CompTIA A+ Cert, Part 07 of 13: Security [Deprecated/Replaced]

Meet the expert: 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. The user should have viewed the "CompTIA A+ Certification: SOHO, Mobile & Printers" course before starting on this course.

Runtime: 49:07

Course description: In this course 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:

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 for Disposal
• Physical Destruction Methods
• Summary

Workstation
• Introduction
• Windows Security Policies
• Windows Firewall
• Software Firewall Conf Setting
• Workstation Sec. Best Practice
• Summary