



SECURITY OF ICT SYSTEMS AND DATA

2 day course: 9.30am – 5pm

This course covers the skills and knowledge needed to identify and prevent security risks to ICT systems and data. Delegates will learn simple methods to protect software, personal and company data, identify and manage risks from unauthorised use, and protect against viruses and hacking.

UNWANTED MESSAGES

- What is spam?
- Protecting against spam

MALICIOUS PROGRAMS

- Computer viruses
- Malware
- Spyware
- Worms
- Logic bombs
- Trojans
- Adware
- Rogue diallers
- Protecting against malicious programs

INFILTRATION

- What is a hacker?
- How do hackers attack?

HOAXES

- Hoaxes
- How to spot a hoax message

PHYSICAL SECURITY

- Backup
- Unauthorised use
- Access control devices (eg locks, biometric controls, CCTV)
- Data visibility
- Shielding
- Access records and authorization

ORGANISATIONAL SECURITY PROCEDURES

- Security audits
- Company policies

IDENTITY/AUTHENTICATION

- Risks of unauthorised access
- User IDs and passwords

LOGGING OFF

- Logging off or locking your computer

IDENTITY THEFT

- What is Phishing?
- Understanding and avoiding identity theft
- Avoiding inappropriate disclosure of information

SOFTWARE SECURITY SETTINGS

- Internet Explorer and Outlook security settings
- Cookies
- Downloading files
- Plan and implement software updates.

CRYPTOGRAPHY

- Hashing
- Symmetric
- Asymmetric
- Public Key Infrastructure
- Key management and Certificates

PROTECTION

- Types of Firewalls
- Configure a Firewall
- Implementing security for wireless networks
- Anti-virus software installation and updates



ASSUMED KNOWLEDGE:

Delegates attending this course should have knowledge of supporting PCs, Windows and applications software in the work place.

THIS COURSE PREPARES YOU FOR:

- *ICT PROFESSIONAL COMPETENCE (PROCOM) DIPLOMA: SECURITY OF ICT SYSTEMS (LEVEL 3)*
- *CERTIFICATE IN ICT SYSTEMS AND PRINCIPLES: PRINCIPLES OF ICT SYSTEM AND DATA SECURITY (LEVEL 3)*