MINISTRY OF DIGITAL

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

CYBERSECURITY ESSENTIALS: STRENGTHEN YOUR DIGITAL DEFENSES

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

This course will provide participants with an understanding of the fundamental concepts and principles of cybersecurity. It is designed to equip individuals with the necessary knowledge and skills to identify, assess, and mitigate common cyber threats while promoting best practices for secure digital environments.

Objectives

Participants will be able to understand fundamental cybersecurity concepts, identify and mitigate cyber threats, implement best practices, secure systems and networks, respond to incidents, adhere to compliance standards, and stay updated on emerging trends.

Pre-Requisites

1. Basic computer literacy, including familiarity with using a computer and navigating the internet.
2. Access to a laptop or desktop with an internet connection.
3. No prior cybersecurity knowledge is required, but a basic understanding of IT concepts is beneficial.
4. Interest in learning foundational cybersecurity practices and concepts.
5. Commitment to participate actively in hands-on exercises and discussions.

Target Participants

1. General Public
2. Beginners with little to no cybersecurity knowledge.
3. IT staff looking to enhance their understanding of cybersecurity fundamentals.
4. Non-technical professionals seeking basic cybersecurity skills.
5. Students and educators interested in cybersecurity awareness.
6. Employees from any sector needing to adopt secure practices in the workplace.

Modules

Module 1: Introduction to Cybersecurity
Module 2: Understanding Cyber Threats
Module 3: Core Cybersecurity Principles
Module 4: Cybersecurity Breaches
Module 5: Core Cybersecurity Framework
Module 6: Data Privacy and Protection
Module 7: Network Security
Module 8: Secure Programming
Module 9: AI Risks in Cybersecurity

Learning Outcome

1. **Understand Cybersecurity Basics**
   - Explain the importance of cybersecurity and its role in protecting digital assets.
   - Define key cybersecurity terms, concepts, and frameworks.
2. **Identify Cyber Threats**
   - Recognize common cyber threats such as phishing, malware, ransomware, and social engineering.
   - Assess the potential impact of these threats on personal and organizational data.
3. **Apply Security Best Practices**
   - Demonstrate proper cyber hygiene practices, including strong password creation and multi-factor authentication.
   - Implement basic security measures to protect data and devices.
4. **Secure Systems and Networks**
   - Describe essential tools and techniques for securing systems and networks, such as firewalls and encryption.
   - Identify and address vulnerabilities in network environments.
5. **Respond to Cyber Incidents**
   - Outline the steps in an incident response process, including detection, containment, and recovery.
   - Understand the basics of business continuity and disaster recovery planning.
6. **Promote Compliance and Awareness**
   - Explain the importance of cybersecurity policies, standards, and compliance frameworks.
   - Encourage cybersecurity awareness and proactive practices within teams or organizations.
7. **Stay Updated on Trends**
   - Discuss emerging cybersecurity technologies and challenges, such as AI, IoT, and cloud security.
   - Recognize the need for continuous learning in the rapidly evolving field of cybersecurity.

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

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my