote a safer and more informed society in the age of AI.

Conclusion

This study covers the growing concern of AI being used in cybercrime, particularly the manipulation of large language models to create phishing attacks. By collecting expert opinions and analyzing real world examples. Researchers can provide insights into how cybercriminals exploit AI. The study also emphasizes the importance of understanding the social impact of these threats, especially on marginalized groups who may be more vulnerable to digital exploitation. Overall, the study not only raises awareness but also encourages the development of ethical guidelines and stronger cybersecurity measures.

References

Choi, S., Dearden, T., & Parti, K. (2024). Understanding the use of artificial intelligence in cybercrime. *International Journal of Cybersecurity Intelligence & Cybercrime, 7*(2), Article 1. https://vc.bridgew.edu/ijcic/vol7/iss2/1/