CH 9: Supporting and Troubleshooting Mobile Devices

- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Topic A: Secure Mobile Devices

- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

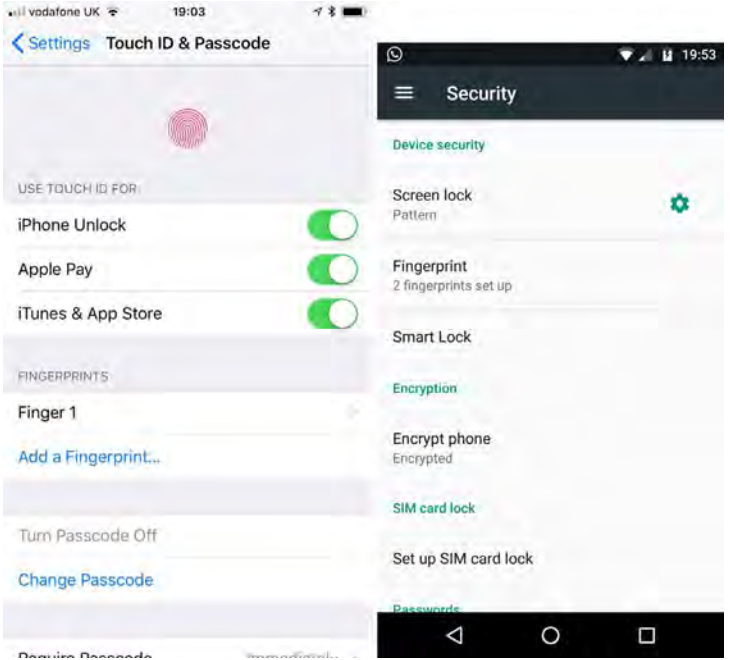
Popular Security Controls for Mobile Devices

- Organizations security practices, including
  - Policies
  - Procedures
  - Training
- Keep these mobile devices secure physical infrastructure.
- Do not leave mobile devices unattended.

Mobile Device Access Control

- Screen locks and biometric authentication
  - Screen locks require:
  - Password, Passcode
  - PIN, or Gestures

  Biometric authentication:
  - Fingerprint
  - Facial recognition
  - Pattern



Mobile Device Access Control

- Lockout policies
  - Limits failed logins.
  - Lockouts can escalate in duration: 10 seconds for 1 lockout; 30 minutes for next.

- Remote wiping
  - Resets a stolen device to factory defaults.
  - All personal data removed.
  - Possibly erase memory cards, too.

Mobile Device Updates

- Security

  Mobile devices can use the same classes of security software as PCs and laptops to protect against malware, phishing, and software exploits.

- Patching/OS updates
  - IOS: Settings > General > Software > Update
  - App Icon Notifications on the app will make you aware of App updates.
  - Android: **Settings > System > Advanced > System updates**
  - Will uses the notification bar to deliver updates.

Mobile Device Antivirus

- Antivirus/anti-malware
  - Anti-malware designed for mobile devices work more like content filters to block access to known phishing sites and block adware/spyware activity by apps.

- Antivirus
  - Additional layer of protection to marketplace security
  - Monitor app behavior and permissions requests
  - Will detect configuration errors
  - Monitor the permissions assigned to apps

Mobile Device Firewalls

- Firewall apps

  Will monitor app activity and prevent connections to ports or IP addresses.

- Firewall apps
  - Filter outgoing connections
  - Require Root level access to control
  - VPN-based filtering (None Root Access)

- Firewall apps
  - Comodo
  - Tiny Wall
  - Net Defender

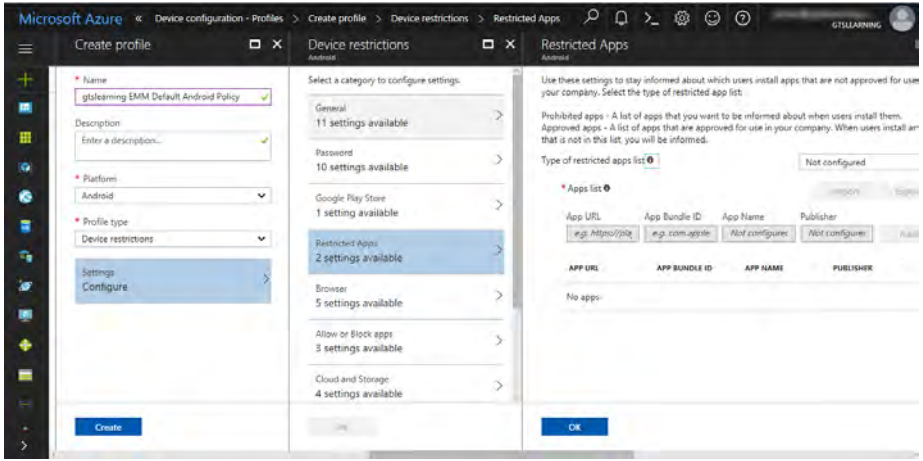
Mobile VPN Configuration

Virtual Private Network (VPN): A secure tunnel created via an unsecure network (typically the Internet).

Mobile VPN: A VPN that can maintain the VPN link across multiple carrier networks.

- Tunnel contents is encrypted to secure communications.
- Links maintained even in sleep mode.
- Available as third-party apps for Android and iOS.

Enterprise Mobility Management



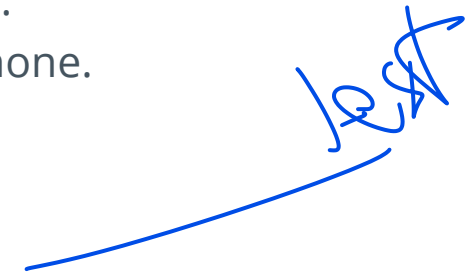
- Mobile device management (MDM)
  - Enrollment
  - App/feature control
  - Profile of security requirements

Mobile MDM

- MDM: (Mobile Device Management)
- Is a class of enterprise software designed to apply security policies to the use of smartphones & Tablets
- Mobile application management (MAM)
  - Authentication policies
  - Control device features (webcam/microphone)
  - Remote device reset/data wipe

Mobile MDM: Encryption

- Device Encryption:
  - iOS, various levels of encryption.
  - Encryption key is stored on the device.
  - OS just deletes the key to Wipe the phone.



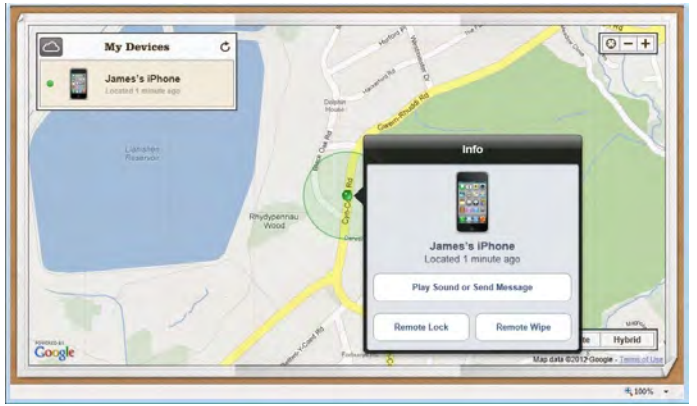
- MDM Types:
  - BYOD- Bring your own device
  - COBO- Corporate owned, business
  - COPE- Corporate owned, personally enabled
  - CYOD- Choose your own device

Mobile MDM: Data Protection

- Email Encryption:
  - Email "Data Protection" option are subject to a second round of encryption using a key derived from the user's credential.

- Data Protection:
  - Not all user data is encrypted by DP
  - Options / Contacts / SMS messages /Pictures
  - On Android -there are substantial differences to encryption options between versions
  - IOS- DP is enabled automatically after passcode lock on the device.

Mobile Device: Locator Apps and Remote Wipe



- GPS apps
  - Requires line of sight to satellites.
  - Geo-tracking related to Location Services.
  - Location Services also supports apps like **Find My Phone**.
  - IPS: (Indoor) uses location detection by triangulating its proximity radio sources, like Wi-Fi or Bluetooth beacons.
  - The Location Service uses GPS and/or IPS to calculate a device's position on a map!

Mobile Device Backup

- Remote backup apps:
  - iCloud, Google Sync or OneDrive
  - Not Included - SMS and call history

- IOS: macOS or Windows via iTunes program.
- More options - MDM
- Android: File explore, Droid Transfer, File Transfer to (Mac)

Multifactor Authentication and Authenticator Applications

- Factors:
  - Something you know
  - Something you are
  - Something you have
  - Somewhere you are
- Multifactor authentication requires two different factors.
- Authenticator apps help implement multifactor authentication.
  - 2-step verification: password/PIN (what you know) and cards (what you have).

IOT Internet of Things Security

- This describe the global network personal devices, home appliances, home control systems, vehicles,
- These items have sensors, software, and network connectivity
- Allowing them to communicate and pass data among themselves and computers

- Mobile application management (MAM)
  - Authentication policies
  - Control device features (webcam/microphone)
  - Remote device reset/data wipe

IOT Internet of Things Security

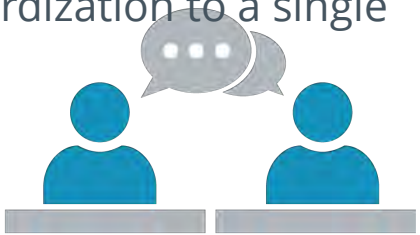
- Security concerns
  - Inadequate security monitoring/patching
  - Weak defaults admin passwords
  - Shadow IT- employees deploy a IOT device without going through management

IOT Internet of Things Security

- Home Automation Systems:
  - Hub/Control system: Talks to Wi-Fi, IOT are (headless) no user control interface, smartphone app or Voice to configure
  - Smart device type: Most devices use a Linux or Android kernel
  - Wireless mesh networking: coms between devices are likely to use mesh networking, such as Z-Wave or Zigbee.

Discussing Mobile Device Security

- **A company wants to minimize the number of devices and mobile OS's to support but allow use of a device by employees or personal email and social networking.**
- **What mobile deployment model is the best fit for these requirements?**
- **ANSWER:**
  - Corporate owned, personally enabled (COPE) will allow standardization to a single



Discussing Mobile Device Security

- **What two types of biometric authentication mechanism are supported on smartphones?**

- **ANSWER:**
  - Fingerprint
  - Facial

Discussing Mobile Device Security

- **True or false? Updates are not necessary for iOS devices because the OS is closed source.**

- **ANSWER:**
  - False— It is still subject to updates to fix problems and introduce new features.

Discussing Mobile Device Security

- **What might a locator application be used for?**

- **ANSWER:**
  - To identify the location of a stolen phone, find one's family member, and to provide localized services (Uber).

Discussing Mobile Device Security

- **How can the use of mobile devices by employees affect the security of an organization as a whole?**

- **ANSWER:**
  - Mobile devices can function much like regular computers
  - They are used to send emails and to access systems and data network
  - They are a vulnerability.

Discussing Mobile Device Security

- **What technology mitigates against an online account being accessed from an unknown device?**

- **ANSWER:**
  - Two-step verification—the site sends a code to a registered phone or alternative email address, prompting the user to verify the validity of the device.

Discussing Mobile Device Security

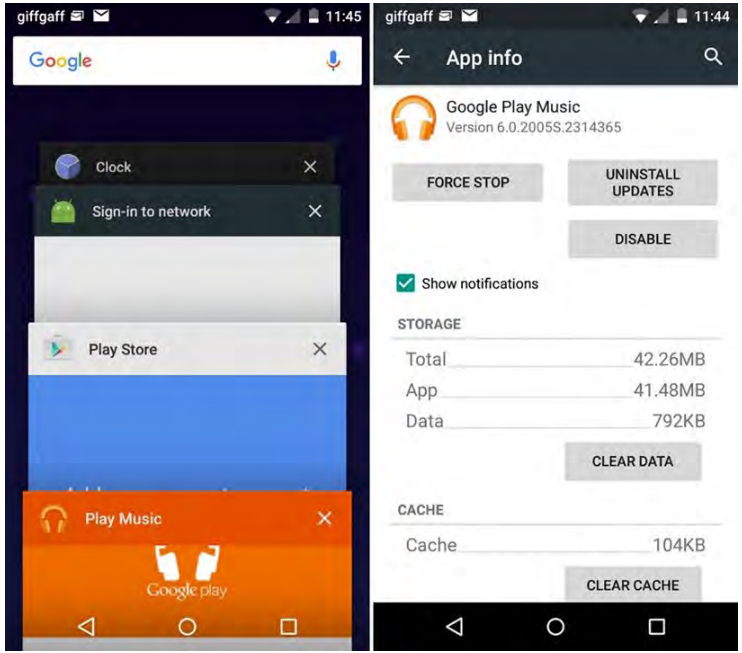
- **What is MDM?**

- **ANSWER:**
  - Mobile Device Management (MDM) is a class of management software designed to apply security policies to the use of smartphones and tablets in the enterprise.

Topic B: Troubleshoot Mobile Device Issues

Mobile OS Troubleshooting Tools

- Adjust Settings
- Close running apps
  - Force stop
  - Force Quit
- Uninstall and reinstall apps
- Reset the device
  - Soft reset
  - Forced restart
  - Factory default reset



Android Force Stop

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

Guidelines for Using Mobile Troubleshooting Tools

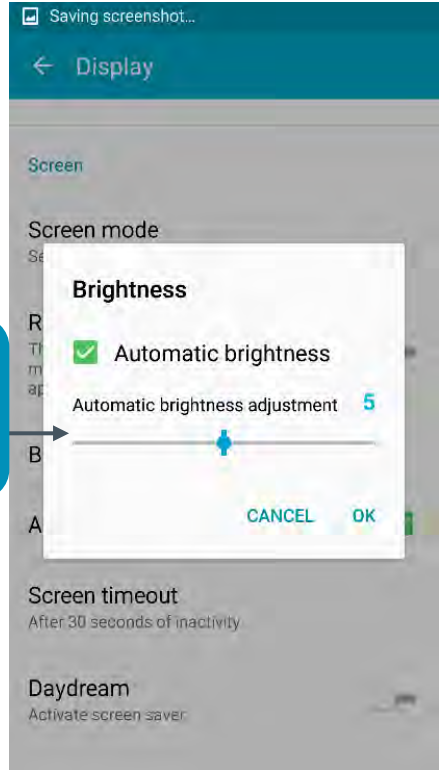
- Adjust settings for the core OS and for apps.
- Close running apps draining the battery or are unresponsive.
- Uninstall apps that are no longer needed
- Try a soft then a forced reset for frozen or unresponsiveness.
- Perform a factory default reset

Mobile OS Issue Troubleshooting

- Dim display
- Touchscreen unresponsive or inaccurate
- External monitor issues
- Sound issues
- Overheating

Check for overheating

Check or change display brightness



Guidelines for Troubleshooting Mobile OS Issues

- Dim display.
  - Open the **Display** settings and adjust the automatic brightness
  - Check for apps that dim the backlight to conserve power.

- Unresponsive or inaccurate touchscreen.
  - Check screen protectors.
  - Check that adequate resources available.
  - Use a re-calibration utility.

- Issues with external monitor.
  - Verify that the cable is good.
  - Verify that a casting dongle is configured correctly

Guidelines for Troubleshooting Mobile OS Issues

- Sound issues.
  - Verify volume controls.
  - Verify silent mode is not enabled.
  - Check volume controls within the app.
  - Verify if it is configured to use Bluetooth.

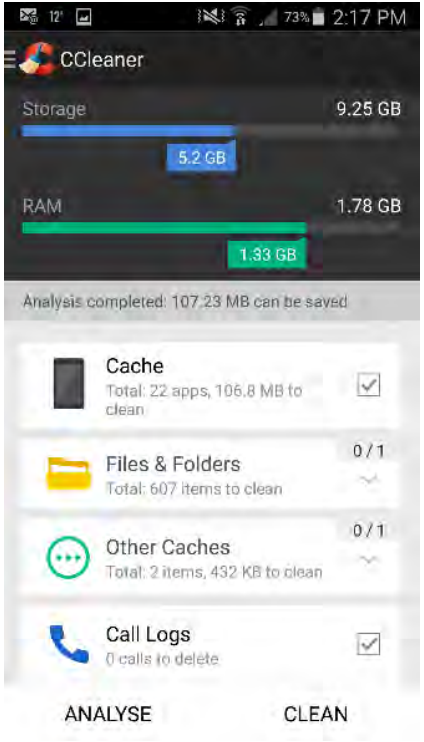
- Overheating.
  - Determine if the device is being used intensively.
  - View battery status information.
  - Direct sunlight or other heat sources.

Mobile App Issue Troubleshooting

- Apps not loading.
- App log errors.
  - Enter developer mode to view log files.

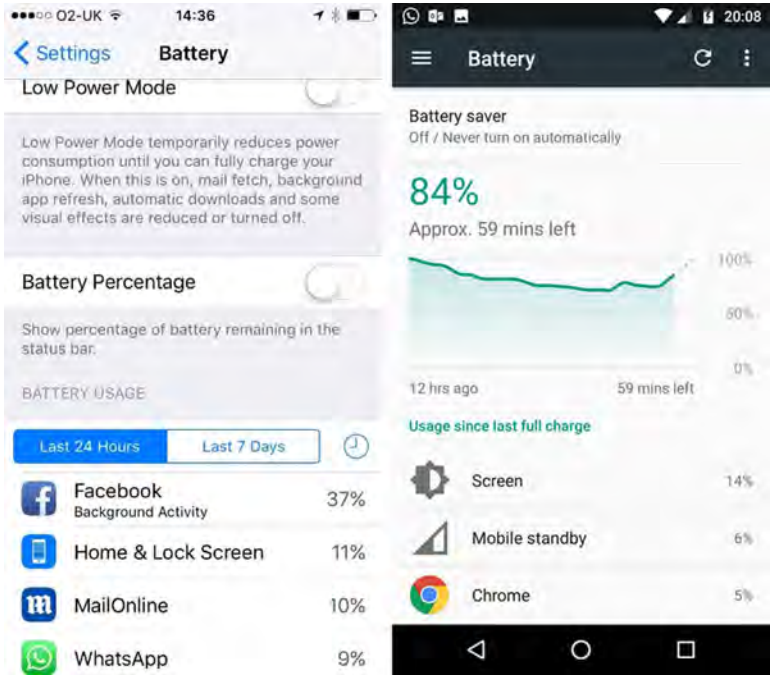
Mobile App Issue Troubleshooting

- Slow performance:
  - Resources might be too low.
  - Use an app such as CCleaner.
  - Try soft resets, then factory default reset (as a last resort).
  - Examine recently installed apps.



Mobile App Issue Troubleshooting

- Battery life:
  - It will degrade over time.
  - GPU and CPU intensive apps drain a battery quickly.
  - Malicious apps using power-intensive services.
  - Uninstall the app, or prevent it from running in the background.



Guidelines for Troubleshooting Mobile App Issues

- If an app is not loading:
  - Verify that it wasn't installed on a memory card that is not in the mobile device.
  - Verify that the app is not corrupted; uninstall and reinstall the app.
- Put the device in developer mode to access log files.
- Slow performance:
  - Check for newer apps
  - Check that apps are functioning correctly and are not running in the background.

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 (NFC) Feature enable/disable or signal strength issue

- Troubleshooting AirDrop issues
  - iOS feature for file transfer between iOS and macOS devices vie Bluetooth
  - The sender must be in the recipient's contacts list, or AirDrop must be configured to receive files from everyone
  - Bluetooth configuration and signal strength

Mobile Wireless Issue Troubleshooting

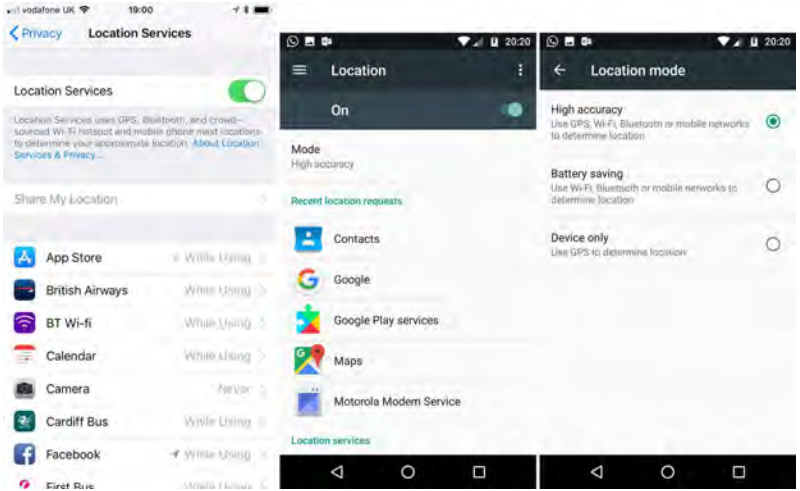
- Issues with any wireless connection type
  - Wi-Fi
  - Bluetooth
  - Cellular radio
- Determine whether
  - Configuration error
  - Hardware error
  - Interference problem
    - Wi-Fi analyzers

Guidelines for Troubleshooting Mobile Wireless Issues

- Interference issues
  - Use a Wi-Fi Analyzer for signal strength.
- Configuration issues
  - airplane mode.
  - a radio service (NFC) has not been disabled.
  - Settings will verify that configuration are correctly configured.
  - Wi-Fi access point supports same standard as mobile device.
- If none of these are the issue, determine if an OS or firmware update is needed.

Mobile Device Security Troubleshooting

- Utilization symptoms
  - Rogue apps running in background -power drain and high resource use
  - Unauthorized location tracking
    - Disable location services unless required by apps
  - Install patches and upgrades



Root Access Security Concerns

- Owner-level permissions
  - In iOS and Android, the user account created during setup can install apps, and configure settings. User are restricted from making any system-level changes.
  - Users who want to avoid the restrictions that some OS vendors, and telecom providers must use some type of privilege escalation:
  - Root access or custom ROM: (Android) Some vendors provide authorized mechanisms for access to the root account on their device.
  - This may be necessary to exploit a vulnerability or use custom (firmware) a new Android OS image applied to the older device.

Root Access Security Concerns

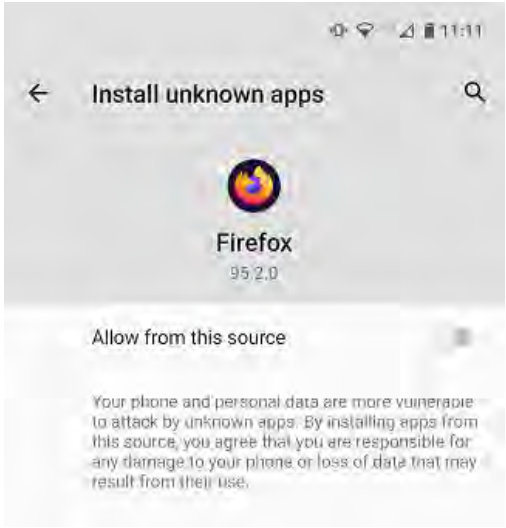
- Root-level permissions
  - Jailbreaking iOS is more restrictive than Android to gain Root privileges
  - Sideload apps, change carriers, and customize the interface

- Rooting or jailbreaking mobile devices involves subverting the security controls built into the OS to gain unrestricted system-level access

- The device can no longer be assumed to run a trusted OS. (Warranty)

Mobile App Soofing Security Concerns

- App spoofing
  - Rogue developers placing malicious apps in trusted stores
  - Fake reviews and manipulated download figures
- Bootleg app stores
  - Pirated apps –looks like a legitimate app
- Install apps by sideloading - This breaks licensing and copyrights laws, malware risks.
- Under iOS, using the developer tools can be a means of installing apps from outside the App Store without having to jailbreak the device



Mobile Device Security Troubleshooting

- Enterprise apps and Android package (APK) sideloading
  - Enterprise store distribution
  - Android APK sideloading from untrusted sources
  - System lockout:
  - Forgotten password
  - On purpose when the device is reported stolen or lost

- Troubleshooting email problems:
  - Verify credentials and email settings are correctly entered
  - Verify corporate email password change is replicated to mobile devices
  - Use digital certificates to encrypt messages

Mobile Device Security Troubleshooting

- User behavior issues
  - Careless use
  - Failure to follow security best practices
  - Use of insecure hotspots
  - Unintended Bluetooth pairing
- System lockout
  - Forgotten password
  - On purpose when the device is reported stolen or lost
- Troubleshooting email problems
  - Verify credentials and email settings are correctly entered
  - Verify corporate email password change is replicated to mobile devices
  - Use digital certificates to encrypt messages

Mobile Device Security symptoms

- General symptoms
  - High number of ads: Free apps are all supported by advertising
  - Fake security warnings: (Scareware) is used by to persuade users to install an app or give a Trojan app additional permissions
  - Sluggish response time: Malware is likely to try to collect data
  - Limited/no Internet connectivity: Malware may corrupt the DNS and/or search provider to perform redirection and force users to spoofed sites.
  - Unexpected application behavior
  - Permissions and device usage
  - High utilization and network traffic
  - Leaked personal files/data
  - Breach notification
  - Unauthorized account access
  - Location tracking

Mobile Device Security symptoms

- Unexpected app behavior
  - Bootleg or spoofed app acts like a Trojan.
  - Permissions and device usage camera/microphone
  - High utilization and network traffic

- Leaked personal files/data
  - Compromised, files or personal data might be sold
  - Unauthorized account access
  - Location tracking
  - Breach Notification - Notify users immediately that website or service had a data breach

Troubleshooting Mobile Device Issues

- **True or false? A factory reset preserves the user's personal data.**

- **ANSWER:**
  - False. Restoring to factory settings means removing all user data and settings.

Troubleshooting Mobile Device Issues

- **What is the first step to take when an app no longer loads?**

- **ANSWER:**
  - Try restarting the device. If that does not work, uninstall and then reinstall the app.

Troubleshooting Mobile Device Issues

- **Your organization has several tablet devices that are loaned out as needed when employees are traveling. Some users have reported problems getting the Bluetooth keyboard to work with one of the tablets. What should you do?**

- **ANSWER:**
  - There are a couple of issues that can cause Bluetooth connectivity problems. First, check whether the device batteries need replacing. Another possibility is that the tablet might need a system update. Finally, the devices might not have been set to discoverable mode. For security purposes, only enable discovery mode on your mobile device when want a Bluetooth device to find your device; otherwise, keep that setting disabled. The Bluetooth settings must be configured to allow devices to connect to the mobile device. This is also referred to as pairing.

Troubleshooting Mobile Device Issues

- **A user reports that the touchscreen on his mobile device is not responding properly. What questions should you ask, and what steps might you take to resolve the issue?**

- **ANSWER:**
  - You should ask if the touch screen is greasy, wet, or dirty. If it needs cleaning, remind the user to use only a soft cloth moistened with eye glass cleaner to gently wipe the screen. If cleaning is not an issue, ask if it appears to be scratched, cracked, or otherwise damaged. If so, make arrangements to have the touch screen replaced. If there is no visible damage, recalibrate the screen for the user, and check for updates.

Troubleshooting Mobile Device Issues

- **What is a Wi-Fi Analyzer used for?**

- **ANSWER:**
  - A Wi-Fi Analyzer is used to check connectivity issues with wireless. It can check for less congested channels.

Troubleshooting Mobile Device Issues

- **What are the causes of severe battery drain?**

- **ANSWER:**
  - The display, radio, and CPU are the components that draw the most power. If an app is overutilizing these resources, it could be faulty, badly written, or this could be a sign of malware activity.

Reflective Questions

1. In your professional experience, have you supported mobile devices? If not, what kind of experience do you have with them?

2. What type of technical support do you think will be expected of an A+ technician as mobile devices become even more prominent within the workplace?