

Course Objectives

This Security Essentials course is for anyone who needs to understand the concepts relating to the secure use of IT in daily life and the skills to maintain a safe and secure environment. It's suitable for complete beginners.

By the end of this course you will be able to understand the importance of connecting to a network securely, online security and how to back up your data and information.

Estimated Course duration is 2 - 3 hours. Each lesson takes on average 3-5 minutes to complete.

Security Concepts

- Security Terms
- Data Threats
- Reason for Data Protection
- Data Protection Principles
- Social Engineering
- Identity Theft
- File Security
- Encryption

Malware

- Malware Types
- Malware Methods
- Understanding Anti-Virus Software
- Updating and Scanning
- Dealing with Infected and Suspicious Files

Network Security

- Network Security
- Firewalls
- Wireless Security
- Personal Hotspots

Access Control

- Preventing Unauthorised Data Access
- Access Control
- Password Management

Secure Web Use

- Autocomplete Settings
- Deleting Browsing Data
- Secure Browsing
- Pharming
- Content Control

Communications

- Social Networking Risks
- Email Encryption
- Digital Signatures
- Fraudulent Emails
- Phishing
- Email Attachment Risks
- Using Social Networking
- VoIP and Instant Messaging
- Using Mobile Apps
- Mobile Security
- Device Security
- Backup Procedures
- Data Storage
- Data Deletion
- Permanent Data Disposal

Security Essentials Test (included in this package)

This test covers questions across Security Concepts, Malware, Network Security, Access Control, Secure Web Use, Communications and Secure Data Management. It has 20 randomly asked questions from a pool of 80. Questions are either true/false, multiple choice, hotspot, fill in the blank or match.

The pass mark is 80% and you will receive a certificate upon passing. You can re-take the test.