



**CYBER SECURITY**  
**FUNDAMENTALS**  
5 Days Workshop Series

# COURSE DESCRIPTION

The Cybersecurity Fundamentals Online Course will provide learners with principles of data and technology that frame and define cybersecurity. Learners will gain insight into the importance of cybersecurity and the integral role of cybersecurity professionals.

The interactive, self-guided format will provide a dynamic learning experience where users can explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

## COURSE CONTENT:

### Day 1

#### Module 1

- Getting Started
- Cyber Security Fundamentals
- What is Cyberspace?
- What is Cyber Security?
- Why is Cyber Security important?
- Who is a Hacker?

#### Module 2

- Types of Malware
- Worms
- Viruses
- Spyware
- Trojans

### Day 2

#### Module 1

- Cyber Security Breaches
- Phishing
- Identity Theft
- Harassment
- Cyberstalking

#### Module 2

- Types of Cyber Attacks
- Password Attacks
- Denial of Service Attacks
- Passive Attack
- Penetration Testing

### Day 3

#### Module 1

- Prevention Tips
- Craft a Strong Password
- Two-Step Verification
- Download Attachments with Care
- Question Legitimacy of Websites

#### Module 2

- Mobile Protection
- No Credit Card Numbers
- Place Lock on Phone
- Don't Save Passwords
- No Personalized Contacts Listed

## Day 4

### Module 1

Social Network Security  
Don't Reveal Location  
Keep Birthdate Hidden  
Have Private Profile  
Don't Link Accounts

### Module 2

Prevention Software  
Firewalls  
Virtual Private Networks  
Anti-Virus & Anti-Spyware  
Routine Updates  
Case Study

## Day 5

### Module 1

Critical Cyber Threats  
Cyber terrorism  
Cyberwarfare  
Cyberespionage

### Module 2

Defense Against Hackers  
Cryptography  
Digital Forensics  
Intrusion Detection  
Legal Recourse  
Q&A Session





# LEARNING OBJECTIVES:

- Explain the core information assurance (IA) principles.
- Identify the key components of cybersecurity network architecture.
- Apply cybersecurity architecture principles.
- Describe risk management processes and practices.
- Identify security tools and hardening techniques.
- Distinguish system and application security threats and vulnerabilities.
- Describe different classes of attacks.
- Define types of incidents including categories, responses and timelines for response.
- Describe new and emerging IT and IS technologies.
- Analyze threats and risks within context of the cybersecurity architecture.
- Appraise cybersecurity incidents to apply appropriate response.
- Evaluate decision making outcomes of cybersecurity scenarios.
- Access additional external resources to supplement knowledge of cybersecurity.



## LEARNING OUTCOME:

- Evaluate the computer network and information security needs of an organization.
- Assess cybersecurity risk management policies in order to adequately protect an organization's critical information and assets.
- Measure the performance of security systems within an enterprise-level information system.
- Troubleshoot, maintain and update an enterprise-level information security system.
- Implement continuous network monitoring and provide real-time security solutions.
- Formulate, update and communicate short- and long-term organizational cybersecurity strategies and policies.

## TRAINING METHODOLOGY:



**VIRTUAL SCENARIOS**



**TEAM ACTIVITIES**



**CASE-STUDY**



**APPLICATION OF IR 4.0**



**CLASSROOM TRAINING**

# Limited Seats Book your slot now!

Call: +6 019-623 9006  
Email: [indran@ecot.com.my](mailto:indran@ecot.com.my)

**EFFINGHAM CENTRE OF TECHNOLOGY**  
D-1-10, Block D No.2, Jalan PJU 1A/41B  
Pusat Dagangan NZX Ara Damansara  
43701 Petaling Jaya Selangor Darul Eshan



**Registered  
Training Provider**