220-1101-02: CompTIA A+ Certification: Part 7 of 9: Security Threats

Meet the expert: Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

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

Runtime: 02:32:24

Course description: In this course for the CompTIA A+ 1101-1102 exam, we will cover how to understand security threats as well as how to secure workstations, mobile devices and networks.

Course outline:

Understanding Threats to Security
- Introduction
- Understanding Threats to Security
- User Threats
- Social Engineering
- Phishing
- Network Threats
- Password Attacks
- Vulnerabilities
- Malicious Code Attacks
- Malware Types
- Physical Threats
- Summary

Understanding Common Prevention Methods
- Introduction
- Understanding Common Prevention Methods
- Physical Access Restrictions
- Physical Security
- Anti-Malware
- Demo: Anti-Malware
- Anti Spyware
- Best Practices
- Firewalls
- Hardware Firewalls
- Firewall Functionality
- Proxy Firewalls
- Stateful Packet Inspection
- Host Based Firewalls
- Windows Firewall with Advanced Security
- Demo: Windows Defender
- User Authentication
- Password Best Practices
- Demo: Password Check
- Multifactor Authentication
- Virtual Private Networks
- Data Loss Prevention
- System Hardening
- Trusted Software
- User Education
- Demo: Data Loss Prevention
- Summary

Securing Workstations
- Introduction
- Securing Workstations
- Least Privilege
- Password Best Practices
- Account Management
- Disabling Autorun
- Data Encryption
- Demo: Bitlocker and EFS
- Patch Management
- Summary

Securing Mobile Devices
- Introduction
- Securing Mobile Devices
- Screen Locks
- Finding Mobile Devices
- Backup Mobile Devices
- Login Restrictions
- Antimalware and Updates
- Encryption and Biometrics
- Policies and Procedures
- Best Practices
- Summary

Data Destruction and Disposal Methods
- Introduction
- Destruction and Disposal
- Physical Destruction
- Drilling
- Additional Physical Methods
- Recycling or Repurposing
- Repurposing Options
- Summary

Security for SOHO and Wireless Networks
- Introduction
- SOHO Networks
- Wireless Security Options
- Device Configuration
- Confiure IP and MAC Filters
- Configure SOHO Firewalls
- Security for SOHO and Wireless
- Demo: Security Configuration on Router
- Summary