CYBERSECURITY AND AI:

FROM FUNDAMENTALS TO FUTURE THREATS

WORKSHOP INSTRUCTOR:
Mr Foo Yong Qi
Instructor (Educator Track) and PhD in Computer Science Candidate, NUS School of Computing
https://www.comp.nus.edu.sg/cs/people/e0202247/

Cybersecurity is no longer just about firewalls and passwords - it's an escalating battle where attackers increasingly leverage artificial intelligence (AI) to automate and refine their tactics.

This workshop aims to equip technical professionals with a solid grounding in core cybersecurity principles while exploring how AI is transforming both threats and defenses. Through real-world examples, and hands-on exercises, participants will learn to navigate this evolving landscape with confidence.

1. **Cybersecurity Fundamentals:** Core concepts, defense pillars, risk management
2. **AI-assisted Cyber Threats:** Adversarial machine learning, AI-generated social engineering
3. **AI-assisted Defense:** Anomaly detection, automated threat response

Who should attend?

- Professionals (e.g. data scientists and data engineers) with some technical background who wants to gain an understanding of cybersecurity and AI.
- Prior knowledge on AI or cybersecurity are not required.

EXCLUSIVE FOR COMPUTING MEMBERS