

Cyber Security Foundation - CSFPC

Duration: 16 hours

Module 0: Cybersecurity for Small Businesses

- Why cybersecurity matters for individuals and small organizations
- Common cyber risks faced by small entities
- Simple steps to improve digital safety on a budget

Module 1: Cybersecurity Fundamentals

- Core principles: Confidentiality, Integrity, Availability (CIA triad)
- Types of cybersecurity: Network, Information, Physical, Endpoint
- Introduction to threats, vulnerabilities, and controls

Module 2: Risk Management

- Basics of identifying and assessing risks
- Common threats and their impacts
- Risk mitigation approaches (qualitative methods)
- Creating a basic risk register (manual/spreadsheet-based)

Module 3: Law / Regulation

- General understanding of cybersecurity-related laws
- Key concepts: data protection, breach, consent, data subject
- Importance of compliance in a digital environment

Module 4: Human Factors

- Why people are a key part of security
- Social engineering: types and warning signs
- Tips to build personal and team-level cyber awareness

Module 5: Privacy & Online Rights

- Importance of protecting personal information
- Concepts: digital footprint, cookies, device tracking
- Practical privacy tips for individuals and small teams

Module 6: Malware & Attack Technologies

- Common types of malware: viruses, worms, ransomware, etc.
- Basic attack methods like phishing and spoofing

- How to recognize and avoid infection attempts
- Preventive measures using free tools and settings

Module 7: Adversarial Behavior

- What motivates cyber attackers
- Overview of basic attack lifecycle (scanning to exploitation)
- How attackers commonly exploit human and technical gaps

Module 8: Security Operations & Incident Management

- Introduction to monitoring and managing security
- Steps to take during and after a cyber incident
- Importance of backups and basic recovery planning
- Creating a simple incident response checklist