

5 Days

CompTIA IT Fundamentals

The CompTIA IT Fundamentals Certification is an entry-level course for an individual who wants to gain understanding about the world of Information Technology. From networking to cyber security, from hardware to software basics, this course provides a broad horizon of all the terminologies and technicalities of IT.

This course sets foundations of higher courses of CompTIA such as A+, Network+, Security+ etc., as it equips the individual with all fundamentals of IT.

This course will prepare the candidates to conduct FCO-U51 that will qualify them for IT Fundamentals Certification.

Course Details

Course Outline

1.0 Software

1.1 Compare and contrast common Operating Systems and their functions and features

- Software compatibility for different OS types and versions
- Awareness of hardware compatibility for OS support
- Basic functions of an operating system

1.2 Identify common programs, applications and their purpose

- Productivity Software, Collaboration Software, Utility Software, Specialized Software
- Common file types

1.3 Given a scenario, use software management best practices

- Patching/updates for OS, drivers, applications and security software
- Software version identification and compatibility
- Licensing

1.4 Identify the following alternative technologies and their purpose

- Virtualization
- Cloud Computing
- Web applications
- VoIP
- Telepresence
- Gesture-based interaction

1.5 Explain the basic software features and functions of wireless devices

- Unlocking/security
- Bluetooth pairing
- Wireless connection setup
- Email configuration
- Screen orientation
- Airplane mode

2.0 Hardware

2.1 Identify basic wired and wireless peripherals and their purpose

- Output devices
- Input devices
- Input & Output devices

2.2 Compare and contrast common computer connector types

- Video
- FireWire
- eSATA
- Thunderbolt
- USB
- PS/2
- Parallel
- Serial
- RJ-45 & RJ-11
- Audio
- Power

2.3 Identify the purpose of internal computer components

- CPU
- Power Supply
- RAM
- Storage
- Expansion cards
- Motherboard/mainboard
- System cooling

3.0 Security

3.1 Define basic security threats

- Malware
- Phishing
- Social engineering
- Spam
- Password cracking
- Physical security

3.2 Given a scenario, use security best practices

- Password management
- Device hardening
- Open Wi-Fi vs. secure Wi-Fi
- Multifactor authentication
- Suspicious emails
- Act on security software alerts
- Admin vs. user vs. guest account

3.3 Given a scenario, use web-browsing best practices

- Recognize a secure connection/website
- Recognize invalid certificate warnings
- Recognize suspicious links
- Recognize suspicious banner ads
- Recognize adware symptoms
- Limit the use of personal information (PII)
- Update browsers and plugins
- Disable unneeded/suspicious browser plugins, toolbars, and extensions
- Disable autofill forms/passwords
- Clear browser cache/history/cookies
- Recognize untrusted source warnings
- Risks of using public workstations

4.0 Networking

4.1 Given a scenario, set up and configure a basic SOHO router (wired / wireless)

- Verify wired connection, if applicable
- Set WEP vs. WPA vs. WPA2
- Change SSID from default
- Apply a new wireless password
- Change admin password for router
- Connect to the new network
- Verify internet connectivity
- Update firmware if necessary

4.2 Compare and contrast cellular, wireless and wired data connections

- Levels of security
- High vs. low mobility
- High vs. low availability
- High vs. low reliability
- High vs. low throughput/bandwidth

4.3 Compare and contrast different methods of sharing and storage

- HTTP vs. HTTPS
- FTP vs. FTPS vs. SFTP (Secure File Transfer Protocol)
- Local vs. hosted storage
- Peer-to-peer
- Network vs. local printing

5.0 Basic IT literacy

5.1 Perform appropriate steps to set up a basic workstation

- Plug in cables
- Power on computer
- Follow initial operating system setup wizard
- Install security software
- Configure peripherals (if applicable)
- Uninstall unneeded software (if applicable)
- Configure and verify internet connection
- Install additional software (if applicable)
- Run software and security updates
- Other user accounts (if applicable)
- Basic cable management

5.2 Explain the basic methods of navigating an operating system

- Executing programs
- Difference between shortcuts and files
- Manipulating files
- Read-only vs. modifiable files
- Navigate a file structure
- Search, sort and display files
- Create screen captures
- Navigate with hotkeys
- Folder and file size
- Accessibility options
- Folder and file permissions

5.3 Given a scenario, implement basic support concepts

- Check for external issues
- Manufacturer documentation
- Manufacturer websites
- Technical community groups
- Internet search engine
- Contact technical support

5.4 Explain basic backup concepts

- Importance of backups
- Scheduling
- Frequency
- Storage mediums
- Backup verification and testing

5.5 Describe the importance and impact of various environmental and safety concepts

- Proper disposal methods
- Power
- Device placement
- Electrostatic discharge concepts
- Ergonomic concepts
- Follow manufacturer safety guidelines

Pre Requisite

No prior experience necessary

Exams

CompTIA IT Fundamentals [FC0-U51 (proctored), FC0-Z51 (no)]

464, Udyog Vihar Phase
V, Gurgaon (Delhi
NCR)-122016, India

+91 8882 233 777

training@mercury.co.in

www.mercurysolutions.co

Date - Apr 20, 2024