

INTO THE MATRIX: NAVIGATING CYBERSECURITY IN THE AI AGE

Level: Fundamental | **Duration:** 3 days

Into the Matrix: Navigating Cybersecurity in the AI Age is a comprehensive training program aimed at equipping participants with the necessary skills to effectively navigate the rapidly changing cybersecurity landscape shaped by artificial intelligence (AI). The curriculum examines the dual role of AI in both enhancing cybersecurity measures and facilitating sophisticated threats. Participants will analyze real-world case studies, address emerging threats such as adaptive malware and deepfakes, and develop strategies for the protection of digital assets. The program also incorporates a discussion on ethical considerations, including data privacy, and explores future trends in cybersecurity through the lenses of predictive analytics and AI-human collaboration. Upon completion, attendees will acquire the requisite knowledge to protect themselves in an AI-driven digital environment.

Objectives

This training program equips participants with the essential knowledge and skills to navigate the complexities of cybersecurity influenced by artificial intelligence (AI). Participants will learn about AI's impact on defense strategies, emerging threats, and effective methods for protecting digital assets.

Target Participants

1. General Public
2. Students and Educators
3. Cybersecurity, IT and Tech Support Personnel

Modules

Module 1: Introduction to AI and Cybersecurity
Module 2: History of AI
Module 3: Role of AI in Cybersecurity
Module 4: Cybersecurity Threats in the AI Era
Module 5: Case Study: AI-Powered Cyberattack
Module 6: Scams Using AI
Module 7: How AI Enhances Cybersecurity for Individuals
Module 8: Cybersecurity Best Practices for the Public
Module 9: Ethical and Privacy Concerns in AI
Module 10: The Future of AI and Cybersecurity

Entry/Enabling Requirements

1. Fundamental Knowledge of Cybersecurity Concepts
 - Understanding of cybersecurity fundamentals, including various threat types (e.g., phishing, malware), basic network security measures, and widely accepted cybersecurity practices.
2. Preliminary Knowledge of Artificial Intelligence
 - Acquainted with core AI concepts, including machine learning, algorithms, and the application of AI across different sectors.
3. Proficiency with Digital Technologies
 - Experience utilizing digital devices and online platforms in a secure manner, accompanied by awareness of prevalent cyber threats and overall digital literacy.
4. Engagement with Emerging Technologies
 - An enthusiasm for exploring and grasping new advancements in AI and cybersecurity, as well as their convergence within the contemporary digital environment.

Learning Outcome

1. Fundamental Principles of AI and Cybersecurity
 - Comprehend core concepts of artificial intelligence and cybersecurity, focusing on how AI enhances cybersecurity measures and introduces novel vulnerabilities.
2. Classification and Assessment of AI-Enabled Cyber Threats
 - Identify various categories of AI-driven cyber threats, including adaptive malware and deepfake technologies, and evaluate their potential ramifications for individuals and organizations.
3. Critical Evaluation of AI Applications in Cybersecurity Case Studies
 - Analyze case studies to investigate the utilization of AI in both cyberattacks and defensive strategies, deriving insights into the efficacy and limitations of AI in cybersecurity applications.
4. Examination of Ethical and Privacy Considerations Related to AI
 - Explore ethical dilemmas and privacy issues pertinent to the application of AI in cybersecurity, emphasizing data management and the necessity for transparency and ethical AI implementation.
5. Forecasting Emerging Trends in AI and Cybersecurity
 - Articulate developing trends and prospective innovations in AI and cybersecurity, including predictive cybersecurity techniques and the critical role of human oversight in AI-integrated environments.

For additional information, please visit www.cyberguru.my. You can also contact us at training@cybersecurity.my or call at 03 8800 7999