



جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة المخاطر

AI-Driven Cybersecurity Threats and Organizational Consequences

Nawaf Fahad Alarfaj

Supervised by:

د. الفیصل عبد الحمید

د. فايز جراد

Academic Year:

2024

Introduction:

The study investigates the implications that AI-driven cybersecurity threats have on organizations. It underscores the dual nature of AI as both a tool for improving security and a facilitator of sophisticated attacks.

Problem of the Study:

AI-powered cyberattacks are increasingly posing threats to companies, creating a need for instituting prompt defense approaches to avert the threats.

Importance of the Study:

Gaining insights on AI-driven threats is essential for devising vigorous cybersecurity measures that will boost the resilience of organizations and protect sensitive data.

Objectives of the Study:

- To evaluate how companies can boost defenses to overcome AI-powered attacks.
- To pinpoint future hacking approaches using AI tools.
- To identify measures for enhancing phishing attacks' resilience.

Research Questions:

- How can various organizations enhance their safeguards against AI-powered cyberattacks?
- What avenues will future hackers use to access AI tools?
- What approaches can companies institute to boost resilience against phishing emails?

Hypotheses of the Study:

- Companies that invest in breakthrough AI technologies will considerably minimize their susceptibility to cyberattacks.
- Future hackers will continuously use generative AI tools to perform sophisticated attacks.

- Multifaceted security methods will effectively alleviate phishing threats.

Previous Studies:

Earlier studies illustrate that cyberattacks are increasingly capitalizing on AI technologies, necessitating organizations to embrace adaptive security measures.

Theoretical Framework of the Study:

Cybersecurity theories that emphasize the connection between technological improvements and developing threats guide the study.

Methodology and Research Methods:

The research employed a case study approach. It analyzed three companies to foster an understanding of effective defense measures against AI-powered attacks.

Study Tools:

The study involved gathering data from surveys, interviews, and examination of current cybersecurity tools and frameworks.

Boundaries of the Study:

The study emphasizes companies in the technology industry by assessing how they respond to AI-powered cyber threats.

References:

Kale, A. (2024). AI-Driven Cybersecurity Threats and Organizational Consequences.

California State University, San Bernardino.

<https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=3173&context=etd>