CompTIA A+ Core 2 Exam 220-1102

Lesson 18

Supporting Mobile Software

Objectives

- Configure mobile OS security
- Troubleshoot mobile OS and app software
- Troubleshoot mobile OS and app security

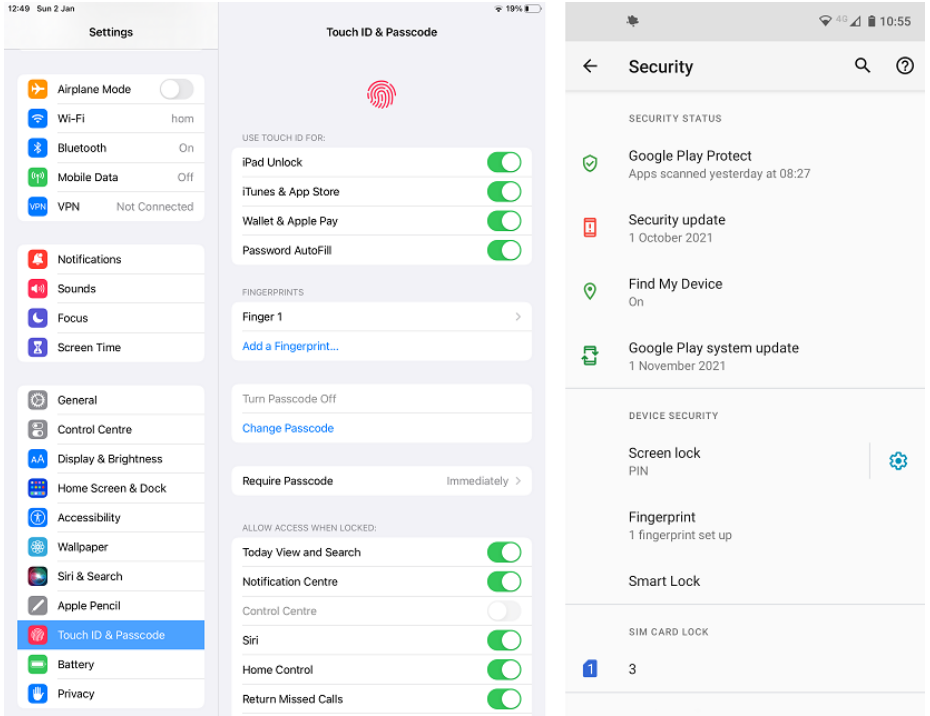
Lesson 18

Topic 18A

Configure Mobile OS Security

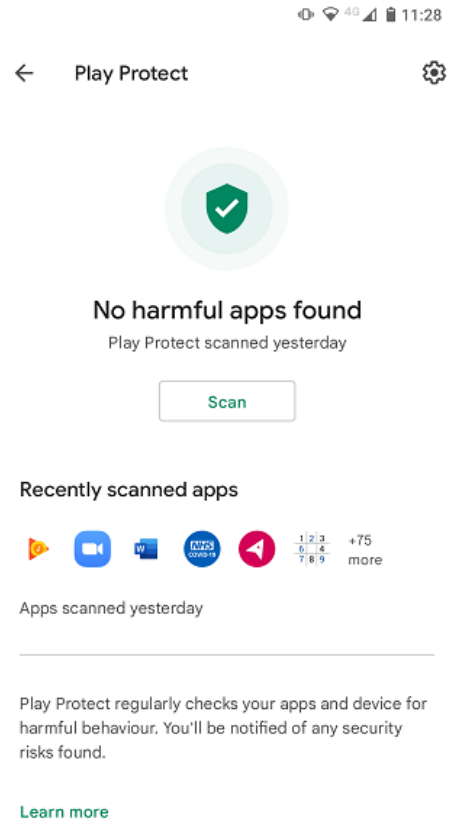
Screen Locks

- Screen lock with swipe
  - No authentication required to unlock
- Secure screen lock
  - Personal identification number (PIN) or password
  - Fingerprint
  - Facial recognition
  - Pattern
- Failed login attempts lockout



Screenshots reprinted with permission from Apple Inc. and Android platform, a trademark of Google LLC.

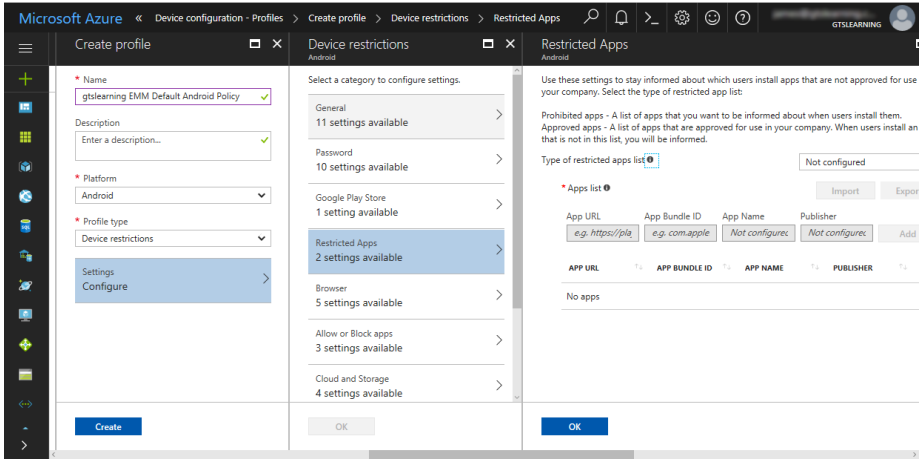
Mobile Security Software



Screenshot courtesy of Google Play Store, a trademark of Google LLC.

- Patching/OS updates
  - iOS versus Android and vendor support
- Antivirus/anti-malware apps
  - Additional layer of protection to marketplace security
  - Monitor app behavior and permissions requests
- Firewall apps
  - Filter outgoing connections
  - VPN-based filtering

Enterprise Mobility Management

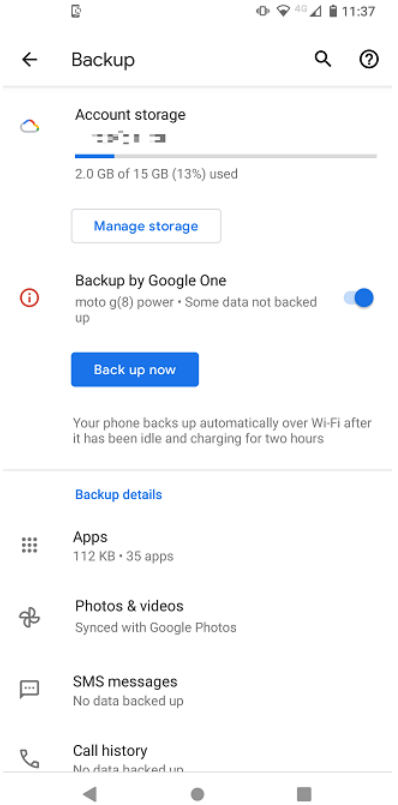


Screenshot courtesy of Microsoft

- Mobile deployment models
  - Bring your own device (BYOD)
  - Corporate owned
- Mobile device management (MDM)
  - Enrollment
  - App/feature control
  - Profile of security requirements

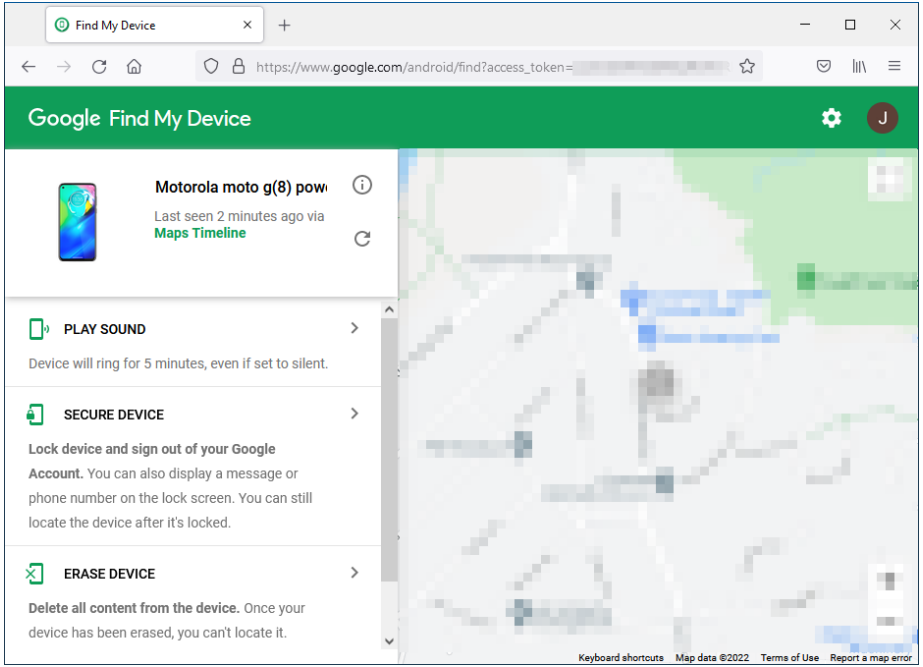
Mobile Data Security

- Device encryption
  - iOS versus Android
- Remote backup applications
  - Back up to cloud service
  - Back up to PC



Screenshot courtesy of Google One™ subscription service of Google LLC.

Locator Apps and Remote Wipe

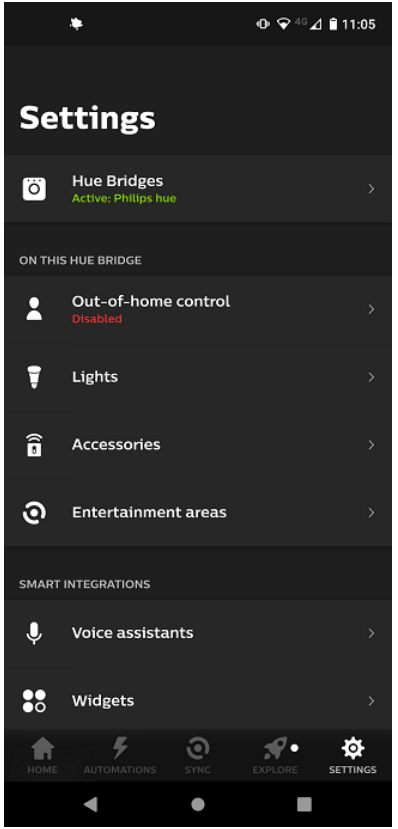


Screenshot courtesy of Google, a trademark of Google LLC.)

- Locator apps
  - Map location of device
  - Display “Please return” or activate ringer
  - Prevent location/network features from being disabled
- Remote wipe
  - Device wipe/factory default reset
  - Enterprise wipe

Internet of Things Security

- Home automation systems
  - Smart hubs and speaker control
    - Smartphone app
  - Smart device type
  - Wireless mesh networking
- Security concerns
  - Inadequate security monitoring/patching
  - Weak defaults
  - Shadow IT use within enterprise networks



Screenshot used with permission from Koninklijke Philips N.V.

Review Activity: Mobile OS Security

- Screen Locks
- Mobile Security Software
- Enterprise Mobility Management
- Mobile Data Security
- Locator Apps and Remote Wipe
- Internet of Things Security

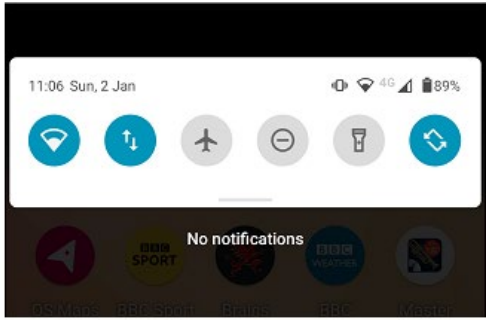
Lesson 18

Topic 18B

Troubleshoot Mobile OS and App Software

Mobile Device Troubleshooting Tools

- Mobile device configuration tools
  - Settings app, Android Notification Shade/iOS Control Center, task list
- Reboot
  - First step in troubleshooting many issues
  - iOS versus Android
- Factory reset
  - Wipes all apps, settings, and user data
  - Last resort step in troubleshooting many issues

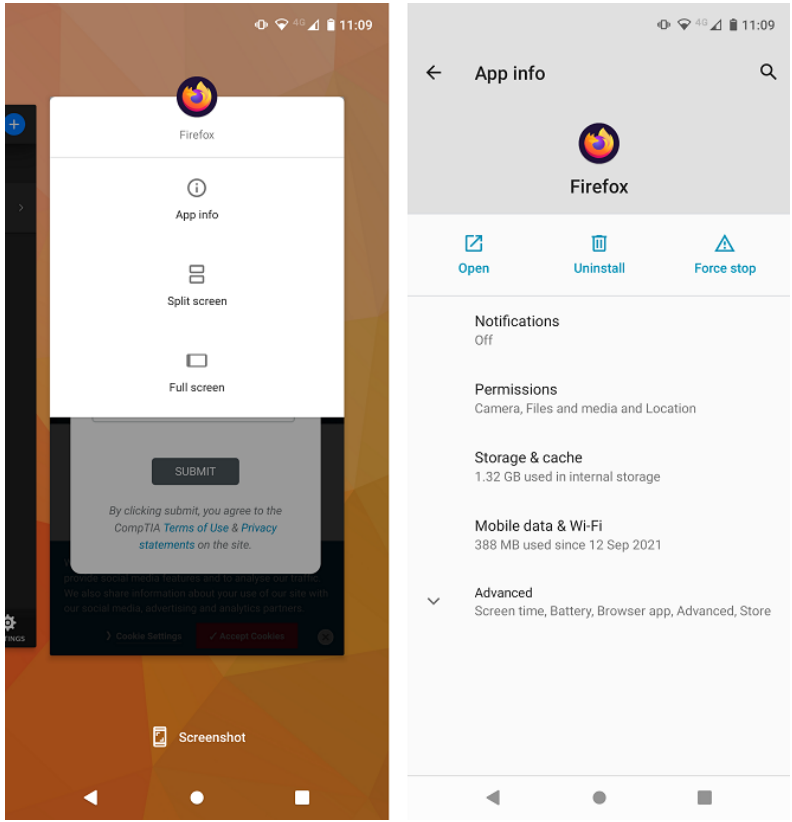


Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

Troubleshoot Device and OS Issues

- OS fails to update
  - Check compatibility, network, power, and storage and try restart
- Device randomly reboots
  - Check for hardware/overheating faults
  - Check if issue persists after reboot/reset and isolate single app as cause
- Device is slow to respond
  - Check if issue persists after reboot/reset and isolate single app as cause
- Screen does not autorotate
  - Check configuration or isolate single app as cause

Troubleshoot App Issues



Screenshot courtesy of Android platform, a trademark of Google LLC.

- Application fails to launch or fails to close/crashes
- Force stop and/or clear cache
- Check for updates
  - Application fails to update
- Uninstall then reinstall
- Mobile device management (MDM) restrictions

Troubleshoot Connectivity Issues

- Signal strength and interference issues
  - Move devices closer together and remove protective case or change hand position
- Configuration issues
  - Airplane mode or feature enable/disable
  - Wi-Fi configuration and Bluetooth pairing
- Troubleshooting near-field communication (NFC)
  - Feature enable/disable or signal strength issue
- Troubleshooting AirDrop issues
  - Enable for contacts or everyone
  - Bluetooth configuration and signal strength

Review Activity: Activity Title

- Mobile Device Troubleshooting Tools
- Troubleshoot Device and OS Issues
- Troubleshoot App Issues
- Troubleshoot Connectivity Issues

Lesson 18

Topic 18C

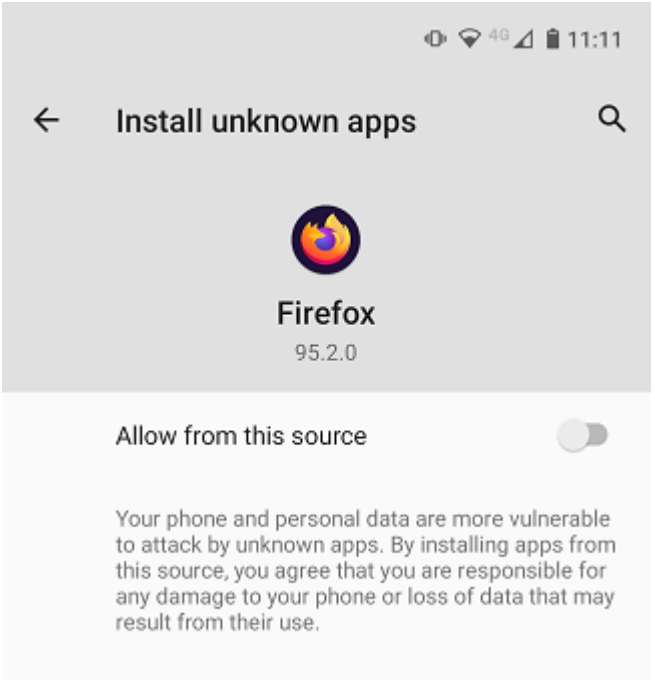
Troubleshoot Mobile OS and App Security

Root Access Security Concerns

- Owner-level permissions
  - Root access for Android devices
  - Jailbreaking iOS devices
- Detecting and blocking on enterprise networks
- Developer mode

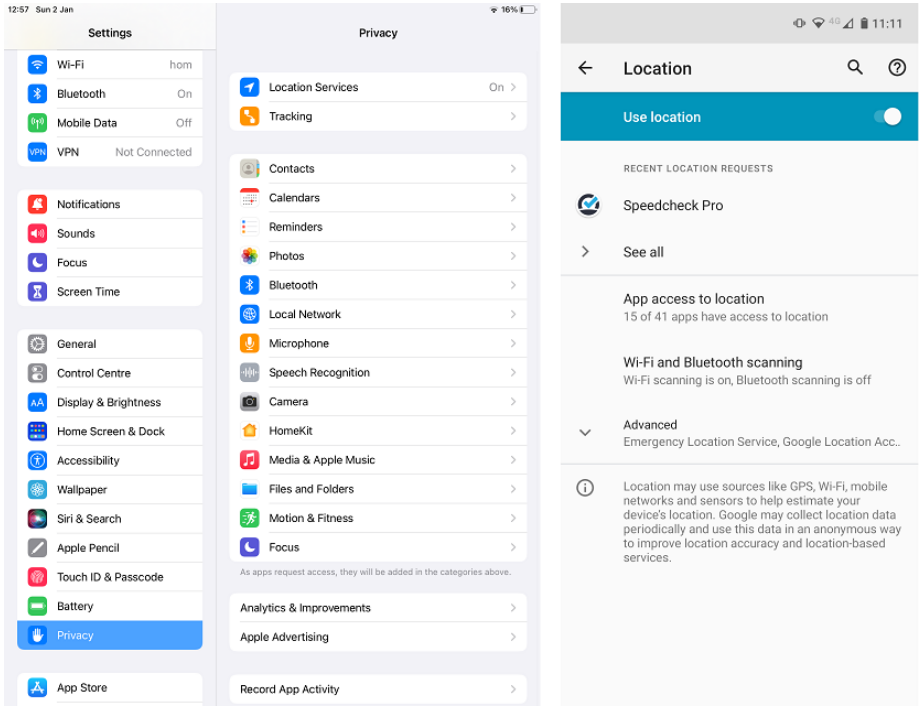
Mobile App Source Security Concerns

- Trusted app sources/stores
- App spoofing
  - Rogue developers placing malicious apps in trusted stores
  - Fake reviews and manipulated download figures
- Enterprise apps and Android package (APK) sideloading
  - Enterprise store distribution
  - Android APK sideloading from untrusted sources
- Bootleg app stores
  - Pirated apps



Screenshot courtesy of Android platform, a trademark of Google LLC and Mozilla

Mobile Security System Symptoms



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

- General symptoms
  - High number of ads, fake security warnings, sluggish response time, limited/no Internet connectivity
- Unexpected application behavior
  - Permissions and device usage
  - High utilization and network traffic
- Leaked personal files/data
  - Breach notification
  - Unauthorized account access
  - Location tracking

Review Activity: Mobile OS and App Security

- Root Access Security Concerns
- Mobile App Source Security Concerns
- Mobile Security Symptoms

CompTIA A+ Core 2 Exam 220-1102

Lesson 18

Summary