Chapter 26

Maintaining and Securing Mobile Devices

Episode 26.01

Episode title: **Maintaining Mobile Devices**

3.3 Given a scenario, troubleshoot common mobile OS and application security issues

Objective:
- Security concerns
  - Developer mode
  - Unauthorized/malicious application
    - App spoofing

L3s

- 0:32 - Objective term- Code division multiple access (CDMA) phones
- 0:38 - Objective term - Global System for Mobile Communications (GSM)
- 1:27 - Firmware
- 1:44 - Baseband updates
- 1:50 - Broadband updates and radio firmware updates
- 2:10 - Objective term - Preferred Roaming List (PRL)

L3s

- 2:42 - Product Release Information (PRI)
- 4:05 - International Mobile Subscriber Identity (IMSI)
- 4:14 - International Mobile Equipment Identity (IMEI)
- 6:04 - Objective term - Virtual private network (VPN)
- 7:02 - 1. Give it a name
- 7:02 - 2. Set up VPN
- 7:02 - 3. Know the server IP address
- 7:21 - Objective term - Remote backups/syncing data

L3s

- 7:54 - Objective term - Antivirus/Anti-malware
- 9:12 - Objective term - Android Package Kit (APK) are for Android files
- 9:27 - Objective term - Android phones can be configured with root access for more (possibly unsafe) options. Similarly, you can jailbreak iPhones.
- 9:39 - Objective term - Trusted sources from the store are safer. Untrusted sources can introduce malicious applications or malware.
- 9:47 - Objective term - Firewalls

L3s

- Developer mode (macOS)
- Developer options (Android)
- App Spoofing

Troubleshooting Security Issues

Verifying the operating system

- Apps are current
  - Updates
  - Patches
  - Fixes

Security elements

- Same features as other computing devices
  - Malware threats
  - Unauthorized access
  - Theft
  - Possibility of a lost device

Unauthorized or Malicious Apps
Downloaded from an untrusted source

- Threats
  - Sensitive information
  - Data breach
  - Theft
- Issues
  - Slow performance
  - Increased data usage
  - Frequent pop-up ads
  - Request for personal information
  - Unexpected apps running

Keep issues or change to identifiers or symptoms(etc.)?

Episode 26.03

Episode title: **Mobile Synchronization**

Objective: 1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.

•Mobile device synchronization

    o Recognizing data caps

L3s

- 0:15 - Objective term - Synchronization
- 0:43 - Objective term - Contacts
- 0:57 - Synchronization vs. backups
- 1:28 - 1. Synchronize to the desktop
- 1:59 - iTunes
- 2:21 - 2. Synchronize to an automobile
- 2:54 - 3. Synchronize to the cloud

L3s

- 3:25 - Objective term - Types of data to synchronize
- 4:10 - Bookmarks
- 5:03 - Location data
- 5:26 - eBooks
- 5:54 - Social media data
- 6:31 - Hootsuite
- 6:52 - Applications
- 7:10 - Software requirements to install
- Data cap

Data Cap

Represents a limit on data
- Amounts
  - Transferred
  - Stored
  - In a synchronized location
- Over a period
  - Downloads
  - Uploads
  - Synchronized
  - Back ups
  - Typically takes a month

Keep issues or change to identifiers or symptoms(etc.)?

Episode 26.04

Episode title: **Mobile Device Security**

Objective: 2.8 Given a scenario, apply common methods for securing mobile devices

L3s

- 0:49 - Objective term - Screen lock
- 1:27 - Objective term - Screen lock options can include facial recognition, PIN codes, fingerprints, patterns, or swipe
- 1:58 - Objective term - Face recognition
- 2:16 - Objective term - Multifactor authentication (MFA)/Two-factor authentication (2FA)

L3s

- 2:34 - Objective term - MFA can include requiring a voice call or code verification via SMS text
- 3:07 - Objective term - Failed login attempt restrictions
- 3:22 - Objective term - Some failed login security settings will remotely erase/wipe your device
- 3:34 - Objective term - Authenticator apps
- 4:43 - Objective term - Locator apps
- 5:36 - Device lockout

L3s

- 5:51 - Objective term - Erase/remote wipe device
- 6:12 - Objective term - Mobile device management (MDM)
- 6:25 - Objective term - Bring Your Own Device (BYOD)
- Hardening
- Hardening configuration profile
- Endpoint security
- Mobile device management

<u>Hardening</u>

Eliminates vulnerabilities and reduces threat exposure

- Create a hardened device
  - Avoid granting apps root access
  - Use a secure browser for personal actions
  - Use encryption
  - Set up a secure lock screen
  - Backup to the cloud

Episode 26.05

Episode title: **Mobile Security Troubleshooting**

Objective: 2.1 Summarize various security measures and their purposes

L3s

- 0:50 - Signal drop/weak signal/connectivity issues
- 1:46 - Objective term - Power drain, slower data speeds, high resource utilization
- 2:05 - Objective term - Run antimalware
- 2:27 - Change your passwords if you think you've been hacked

L3s

- 2:43 - Objective term - Unintended Wi-Fi/Bluetooth connection
- 4:19 - Leaked personal files/data
- 4:31 - Unauthorized account access
- 4:40 - Objective term - Unauthorized location tracking
- 4:46 - Unauthorized camera/microphone activation
- Security Assertion Markup Language (SAM-L)
- Single sign-on (SSO)
- Just in time (JIT) access
- Privileged Access Management (PAM)
- Identity and Access Management (IAM)
- Data Loss Prevention (DLP)

Episode 26.06

Episode title: **Mobile Device Troubleshooting**

Objective: 5.4 Given a scenario, troubleshoot common mobile device issues

3.2 Given a scenario, troubleshoot common mobile OS and application issues

L3s

- 0:30 - Objective term - Inaccurate/non-responsive touchscreen or digitizer
- 1:06 - Objective term - Try to calibrate the touch sensors
- 1:22 - Dim display
- 2:17 - Cannot display to external monitor
- 2:58 - No sound from speakers

L3s

- 3:25 - Intermittent/no wireless connectivity
- 4:33 - Objective term - No Bluetooth connectivity
- 5:09 - Objective term - Apps fail to launch/update, log errors, crashing
- 6:03 - Slow performance/slow to respond
- 6:22 - Extremely short battery life
- 6:55 - Objective term - Overheating

L3s

- 7:19 - Objective term - (Overcharging overheating can lead to swollen batteries that can explode...watch out!)
- 7:43 - Frozen system
- 8:35 - System lockout
- Swollen battery
- 3:38 - Digitizer issues