Unit R050: IT in the digital world. Topic Area 4: Cyber security & Legislation

4.1 Threats
Denial of service (DOS)
Hacking including
- **Black hat**
- **Grey hat**
- **White hat**

Types of Malware:
- Adware
- Botnet
- Ransomware
- Spyware
- Trojan horse
- Virus
- Worm

Types of Social engineering
- Baiting
- Phishing
- Pretexting
- Quid pro Quo
- Scareware
- Shoulder surfing

4.2 The impacts of a cyber-security attack on individuals and/or organisations:
Data destruction
Data manipulation
Data modification
Data theft – in transit and at rest Denial of Service (DoS) to authorised others
Identity theft

4.3 Prevention measures:
Physical
Biometric devices
- Firewalls
- Keypads
- Radio-frequency identification (RFID)
- Secure backups

Logical
- Access rights and permissions
- Anti-virus / malware software Two-Factor Authentication (2FA) Encryption
- Firewalls
- Secure backups
- Usernames & passwords

Secure Destruction of data
- Data erasure
- Data sanitation Magnetic wipe Physical destruction

4.4 Legislation related to the use of IT systems
- Computer Misuse Act
- Copyright, Designs and Patents Act Data Protection Act
- Freedom of Information Act
- Health & Safety at Work Act

Keywords:
Botnet: a group of infected computers controlled remotely by a hacker to carry out malicious tasks
Adware: software that displays unwanted ads on your device **Ransomware:** encrypts or locks your files until you pay a ransom to the attacker to regain access to them.
Spyware: software that tracks and gathers information without your knowledge.
Trojan horse: malware that disguises as a legitimate program.
Virus: malware that attaches to other programs and replicates itself.
Worm: malware that replicates and spreads across networks.
Baiting: tricking people by offering something in exchange for sensitive information or money.
Phishing: tricking people by pretending to be a trustworthy source.
Pretexting: tricking people by assuming a false identity.
Quid pro Quo: tricking people by offering something in return for sensitive information or money.
Scareware: tricking people by scaring them with false information.
Shoulder surfing: tricking people by observing them while they enter sensitive information.