CompTIA A+ (220-1102) Training (18 Hours)

Course Description

This online instructor led training course provides the knowledge necessary to support basic computer hardware and operating systems in today's business world.

In this course students will learn best practices in troubleshooting, networking and security across a variety of device types in order to support their organization and set the stage for their own IT careers. This course will boost students' confidence to handle the most challenging technology problems more efficiently and will help build customer service and communication skills.

StormWind's two part CompTIA A+ course covers the hardware and software objectives students must master in order to pass the 220-1101 exam and the 220-1102 exam, both of which are required to achieve the CompTIA A+ Certification. The A+ Certification is part of specialized certification tracks for corporations such as Microsoft, Hewlett-Packard, and Cisco. Many technology companies have made CompTIA A+ certification mandatory for their service technicians.

Skills Learned

After completing this online training course, students will be able to:
- Identify basic features of Microsoft Windows editions
- Use the appropriate Microsoft command-line tool
- Use features and tools of the Microsoft Windows 10 operating system (OS)
- Configure Microsoft Windows networking features on a client/desktop
- Identify common features and tools of the macOS/desktop OS
- Summarize various security measures and their purposes
- Explain common social-engineering attacks, threats, and vulnerabilities
- Use best practice procedures for malware removal
- Explain basic change-management best practices
- Implement workstation backup and recovery methods
- Use remote access technologies

Audience Profile

This course is appropriate for computer technicians, IT support staff, and help desk professionals with 6 to 12 months of hands-on experience. It will also help prepare professionals seeking CompTIA A+ certification (220-1101/220-1102).

Prerequisites

- Basic end-user skills with Windows-based PCs
- Basic knowledge of computing concepts

Operating Systems

Microsoft Windows Editions
Microsoft command-line tool
Microsoft Windows 10 features and tools
Microsoft Windows 10 Control Panel utility
Windows settings
Microsoft Windows networking features
Installation and configuration concepts
Common Operating System (OS) types
OS installation and upgrade
Common features of macOS
Common features of Linux distributions

Security

Security measures
Wireless security
Detecting and removing malware
Social engineering
Basic security settings in Microsoft Windows
Security best practices for workstations
Mobile and embedded device security
Data destruction and disposal
Small office/home office (SOHO) security
Internet browser security

Software Troubleshooting

Troubleshoot Windows OS
Troubleshoot PC security issues
Malware removal
Troubleshoot mobile OS
Troubleshoot mobile OS security

Operational Procedures

Documentation and support system information management best practices
Change management best practices
Workstation backup and recovery
Common safety procedures
Environmental
Prohibited content, privacy, and licensing
Proper communication and professionalism
Basics of scripting
Remote access technologies