

Cyber security Essentials

What You Will Learn

- 1 ☐ Introduction to Cyber security
 - What is cyber security?
 - Why cyber security matters
 - Cyber security domains and careers
 - Cyber security challenges in the modern world
- 2 ☐ Cyber Threats, Vulnerabilities & Attacks
 - Types of cyber threats (malware, phishing, ransom ware)
 - Social engineering attacks
 - Vulnerabilities and exploits
 - Real-world cyber-attack examples
- 3 ☐ Network Security
 - Securing networks and devices
 - Firewalls and intrusion prevention
 - Secure network design basics
 - Monitoring and threat detection
- 4 ☐ Operating Systems & Endpoint Security
 - Securing Windows, Linux, and mobile systems
 - User authentication and access control
 - Patch management and updates
 - Endpoint protection strategies
- 5 ☐ Cryptography & Data Protection
 - Basics of encryption
 - Symmetric vs asymmetric encryption
 - Hashing and digital certificates
 - Protecting data in transit and at rest
- 6 ☐ Cyber security Operations
 - Incident response basics
 - Security policies and procedures
 - Risk management concepts
 - Security monitoring and analysis
- 7 ☐ Ethics, Laws & Cyber security Careers
 - Ethical behavior in cyber security

- Cyber laws and regulations
- Cyber security job roles and pathways
- Preparing for a career in cyber security

Course Outcomes

By the end of this course, learners will be able to:

- Understand core cyber security concepts and terminology
- Identify common cyber threats and attack methods
- Apply basic network and system security principles
- Explain how encryption protects data
- Recognize cyber security career paths and required skills
- Build a strong foundation for advanced cyber security certifications