1001-02: CompTIA A+ Certification, Part 11 of 13: Security

Meet the expert: A lifelong fascination with technology led a varied career in technology. I have over 20 years of experience supporting end users, and small businesses. On top of that, I have been an Information Technology instructor for Edmonds Community College, where I instructed on CompTIA’s A+, and Network+ material. During that time I created curriculum for not only those courses, but also for CompTIA’s Security+ certification. I currently hold the following certifications: A+, Network+, Server+, Cloud+, and Project+.

Chuck Nailen has been providing classroom training for more than 16 years. He does training for in department-supported CompTIA curriculums, Microsoft curriculums, and Department of State (DoS) proprietary platforms in support of SAIT and DoS programs. He holds many certifications including National Career Readiness Certificate-Gold Level, MCSA, MCT, MCITP, MCTS, and others.

Prerequisites: This course assumes the user has little to experience with computer hardware or software.

Runtime: 56:55

Course description: In this course for the CompTIA A+ 1001-1002 exam, we'll talk about corporate security policies and filing security incident reports. We'll also cover strong password and other common security policies and how to educate user about them. Also covered are ways to keep workstations secure. Having this information in your arsenal of tools not only will make you a better technician, it can also help with security in your home network.

Course outline:

Security Fundamentals
- Introduction
- Corporate Security Policies
- Security Incident Reports
- Principle of Least Privilege
- Strong Passwords
- User Education
- Common User Security Practices
- Authentication Methods
- Biometric Authen. Methods
- Summary

Threats and Vulnerabilities
- Introduction
- Malware
- Types of Malware
- Social Engineering
- Types of Social Engineering
- Threats & Vulnerabilities
- Common Wireless Sec. Threats
- Summary

Security Protection Measures
- Introduction
- Physical Security
- Physical Security Measures
- Digital Security
- Antivirus Software
- Anti-Spyware Software
- Firewalls
- Social Engineering Prevention
- Hard Drive Sanitation
- Hard Drive Disposal
- Physical Destruction Methods
- Windows Security Policies Introduction
- Domains
- Organizational Units
- Group Policies
- Other AD Features
- Summary

Workstation Secuity
- Introduction
- Windows Security Policies
- Windows Firewall
- Software Firewall Conf Setting
- Workstation Security Best Practices
- Summary