

Chapter 25

Maintaining and Securing Mobile Devices

Episode: **Maintaining Mobile Devices**

Objective(s):

Core 1: 1.4 Given a scenario, configure basic mobile-device network connectivity and application support.

Core 2: 2.7 Explain common methods for securing mobile and embedded devices.

Core 2: 3.5 Given a scenario, troubleshoot common mobile OS and application security issues.

Episode Description

A+

Mobile devices are surprisingly self-maintaining these days, but there are a few issues that come up occasionally. A big part of this is understanding the names and functions of certain settings unique to smartphones.

CompTIA

Key Terms

A+

- 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)

CompTIA

Key Terms

A+

- 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 2. Set up VPN3. Know the server IP address
- 7:21 - Objective term - Remote backups/syncing data

CompTIA

Key Terms

A+

- 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

CompTIA

Quick Review

- CDMA phones do not use SIM cards; GSM phones use SIM cards
- IMSI defines critical SIM information, IMEI defines the phone itself
- All mobile OSes have built-in VPN and backup software
- Anti-malware is common for Android, less so for IOS

Episode: **Mobile Devices and E-mail**

Objective(s):

Core 1: 1.4 Given a scenario, configure basic mobile-device network connectivity and application support.
Core 1: 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
Core 1: 2.4 Summarize services provided by networked hosts.
Core 2: 2.1 Summarize various security measures and their purposes.
Core 2: 2.7 Explain common methods for securing mobile and embedded devices.

Episode Description

A+

Corporate or ISP e-mail setup requires various configuration options, such as POP or IMAP for incoming mail and SMTP for outgoing mail. S/MIME was a way to encrypt e-mail attachments. Standard Google or Apple accounts set up with a simple username and password. This episode explores these options.

CompTIA

Key Terms

A+

- 0:33 - Two different protocols for incoming email: POP3 or IMAP
- 0:40 - Outgoing protocol: SMTP
- 1:01 - Objective term - Corporate email configuration
- 2:20 - Objective term - 1. FQDN of SMTP mail server
- 2:30 - 2. Username & password

CompTIA

Key Terms

A+

- 2:35 - Objective term - 3. Port number for SMTP (usually port 25)
- 2:44 - 4. FQDN for IMAP mail server
- 2:56 - 5. Username & password
- 3:00 - Objective term - 6. Port Number for IMAP (usually port 143)
- 4:35 - SSL STARTTLS
- 4:39 - SMTP encrypted port: 465 or 587
- 4:46 - IMAP encrypted port: 993

CompTIA

Key Terms

A+

- 4:49 - Objective term - POP3 encrypted port: 995
- 4:53 - Point-to-point encryption (P2PE)
- 5:44 - Secure/Multipurpose Internet Mail Extensions (S/MIME)
- 6:14 - ASCII code
- 7:17 - ProtonMail
- 8:11 - Objective term - Mobile account setup (Example: Google, Yahoo, iCloud, Microsoft 365 etc.)

CompTIA

Quick Review

- E-mail setup on smartphones always means adding an email account
- Traditional emails require SMTP and an IMAP/POP mail server address and account passwords
- Most traditional e-mail servers use encrypted port numbers
- Mobile cloud account setup is as easy as typing in your username and password

Episode: **Mobile Device Security**

Objective(s):

Core 1: 1.4 Given a scenario, configure basic mobile-device network connectivity and application support.

Core 2: 2.1 Summarize various security measures and their purposes.

Core 2: 2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Core 2: 2.7 Explain common methods for securing mobile and embedded devices.

Episode Description

A+

Mobile device security starts with a lock screen but goes beyond with multifactor authentication (MFA) and remote find, lock, and wipe. Corporate environments use mobile device management (MDM) services for even more control over mobile devices.

CompTIA

Key Terms

A+

- 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)

CompTIA

Key Terms

A+

- 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

CompTIA

Key Terms

A+

- 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)

CompTIA

Key Terms

A+

- 6:37 - Objective term - Corporate-Owned Personally-Enabled (COPE)
- 7:14 - Objective term - Corporate devices can also control applications with mobile application management (MAM)

CompTIA

Quick Review

- Screen locks prevent others from accessing your phone using facial recognition, PIN codes, fingerprints, patterns, or swipe
- Multifactor authentication (MFA) means using more than one way to authenticate
- Authenticator apps add an extra layer of security
- Location apps like Find My Phone help locate lost devices

Episode: **Mobile Device Troubleshooting**

Objective(s):

Core 1: 5.5 Given a scenario, troubleshoot common issues with mobile devices.

Core 2: 3.4 Given a scenario, troubleshoot common mobile OS and application issues.

Episode Description

A+

Mobile devices can encounter problems ranging from unresponsive touchscreens to complete system lockout. This episode explores common symptoms, such as slow performance (caused by excessive apps running) or overheating, and their solutions.

CompTIA

Key Terms

A+

- 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

CompTIA

Key Terms

A+

- 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

CompTIA

Key Terms

A+

- 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

CompTIA

Quick Review

- Take time to memorize the many troubleshooting scenarios described in the episode
- Keep in mind that many troubleshooting scenarios are simple misconfiguration
- Practice these scenarios on both Android and iOS if possible