18-1 Backing Up Mobile Devices

Core 2 Objectives

- 1.8

  Explain common OS types and their purposes.
- 2.7

  Explain common methods for securing mobile and embedded devices.

Methods of backing up mobile devices rely heavily on the OS they use. Currently, the most popular mobile OSs are Android by Google (google.com) and iOS and iPadOS by Apple (apple.com). Here is a summary of the tools and techniques covered in more detail in the Core 1 module “Supporting Mobile Devices”:

- **Navigating Android and iOS.** The OS provides a home screen; navigation interface; and ways to download, install, uninstall, open, and close apps.
- **Settings.** The Settings app is used to manage most OS and app settings, although some app settings can be managed within the app.
- **Quick access settings.** Each OS has a quick-access settings screen that is easily accessed from the home screen. Android uses the notification area, and iOS uses the Control Center.
- **OS updates.** Updates to the OS are managed in the Settings app and are normally set to automatically download and update.
- **Wireless connections.** Wireless connections on a mobile device can include cellular voice and data, Wi-Fi, GPS, Bluetooth, NFC (near-field communication), and AirDrop (Apple only). These connections are managed in the Settings app.
- **Purpose of MDM.** Large corporations use **mobile device management (MDM)** software on both the server and mobile device to enforce MDM policies designed to secure corporate data and apps (for example, email) for both corporate-owned and personal devices. For personal devices, these policies are known as **BYOD (bring your own device)** policies.
- **Data syncing.** Google and Apple both provide methods for syncing data via the cloud among mobile devices that use the same Google or Apple account. This data includes email, contacts, calendars, photos, document files, and other content. Sync settings are managed in the Settings app or in individual apps that manage content (for example, the Photos or email app). Synced data is available in the cloud at google.com for Goggle and iCloud.com for Apple.
- **Troubleshooting.** When troubleshooting a mobile device, useful techniques include updating the OS and restarting and rebooting the

device. A technician might be called on to solve problems related to malware infections, display and touch screen issues, connectivity issues, damaged ports and liquid damage, and battery, overheating, and charging issues.

Core to Core

In this module, we dig deeper into several of the skills listed earlier. If you are not familiar with each of these skills—including how to navigate, update, and manage each OS and troubleshoot a mobile device—now would be the time to review this content in the Core 1 module “Supporting Mobile Devices.”

18-1aUpdate the OS

Core 2 Objective

- 2.7

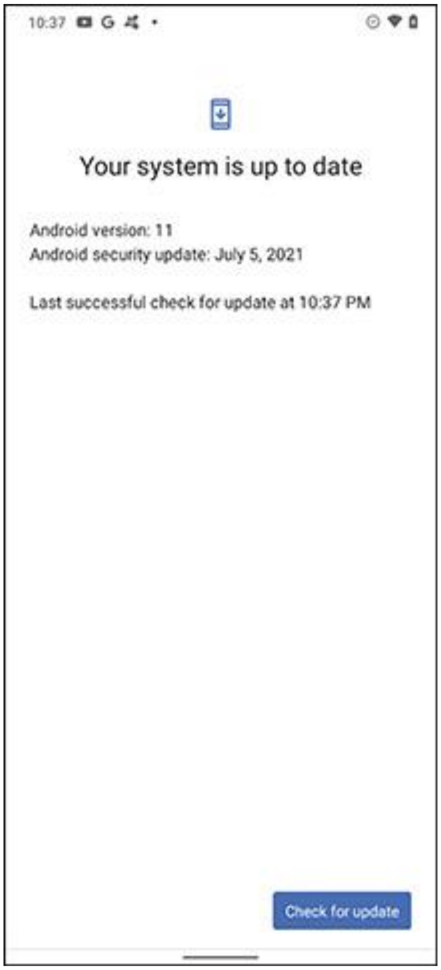
  Explain common methods for securing mobile and embedded devices.

Updates to the Android OS are automatically pushed to the device from the manufacturer. Because each manufacturer maintains its own versions of Android, these updates might not come at the same time Google announces a major update, which limits availability of updates for some devices. Also, vendors don’t continue to make these modifications indefinitely—eventually, a device ages out of the vendor’s updates in what’s called an **end-of-life (EOL)** limitation. When the device does receive notice of an update, it might display a message asking permission to install the update. With some devices, you can also manually check for updates at any time, but not all devices provide this option.

To see if manual updates can be performed on an Android device, go to the **Settings** app and tap **System**, **Advanced**, and **System update** (see Figure 18-1). Tap **Check for update**. The device turns to the manufacturer’s website for information and reports any available updates.

Figure 18-1

Use the Android Settings app to see the latest OS update and manually check for new updates



10:37

Your system is up to date

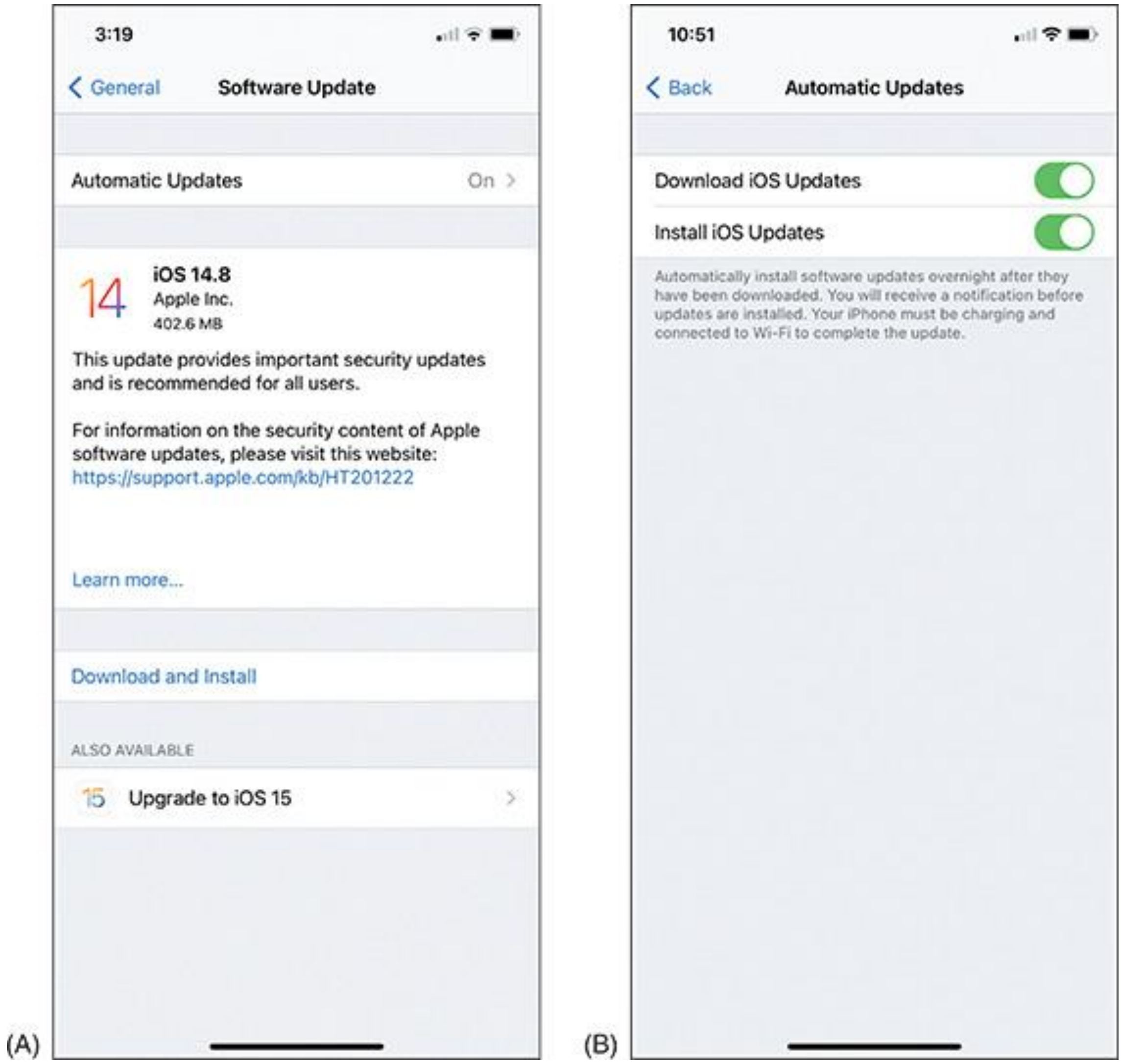
Android version: 11
Android security update: July 5, 2021

Last successful check for update at 10:37 PM

To check for and install updates on an iOS device, you must first be signed in to your device with an Apple ID, which requires an associated credit card number. Then open the **Settings** app, and tap **General** and **Software Update**. Any available updates will be reported here and can be installed (see Figure 18-2A)**.** Tap the right arrow next to "Automatic Updates" to view and change update settings (see Figure 18-2B)**.**

Figure 18-2

iOS has an available update to install



3:19

General

Software Update

Automatic Updates On

14 iOS 14.8

Apple Inc.

402.6 MB

This update provides important security updates and is recommended for all users.

For information on the security content of Apple software updates, please visit this website: https://support.apple.com/kb/HT201222

Learn more...

Download and Install

ALSO AVAILABLE

15 Upgrade to iOS 15

10:51

Back

Automatic Updates

Download iOS Updates

Install iOS Updates

Automatically install software updates overnight after they have been downloaded. You will receive a notification before updates are installed. Your iPhone must be charging and connected to Wi-Fi to complete the update.

18-1bMobile Apps Development

Core 2 Objective

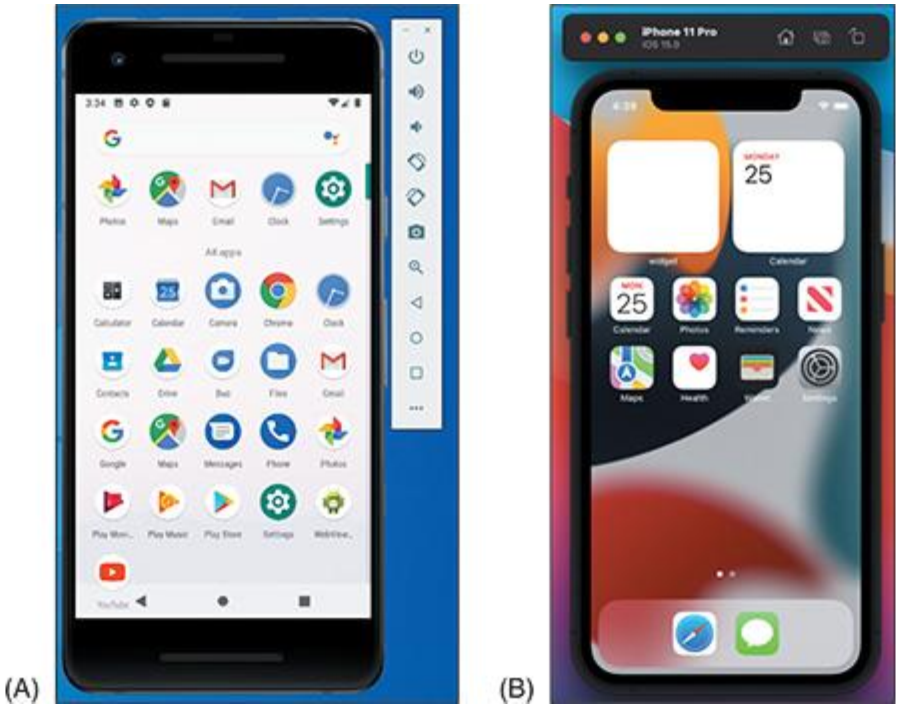
- 1.8

Explain common OS types and their purposes.

Both Android and iOS offer tools for mobile app development that you can use to learn more about supporting and securing mobile devices. To write and test Android apps, an app developer uses a group of tools in an **SDK (software development kit)**, such as Android Studio (developer.android.com) or Visual Studio (visualstudio.microsoft.com). An Android SDK includes an Android **emulator**, which is software that creates a virtual Android device complete with virtual hardware (buttons, camera, and even device orientation), a working installation of Android, and native apps (see Figure 18-3A). Android Studio is free and is released as open source. In a project at the end of this module, you'll download and install Android Studio, and then use it to create virtual Android devices or emulators.

Figure 18-3

(A) Android emulator with the app drawer open; (B) iPhone 11 Pro emulator with home screen



Apple offers its own app-development tools, including the iOS SDK (software development kit), collectively called Xcode at developer.apple.com. Xcode installs free in macOS along with Apple emulators for testing apps (see Figure 18-3B). Although the tools are not available in Windows, there are several workarounds, such as React Native (reactnative.dev), which can install in Windows and build iOS apps using JavaScript, and MacInCloud (macincloud.com), which provides macOS virtual machines that can be used to build iOS apps in the cloud. In a project at the end of this module, you'll download and install Xcode on a Mac computer and use it to run an iPhone emulator.

Note 1

You can follow along with the steps in the following sections using a real smartphone or tablet (Android or iOS), or you can use an Android, iPhone, or iPad emulator. Projects at the end of this module give you step-by-step instructions to install and configure the free Android Studio (which includes several Android emulators) on a Windows computer and the Xcode simulators on a Mac computer. You can use these emulators with real features that work like those on a physical device, including a power button, rotate capability, camera function, and much more.

The first step to secure a mobile device is to maintain good backups. How to back up a device is discussed next.

18-1cBackup and Recovery

Core 2 Objective

- 2.7

Explain common methods for securing mobile and embedded devices.

In the module "Supporting Mobile Devices," you learned to back up app data, which is an important skill. If, however, your mobile device is lost, stolen, or damaged beyond repair, you might need to recover not only app data but also mobile device settings, configurations, and profiles. This section of the module covers how to back up the entire device. Let's start with a summary of backup options:

- **File-level backup.** Syncing emails, contacts, calendars, photos, and other data through online accounts or to your computer is called a **file-level backup** because each file is backed up individually. File-level backups, however, don't include your OS settings, such as your Wi-Fi passwords, account profile, or device and app configuration.
- **Partial image-level backup.** A true **image-level backup** includes everything on the device and can completely restore the device to its previous state. A mobile device OS, however, offers only a partial image-level backup that includes settings, native app data, Wi-Fi passwords, the account profile, and device and app configuration. Third-party app configurations and their data are not included in the OS backup.
- **Combination of file-level and partial image-level backups.** To prepare for catastrophic failure or loss, you need to use both backup methods: Sync app data to your computer or the cloud, and use the OS backup for other types of data and settings. Make sure that syncing and backups include critical apps, their configuration, and data. In reality, though, backups for mobile devices will miss some configurations, such as app installations or third-party app configurations. For this reason, you might also need third-party software, such as Dr.Fone (drfone.wondershare.net), to make a full device backup that includes third-party apps and app data.

Generally, you can back up to the cloud or to your computer. Let's look next at how Android backs up to Google Drive.

Google Drive Backup

To enable Android's backup feature, open the **Settings** app, and tap **System** and then **Backup**. Make sure that **Back up to Google Drive** is turned on, and change the backup account if needed. You can also fine-tune what content is included in the backup and back up now. Your backup data is stored on Google servers and is associated with your Google account. When you first turn on a new Android device, you are given the chance to enter your Google account information and restore an existing Google backup to the new device.

Caution

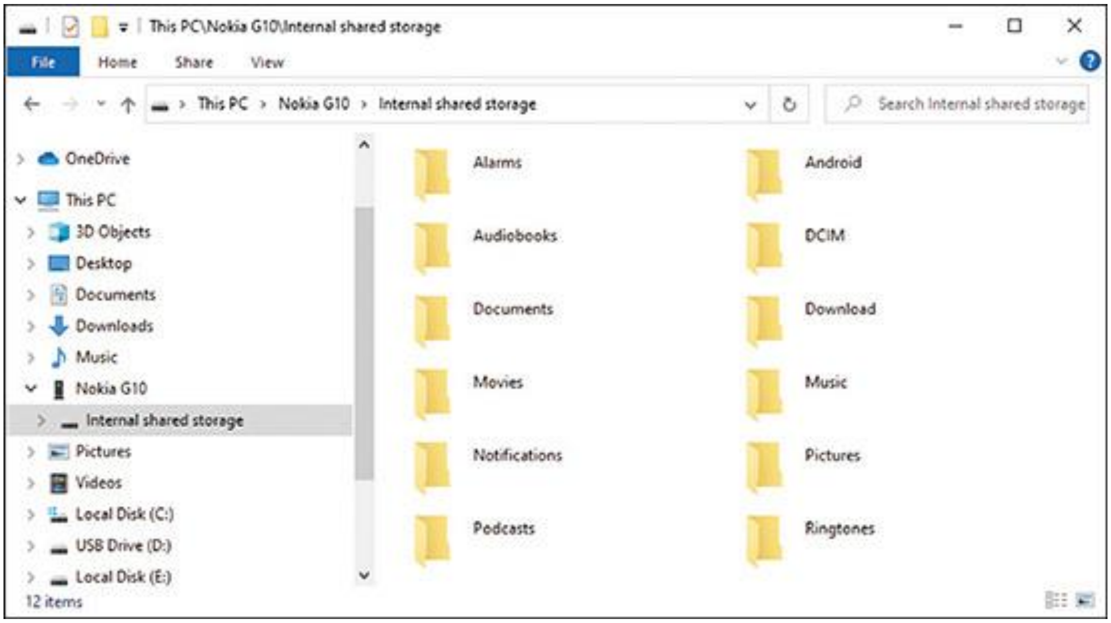
You cannot restore a backup to a new device if the new device uses a version of Android that is lower than the Android version of the old device.

Back Up Android Data to a Computer

You can use a USB cable to transfer files between an Android device and a computer. Connect the cable and then open the **Settings** app.
Tap **Connected devices** and then **USB**, and select **File Transfer**. Content can then be accessed in Explorer on a Windows computer (see Figure 18-4) or in Finder on a Mac.

Figure 18-4

Transfer files between a Windows computer and an Android device



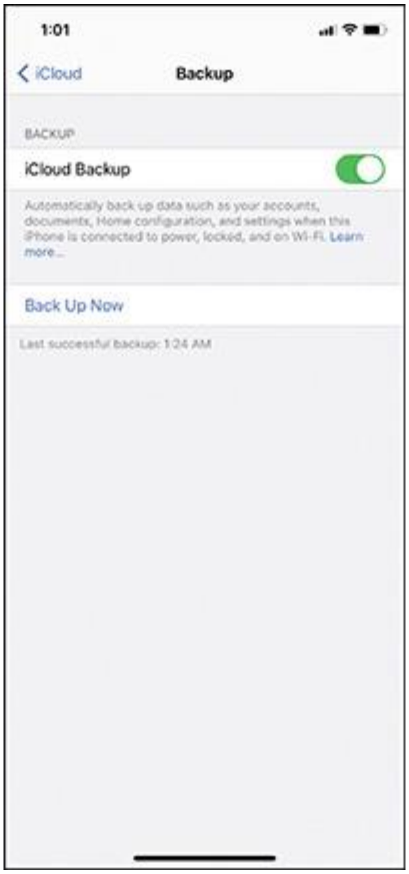
To create a detailed backup of an Android device—including the device configuration as well as the content—to a computer, you need a third-party app or a manufacturer's app. First check with the device manufacturer for its backup app. To use the app, you'll need to first set up a user account with the manufacturer. Also know that an Android device manufacturer is likely to provide cloud storage to keep remote backups of your device.

iCloud Backup

An iPhone or iPad can back up to a computer or to the cloud using iCloud. The best practice is to use both methods. To set up iCloud backups, go to **Settings**, tap the user name, and then tap **iCloud**. Scroll down and tap **iCloud Backup**. See Figure 18-5. When you turn on iCloud Backup, it backs up daily whenever the device is plugged into a power source and connected to Wi-Fi, the screen is locked, and there’s enough unused iCloud storage to hold the backup. However, you can also create a new backup at any time by clicking **Back Up Now**, as shown in Figure 18-5. iCloud backs up app data, call history, device settings, text, photos, and videos unless these items are already included in iCloud syncing.

Figure 18-5

iCloud Backup is on, and you can back up now



iCloud Backup

Automatically back up data such as your accounts, documents, Home configuration, and settings when this iPhone is connected to power, locked, and on Wi-Fi. Learn more...

Back Up Now

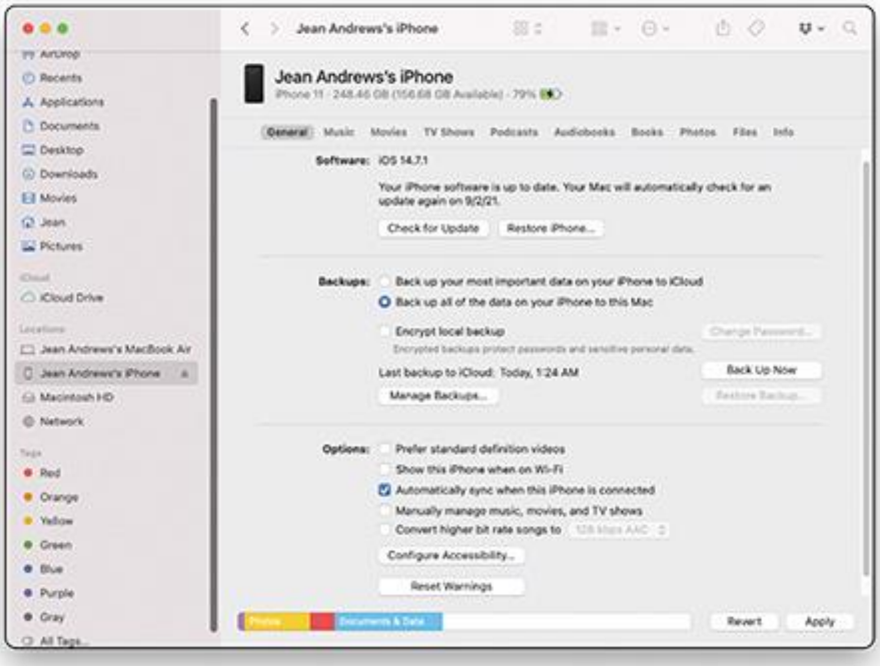
Last successful backup: 1:24 AM

Back Up iOS to a Computer

An iPhone or iPad can back up to a Mac computer without any extra software. On a Mac, connect the iPhone or iPad to the Mac using a cable (for example, a Lightning to USB cable). Unlock the device, and open the **Finder** window. (The Finder window is similar to Explorer in Windows.) Select the device in the left pane (see Figure 18-6). In the right pane, select **General** and **Back up all of the data on your iPhone to this Mac**, as shown in the figure. Notice you also have the option to encrypt the backup. Click **Back Up Now**.

Figure 18-6

Back up an iPhone to a Mac computer



Jean Andrews's iPhone
iPhone 11 · 248.46 GB (156.68 GB Available) · 79%

Software: iOS 14.7.1

Your iPhone software is up to date. Your Mac will automatically check for an update again on 9/2/21.

Backups: ○ Back up your most important data on your iPhone to iCloud
● Back up all of the data on your iPhone to this Mac
□ Encrypt local backup
Encrypted backups protect passwords and sensitive personal data.
Last backup to iCloud: Today, 1:24 AM

Options: □ Prefer standard definition videos
□ Show this iPhone when on Wi-Fi
☑ Automatically sync when this iPhone is connected
□ Manually manage music, movies, and TV shows
□ Convert higher bit rate songs to 128 kbps AAC

To back up to a Windows computer, you must install iTunes software to manage the backup.

Applying Concepts

Back Up an iPhone or iPad to a Windows Computer

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.7

On a Windows computer, do the following to back up an iPhone or iPad:

1. 1
   Go to the Microsoft Store, and search for **iTunes**. Download and install **iTunes** by Apple Inc. iTunes is used to manage digital entertainment media, and its secondary purpose is to back up Apple devices on a Windows computer.

2. 2
   Open **iTunes**, connect your iPhone or iPad to the computer with a USB cable, and unlock the device.

3. 3
   You'll need to enter your passcode to the device or respond to a message on the device asking whether you trust the computer. Enter your response.

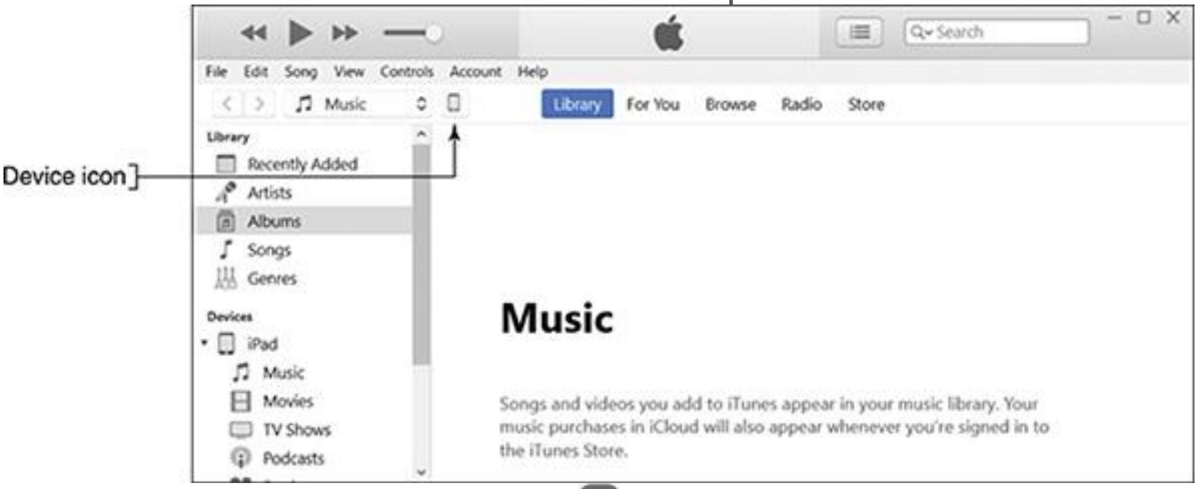
4. 4
   A message in iTunes asks if you want to allow the computer to access the device. Click **Continue**.

5. 5

   In the iTunes window, click the device icon near the top of the screen (see Figure 18-7).

Figure 18-7

Click the device icon in the menu bar to view options for the connected device



Music

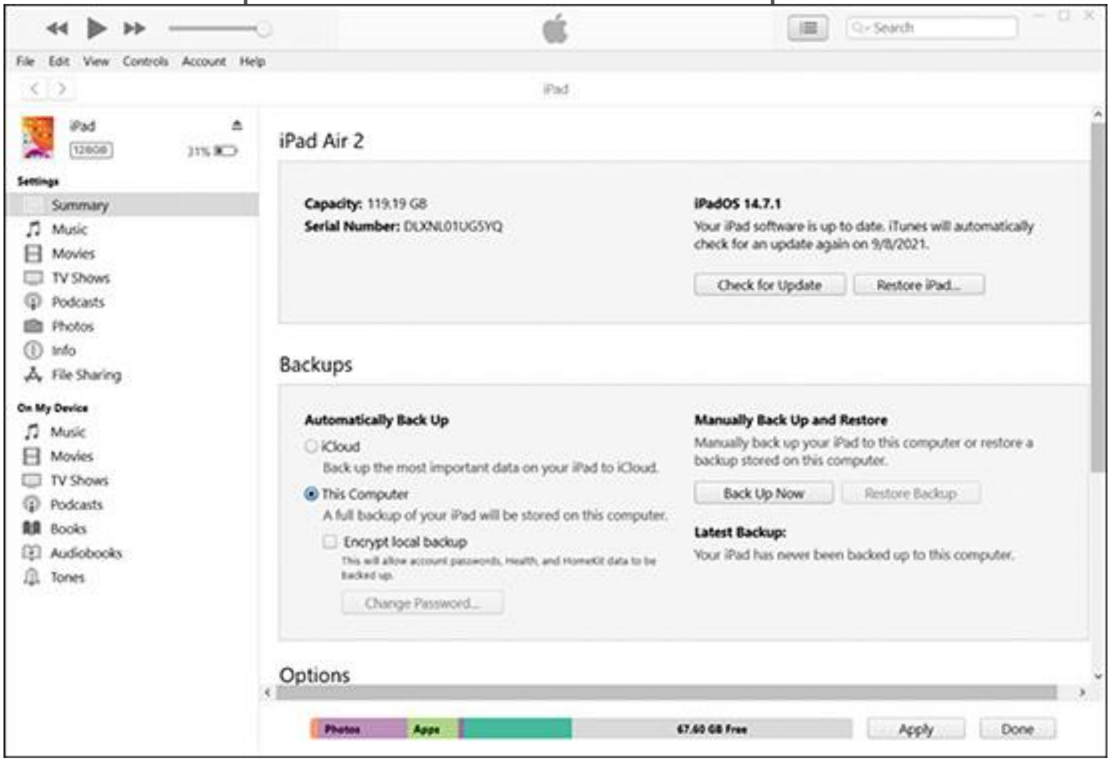
Songs and videos you add to iTunes appear in your music library. Your music purchases in iCloud will also appear whenever you're signed in to the iTunes Store.

6. 6

   Under *Automatically Back Up*, select **This Computer**. See Figure 18-8. Notice you can also select the option to encrypt the backup. Click **Back Up Now** to start the backup.

Figure 18-8

Use iTunes to back up an iPad to this Windows computer



iPad Air 2

Capacity: 119.19 GB

Serial Number: DLXNL01UG5YQ

iPadOS 14.7.1

Your iPad software is up to date. iTunes will automatically check for an update again on 9/8/2021.

Backups

Automatically Back Up

○ iCloud

Back up the most important data on your iPad to iCloud.

● This Computer

A full backup of your iPad will be stored on this computer.

□ Encrypt local backup

This will allow account passwords, Health, and HomeKit data to be backed up.

Manually Back Up and Restore

Manually back up your iPad to this computer or restore a backup stored on this computer.

Latest Backup:

Your iPad has never been backed up to this computer.

Later, if you need to recover from the backup, connect your device to the computer, and in the Finder window on a Mac or iTunes window on a Windows computer, select your device. Then click **Restore Backup** (refer back to Figure 18-6). You can then select a backup based on the date of each backup.

Whatever backup method you use, it's important to occasionally test the backup recovery process to verify that you know how to use it, the recovery works, and you know exactly what's being recovered. After you test the recovery process, you might realize you need additional backup methods in place to make sure everything is covered.

Note 2

If you're about to buy a new phone or tablet, be sure to back up your old device before you switch your carrier service or your Google or Apple account to the new device. If possible, also back up your phone or tablet before taking it in for repair at a service center.

Recover from the Backup

Here are two situations when you might want to use a backup to recover a device:

- **To the original mobile device.** If you have reset the device while troubleshooting a problem and have a backup in the cloud, sign in to the device using your Google or Apple account. You will then be given the option to recover from backup or set up the device as a new device. You'll learn more about resetting a device later in this module. For iOS, if you have a backup on your computer and connect the device to your computer, macOS or iTunes in Windows gives you the option to restore from backup.
- **To a new device.** The same recovery options are offered when you first sign in to a new mobile device using your Google or Apple account—or, for iOS, when you connect a new device to your Mac computer or Windows computer with the iTunes app. When you're setting up a new device, the setup process asks if you want to restore content from a previous backup and also asks which backup to use.

18-2Securing Mobile Devices

Core 2 Objectives

- 2.1

  Summarize various security measures and their purposes.
- 2.7

  Explain common methods for securing mobile and embedded devices.
- 3.5

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

Because smartphones and tablets are so mobile, they get stolen more often than other types of computers. Therefore, protecting data on a mobile device is especially important. Consider what might be revealed about your life if someone stole your smartphone or tablet and the data on it.

- Your apps and personal data could expose email, calendars, call history, voice mail, text messages, Google Pay, Apple Pay, PayPal, banking apps, Dropbox, iCloud Drive, Google Maps, Gmail, QuickMemo, YouTube, Amazon, Facebook, videos, photos, notes, contacts, and bookmarks and browsing history in web browsers.
- Videos and photos might reveal private information and might be tagged with date and time stamps and GPS locations.
- Network connection settings include Wi-Fi security keys, email configuration settings, user names, and email addresses.
- Purchasing patterns and history as well as credit card information might be stored—or at least accessible for use—in mobile payment apps, in apps developed by retailers, through membership card databases, or through email records.

To keep your data safe, consider what apps you can use to protect your data, how to control access to your device, and which BYOD (bring your own device) policies might be used in an enterprise environment to secure corporate data stored on a device.

Most of the methods discussed here require the user to understand the importance of a security measure and how to use it:

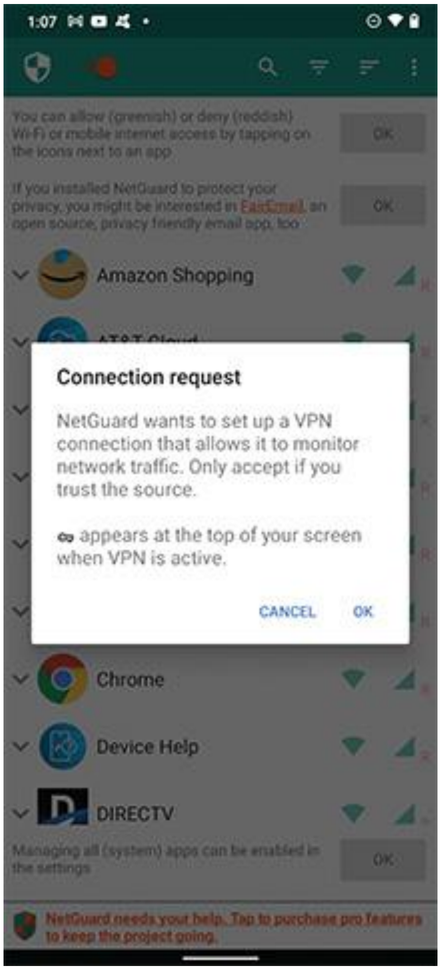
- **OS updates and patches.** Apply OS updates and patches to plug up security holes. Recall that Android automatically pushes updates to many of its devices, but iOS devices require manual updates.
- **Antivirus/anti-malware.** Because Apple closely protects iOS and its apps, it's unlikely an Apple device will need anti-malware software. The Android OS and apps are not as closely guarded, so Android anti-malware apps are recommended. Before installing one, be sure to read reviews about it. Most of the major anti-malware software companies provide Android anti-malware apps.
- **Firewalls.** As with Windows computers, a firewall on a mobile device helps control which apps or services can use network connections. When you install an app, you're required to agree to the permissions it requests in order to get the app. A firewall gives you more control over an app's network access. For example, a firewall can prevent the Facebook app from sending SMS messages.

  Most firewall apps for Android devices mimic a VPN connection, which forces all network communication to be routed through the firewall. Figure 18-9 shows an example of one firewall app, NetGuard

(*netguard.me*), on an Android smartphone; the app allows you to decide which other apps can use the networks.

Figure 18-9

Use NetGuard VPN connection in Android to control which apps can access the Internet



1:07

You can allow (greenish) or deny (reddish) Wi-Fi or mobile internet access by tapping on the icons next to an app

OK

If you installed NetGuard to protect your privacy, you might be interested in FairEmail, an open source, privacy friendly email app, too

OK

Amazon Shopping

AT&T Cloud

Connection request

NetGuard wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

⚯ appears at the top of your screen when VPN is active.

CANCEL OK

Chrome

Device Help

DIRECTV

Managing all (system) apps can be enabled in the settings

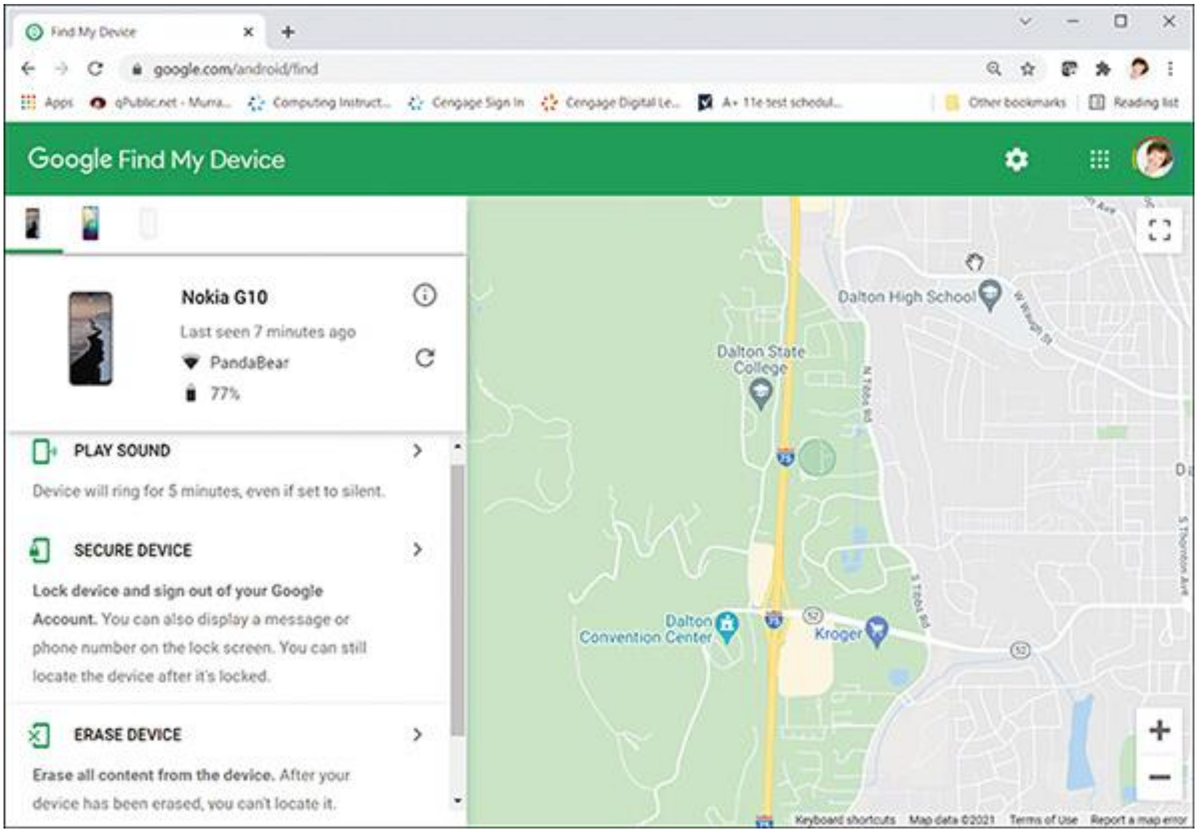
OK

NetGuard needs your help. Tap to purchase pro features to keep the project going.

- **Android locator application and remote wipe.** You can use Find My Device (google.com/android/find), Android's built-in **locator application**, to locate your phone on a map, force it to ring at its highest volume, lock the device, display a message on the screen, or remotely erase all data from the device to protect your privacy, which is called a **remote wipe**. See Figure 18-10. To use the locator app to locate your device or perform a remote wipe, Find My Device must already be turned on using the **Security** screen in the Settings app. Third-party locator applications are also available in the Play Store.

Figure 18-10

Locate a lost Android device using any web-enabled computer or mobile device and your Google account



Nokia G10

Last seen 7 minutes ago

PandaBear

77%

PLAY SOUND

Device will ring for 5 minutes, even if set to silent.

SECURE DEVICE

Lock device and sign out of your Google Account. You can also display a message or phone number on the lock screen. You can still locate the device after it's locked.

ERASE DEVICE

Erase all content from the device. After your device has been erased, you can't locate it.

- **iOS locator application and remote wipe.** Similar to Android's Find My Device, iCloud offers the ability to locate a lost iOS device if the feature is already enabled on the device before it's lost. On an iPad or iPhone, open the **Settings** app, tap the ***user name***, and turn on **Find My iPad** or **Find My iPhone.** To find the device, using any browser, go to icloud.com/find and sign in with your Apple ID. Besides using a browser on a computer to find your device, you can also download Find My iPhone or Find My iPad to another Apple device and use it to locate your lost device. Both apps are free. If your device was stolen or you have given up on finding your device, you can use iCloud to perform a remote wipe.

18-2aDevice Access Controls

Core 2 Objective

- 2.7

Explain common methods for securing mobile and embedded devices.

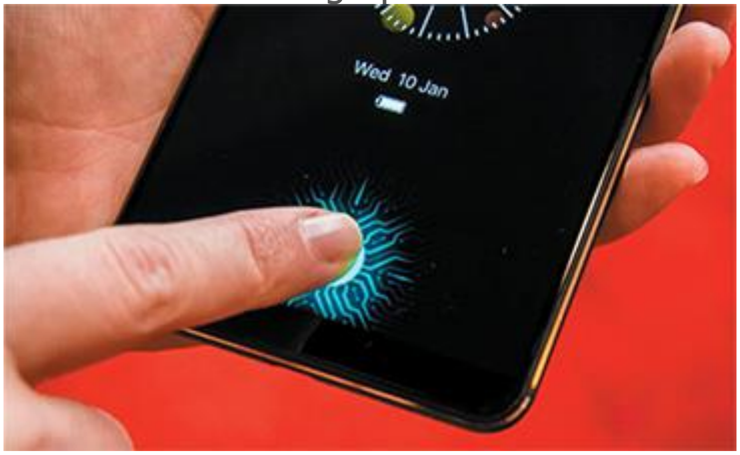
To control access to the device, consider the following lock methods:

- **Lock the screen.** A screen lock requires the correct input to unlock the device. Mobile devices provide a variety of options for unlocking the screen. As the complexity of a lock code increases, so does the security of the device:

- **Swipe lock.** Swipe your finger across the screen to unlock the device. (This is not very secure, but it prevents a pocket dial.)
- **PIN code lock.** Enter a numeric code with numbers.
- **Password lock.** Enter an alphanumeric code with letters and/or numbers.
- **Pattern lock.** Draw a pattern across a display of dots on the screen.
- **Fingerprint lock.** Use a specialized scanner that collects an optical, electrical, or ultrasonic reading of a person's fingerprint and then compares this information to stored data. The fingerprint reader might be on the front or side of the device (see Figure 18-11).

Figure 18-11

Access the device via a fingerprint scan

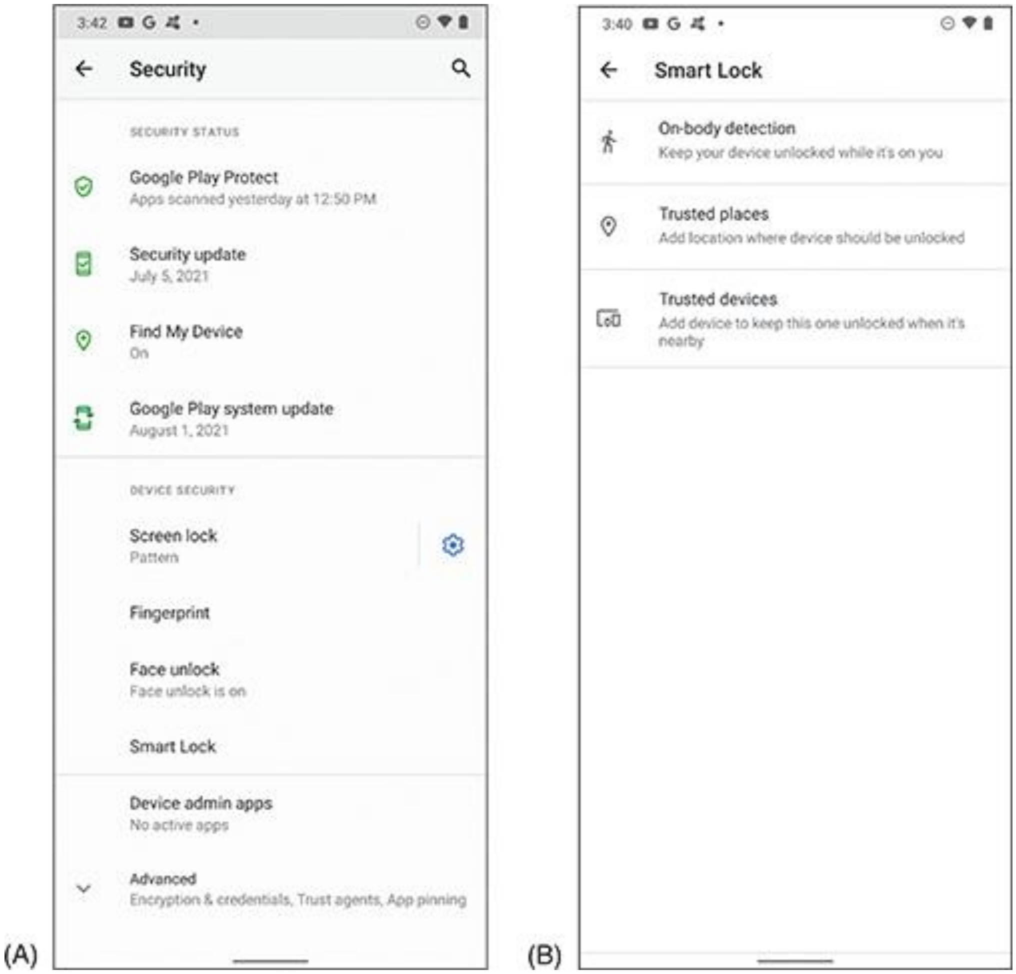


Source: CNET

- **Facial recognition lock.** Use the device's camera to perform facial recognition. A facial lock requires a backup method, such as those shown in Figure 18-12A, because facial recognition is not that secure—your device can be unlocked when you look at it even if you didn't intend to unlock it; someone who looks like you can unlock the device; or someone can hold up the device in front of you to unlock it if your eyes are open.

Figure 18-12

(A) Screen lock options on an Android smartphone; (B) Smart Lock exceptions to keep the screen unlocked



3:42

Security

SECURITY STATUS

Google Play Protect
Apps scanned yesterday at 12:50 PM

Security update
July 5, 2021

Find My Device
On

Google Play system update
August 1, 2021

DEVICE SECURITY

Screen lock
Pattern

Fingerprint

Face unlock
Face unlock is on

Smart Lock

Device admin apps
No active apps

Advanced
Encryption & credentials, Trust agents, App pinning

3:40

Smart Lock

On-body detection
Keep your device unlocked while it's on you

Trusted places
Add location where device should be unlocked

Trusted devices
Add device to keep this one unlocked when it's nearby

Figure 18-12A shows screen lock options on an Android smartphone, including a pattern, fingerprint, and face lock. Android also allows the user to set exceptions to the screen lock, as shown in Figure 18-12B. Using these options, the smartphone might stay unlocked when it detects it's being carried, when it detects its location, such as the user's home or office, or when another trusted device is nearby. Android calls this feature Smart Lock.

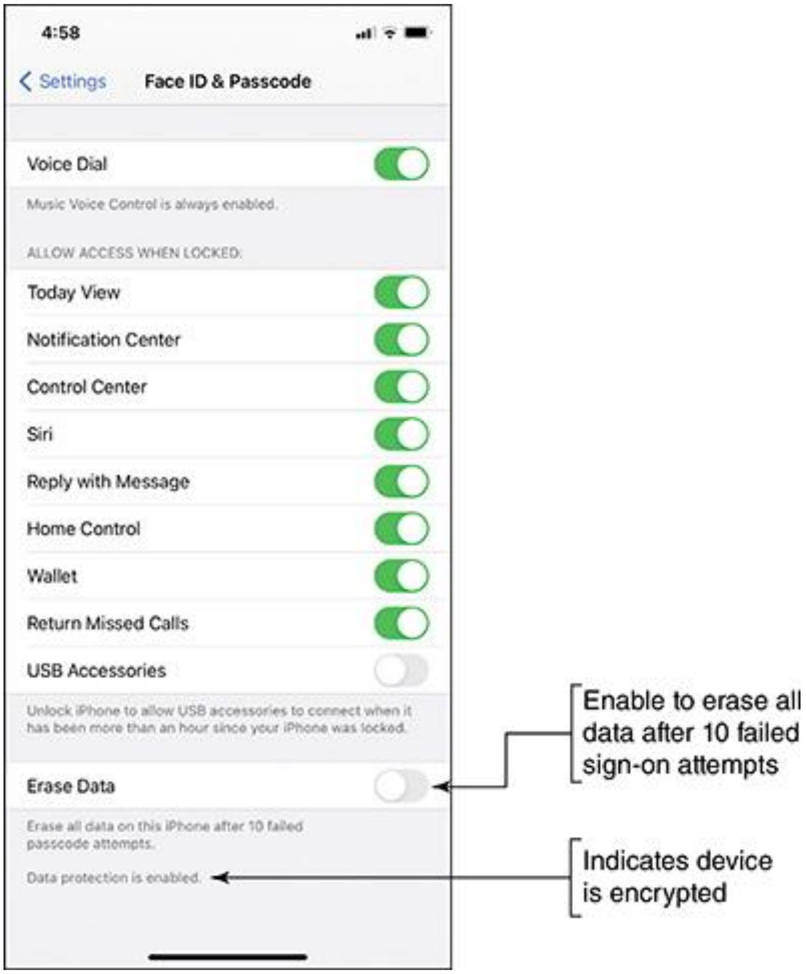
Note 3

Fingerprint and facial recognition are both forms of biometric authentication. Biometric authentication collects biological data about a person's fingerprints, handprints, face, voice, retina, iris, and handwritten signatures to confirm the person's identity. In some states, you cannot legally be forced to give your phone's password to investigators, but you can be required to give your fingerprint.

- **Restrict failed login attempts.** With Android devices, login attempt restriction options vary by manufacturer. With iOS, the device can be set to erase all data after 10 failed passcode attempts. See Figure 18-13. With each attempt, you must wait for a longer time before you can try again. If the device permanently locks and you've created a backup on a Mac or in iTunes in Windows, you can sync to the backup to access the phone. Otherwise, you'll have to use recovery mode, which erases the device.

Figure 18-13

Set iOS to erase all data after 10 failed attempts at sign-on



4:58

< Settings Face ID & Passcode

Voice Dial ☑

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Today View ☑

Notification Center ☑

Control Center ☑

Siri ☑

Reply with Message ☑

Home Control ☑

Wallet ☑

Return Missed Calls ☑

USB Accessories ☐

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data ☐

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

Enable to erase all data after 10 failed sign-on attempts

Indicates device is encrypted

Caution

If you set your device to erase data after repeated failed login attempts, be sure to keep backups of your data and other content. A small child could pick up your smartphone and accidentally erase all your data with just a few finger taps.

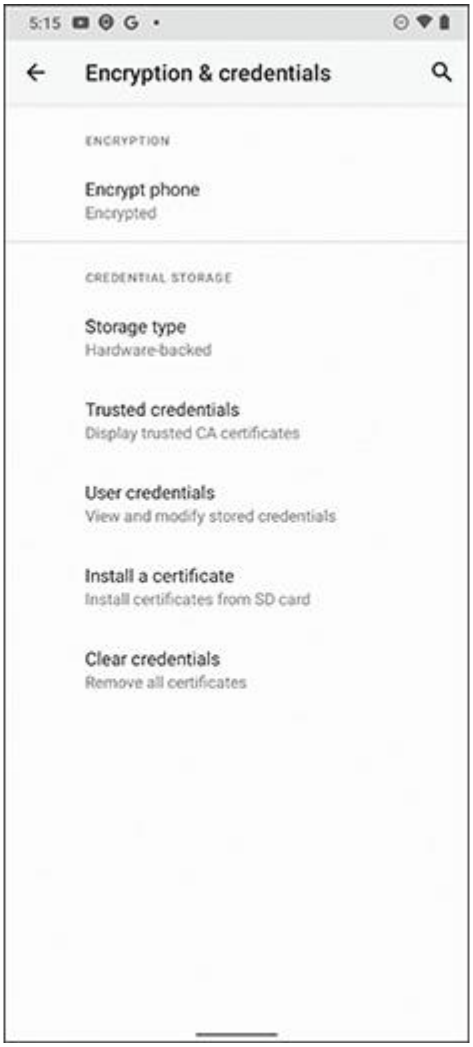
- **Full device encryption.** Both Android and iOS devices offer **device encryption**, which encrypts all the stored data on a device. Encrypting a device's stored data makes it essentially useless to a thief. However, encryption might slow down device performance, and data is only as safe as the strength of the password keeping the data encrypted. Also, data might be vulnerable again when it's being viewed or transmitted because device encryption only encrypts data while it's at rest or stored on the device, not when it's in motion or being transmitted.

  Most Android devices are encrypted by default. To know if the device is encrypted, look in **Settings**, tap **Security**, and then **Encryption &**

credentials (see Figure 18-14). For iPhones and iPads, data is encrypted whenever the device is secured with a passcode. Notice, near the bottom of Figure 18-13, *Data protection is enabled*, which indicates that all data is encrypted.

Figure 18-14

This Android device is encrypted



5:15

Encryption & credentials

ENCRYPTION

Encrypt phone
Encrypted

CREDENTIAL STORAGE

Storage type
Hardware-backed

Trusted credentials
Display trusted CA certificates

User credentials
View and modify stored credentials

Install a certificate
Install certificates from SD card

Clear credentials
Remove all certificates

18-2b Use Trusted Sources for Apps

Core 2 Objective

- 2.7

  Explain common methods for securing mobile and embedded devices.

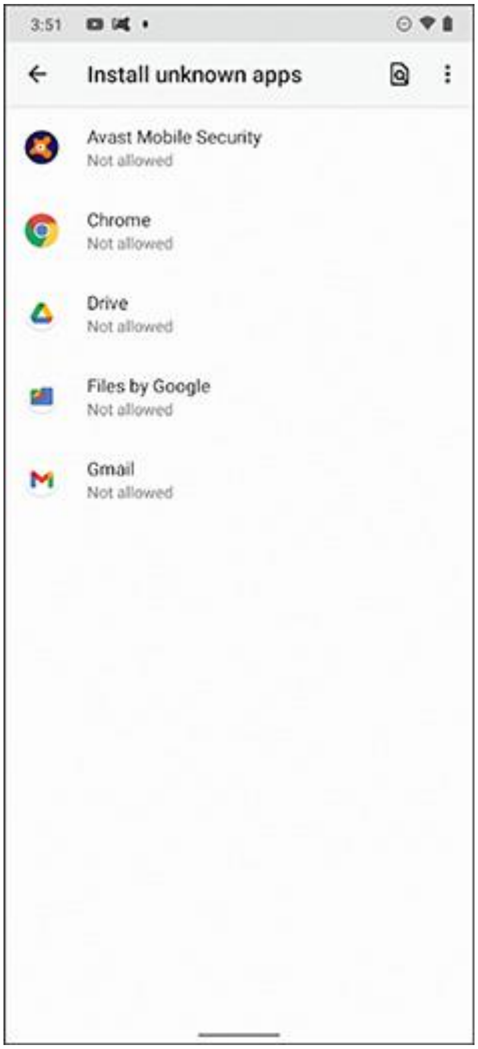
iOS devices are limited to installing apps only from Apple’s App Store. Android devices can download and install apps from other sources, only some of which are trustworthy. **Trusted sources** generally include Google Play Store (play.google.com) and other well-known app stores, such as

Amazon Appstore for Android (amazon.com/appstore), SlideME (slideme.org), your bank's website, your employer, or your school. Before downloading an app, look for lots of reviewer feedback as one measure of safety.

To reduce the threat of apps from untrusted sources, Android requires you to first proactively allow apps from untrusted sources before you can download and install them. To do that, go to **Settings**, **Apps & notifications**, **Advanced**, **Special app access**, and **Install unknown apps** (see Figure 18-15). Select an app, and choose **Allow from this source**. If you decide to use third-party app sources, be sure you already have a good anti-malware program and a firewall running on your device.

Figure 18-15

Choose which apps can install apps from unknown sources



Install unknown apps

Avast Mobile Security
Not allowed

Chrome
Not allowed

Drive
Not allowed

Files by Google
Not allowed

Gmail
Not allowed

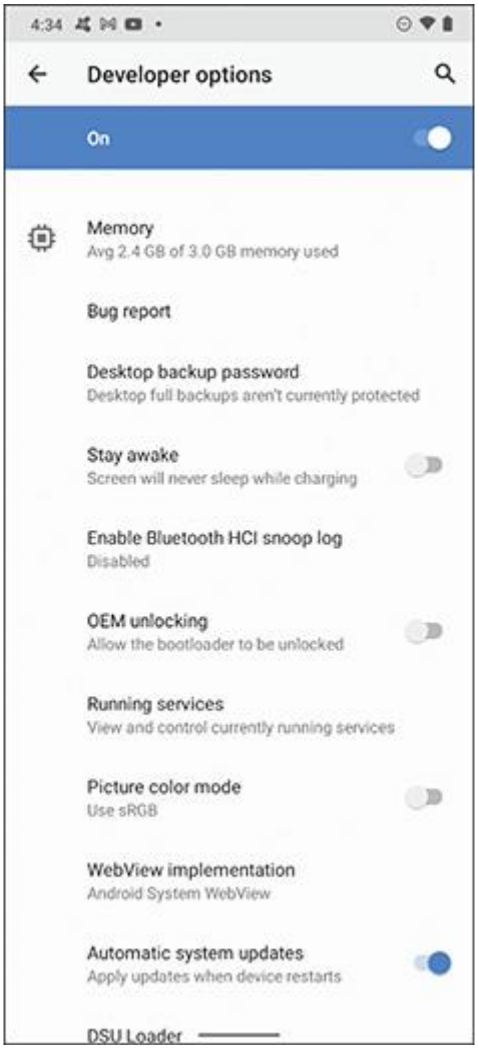
One reason you might want to install an app from an unknown source is when you're developing and testing an app not yet ready for distribution. An Android app developed using Android Studio is compiled into a collection of software files called an **Android package (APK)**, sometimes called an Android package kit, and the APK file has an .apk file extension. When you download an app from Google Play, you download an .apk file, and then Android installs the app on your device. In addition, you can download and install .apk files from any source when your device is set to allow this, a process called sideloading the app.

Security Threats in Developer Mode

You can use Developer mode on your Android device to test and debug apps you are building. Android hides Developer mode by default. To enable it, go to **Settings**, **About phone**, and tap **Build number** seven times. To see the Developer screen, in **Settings**, go to **System**, **Advanced**, and **Developer options.** Notice on the Developer options screen (see Figure 18-16) you can turn Developer options on or off and set many functions in Android designed to test and debug apps.

Figure 18-16

Developer options used to test and debug Android apps



4:34

Developer options

On

Memory
Avg 2.4 GB of 3.0 GB memory used

Bug report

Desktop backup password
Desktop full backups aren't currently protected

Stay awake
Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Disabled

OEM unlocking
Allow the bootloader to be unlocked

Running services
View and control currently running services

Picture color mode
Use sRGB

WebView implementation
Android System WebView

Automatic system updates
Apply updates when device restarts

DSU Loader

Users sometimes turn on Developer mode so they can use an option, such as Force 4x MSAA to improve image quality in a game or enable USB Debugging so a backup app or other type of app on their computer can interface with the Android device over a USB connection. This last option might pose a security threat if an app on the computer is malicious.

Security Threats from Root Access, Jailbreaking, and Bootlegged Apps

To get more control over what can be done with an Android or iOS device, including downloading and installing **bootlegged apps** (illegal apps), some users have discovered they can get root or administrative privileges to the OS and the entire file system (all files and folders), and complete access to all commands and features. For Android, the process is called **rooting**, and for iOS, the process is called **jailbreaking**. After jailbreaking, an iOS phone can get apps from any source, but Apple has the right to void the warranty or refuse to provide support. Rooting and jailbreaking might also violate BYOD policies in an enterprise environment. In addition, rooting or jailbreaking makes a device more susceptible to malicious apps and hackers using a technique called **application spoofing** to present to a user an app pretending to be a legitimate app the user wants when, in fact, it is malicious.

Applying Concepts

Rooting and Jailbreaking

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 3.5

Here is how you can tell if a device is rooted or jailbroken:

- **Rooted Android device.** Use one of these methods to find out if an Android device has been rooted:
  - Download and run a root checker app from Google Play; this will tell you if the device is rooted.
  - Download and run a terminal window app from Google Play. (A terminal window in Linux is similar to a command prompt window in Windows.) When you open the app, look at the command prompt. If the prompt is a #, the device is rooted. If the prompt is a $, the device is likely not rooted. With the $ prompt showing, enter the **sudo su root** command, which in Linux allows you root access. If the prompt changes to #, the device is rooted.
- **Jailbroken iOS device.** To find out if an iOS device has been jailbroken, look for an unusual app on the home screen—for example, the Electra, Meridian, Cydia, or Sileo app. If any of these apps is present, the device has been jailbroken. If you have any app icon on your home screen that is not available in the App Store, the app is most likely a jailbreak app or other malware. When you update iOS or perform a factory reset, the jailbreak will be removed. How to do that is covered later in the module.

Note 4

In Linux, the # command prompt displays when a user has root access, and the $ command prompt displays when a user does not.

18-2cMobile Security in Corporate Environments

Core 2 Objectives

- 2.1

  Summarize various security measures and their purposes.
- 2.7

  Explain common methods for securing mobile and embedded devices.

Recall from the Core 1 module “Supporting Mobile Devices” that corporations and schools might provide corporate-owned devices, which are secured and managed by corporate policies and procedures, or the organization might have BYOD policies and procedures that allow an employee or student to connect their own device to the corporate network.

Regardless of who owns the device, mobile device management (MDM) software downloads and enforces a security profile to the device before allowing it to connect to the network. A **security profile**, sometimes called a work profile, is a set of policies and procedures to restrict how a user can access, create, and edit the organization’s resources. Profile security requirements can include full device encryption, backups, remote wipes, location apps, access control, authenticator apps, multifactor authentication, firewalls, anti-malware measures, and use of VPN connections. All requirements must be clearly outlined with assurance that devices continue to meet the baseline requirements, and users must be educated on how to use them.

Note 5

To find out if an Android device has a corporate security profile installed, open **Settings**, go to **Accounts**, and look for a Work section. A passcode is required to access the section. If you don’t see a Work section, the device does not have a security profile installed. When the device has a security profile, you must enter a passcode to access the profile or enter one to access corporate apps on the device. A corporate app has a briefcase icon.

After an iOS device receives the download from the MDM server, apps on the device that belong to the corporation, called managed apps, are accessed via a passcode.

Although Google and Apple offer free or inexpensive backup services for their OSs, security profiles might require installing a **remote backup application**, which remotely backs up the device's data to the company's secured cloud storage. These apps might also sync files both directions and provide support for larger files. For example, Acronis Cyper Backup (acronis.com) provides enterprise-level backups for Windows, macOS, iOS, and Android devices.

18-3Troubleshooting Mobile Devices

Core 2 Objectives

- 3.4

  Given a scenario, troubleshoot common mobile OS and application issues.
- 3.5

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

When learning to troubleshoot any OS or device, remember the web is a great source of information. Depend on the support.google.com/googleplay and support.apple.com websites to give you troubleshooting tips and procedures for their respective mobile devices. In this section, we'll first explore troubleshooting tools for mobile device OSs, and then we'll consider several common symptoms and problems and what to do about them.

18-3aTroubleshooting Techniques

Core 2 Objectives

- 3.4

  Given a scenario, troubleshoot common mobile OS and application issues.
- 3.5

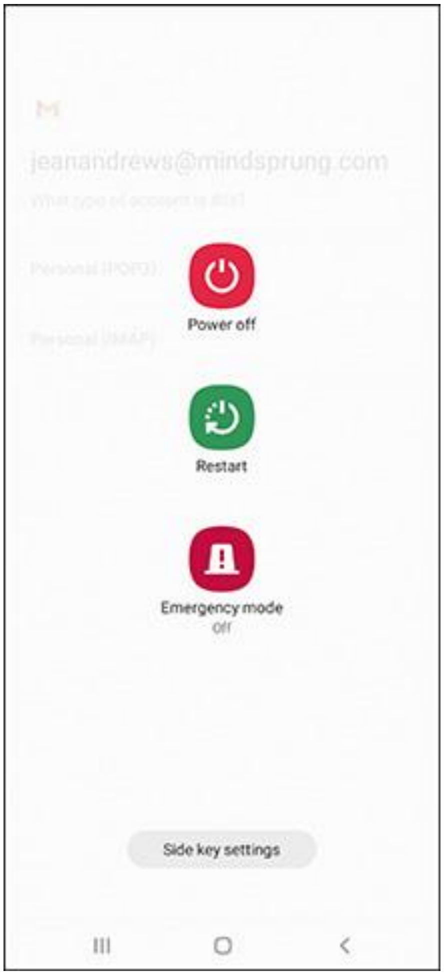
  Given a scenario, troubleshoot common mobile OS and application security issues.

In the Core 1 module "Supporting Mobile Devices," you learned several techniques for troubleshooting mobile devices. In this module, we review these techniques and add some more. The following steps are ordered to solve a problem while making the fewest changes to the system (i.e., try the least invasive solution first). Try the first step; if it does not solve the problem, move on to the next step. With each step, first make sure the device is plugged in or already has sufficient charge to complete the step. After you try one step, check to see if the problem is solved before you move on to the next step. Here are the general steps we're following, although some might not be possible, depending on the situation:

1. **Close, uninstall, and reinstall an app.** If you suspect an app is causing a problem, uninstall it and use the app store to reinstall it.
2. **Restart the device (also called a soft boot).** Recall to restart an Android device, press and hold the power button, and select **Restart**. See Figure 18-17. To restart an Apple device, press and hold the side or top button, and slide the power-off message to the right.

Figure 18-17

Restart or power-off an Android device



3. **Reboot the device (also called a hard boot).** For most Android devices, hold down the power button to see the menu shown in Figure 18-17, and tap **Power off** twice. If that doesn't work, try holding down the power button and the volume-down button at the same time. (Check Android device manufacturers for details.) To reboot an iPhone or iPad, hold down the side or top button and the volume-down button at the same time until the Apple logo appears. (For older iPhones and iPads, press and hold the side or top button and the Home button.)
4. Update, repair, or reinstall the OS, or recover the system from the last backup.

5. Start over by resetting the device to its factory state (all data and settings are lost).

Let's look at the last two steps in a little more detail. For more specific instructions, search the website of the device manufacturer.

Note 6

If the device has a removable battery and it refuses to hard boot, you can open the back of the device and then remove and reinstall the battery as a last resort (unless the device is under warranty).

Update, Repair, or Restore the System

As you progress through troubleshooting steps, try these options to update, repair, or restore a device:

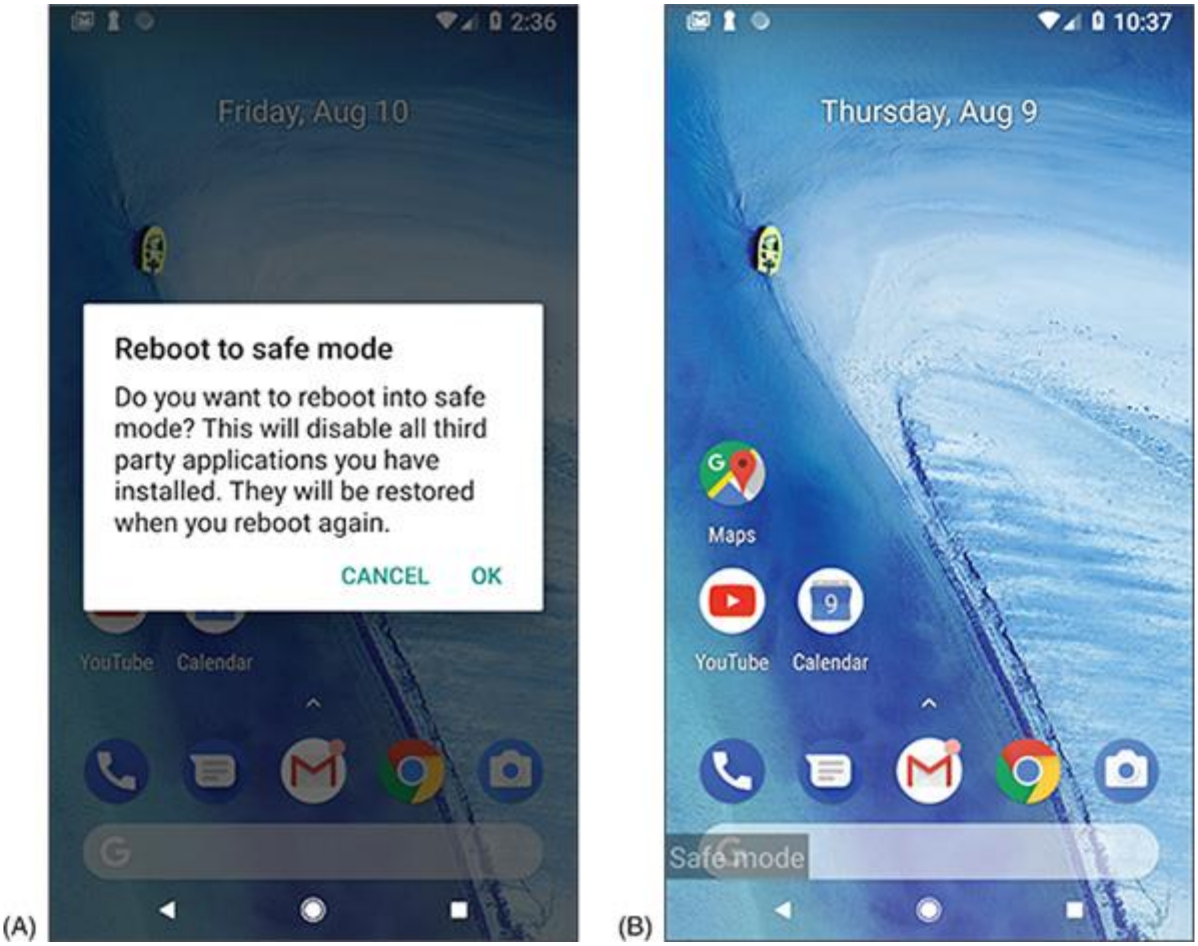
1. **Back up content and settings.** Before you try any of the techniques in this section, first try to back up data and settings using one or more of the methods discussed earlier in the module.
2. **Update the OS.** Try installing any updates, if available.

For Android devices, you can try these options to repair and restore your system:

1. **Boot into Android Safe Mode.** Similar to Windows computers, Android offers a Safe Mode for troubleshooting. In Safe Mode, only the original software installed on the phone will run so that you can eliminate third-party software as the source of the problem. However, be aware that booting to Safe Mode might result in the loss of some settings, such as synched accounts. The combination of buttons to access Safe Mode varies by device, so see the manufacturer's website for specific instructions. For Google's Pixel smartphone, you access Safe Mode by holding down the power button until the power menu appears. Tap and hold the **Power Off** option until the pop-up shown in Figure 18-18A appears. Tap **OK** to restart the phone in Safe Mode, as shown in Figure 18-18B. Notice the *Safe mode* flag at the bottom of the screen. In Safe Mode, only apps native to the Android installation can run, and troubleshooting tools can be accessed through the Settings app to back up data, test configuration issues, or reset the device. To exit Safe Mode, restart the phone normally.

Figure 18-18

(A) Restart in Safe Mode; (B) in Safe Mode, third-party apps don't load



Reboot to safe mode

Do you want to reboot into safe mode? This will disable all third party applications you have installed. They will be restored when you reboot again.

CANCEL OK

2. **Restore from backup.** If you have used Google Drive or a third-party app to back up the Android OS, its data or settings, now is the time to restore the system from this backup.

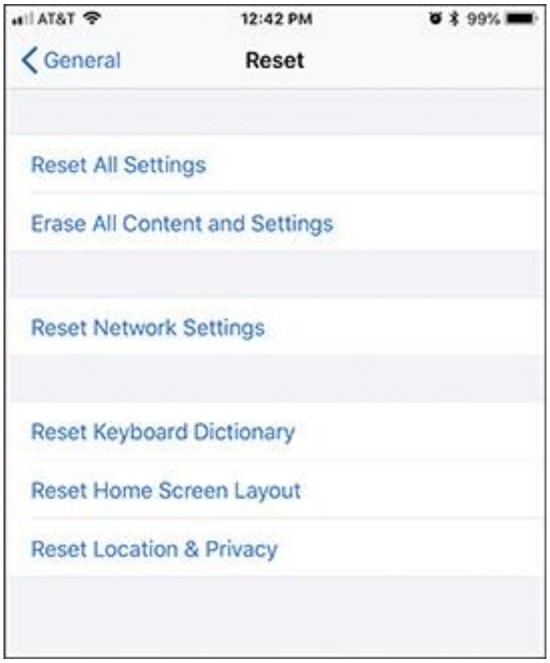
Several troubleshooting apps have been developed to help resolve Android problems. Most of these apps work only if they have already been installed before the problem occurs. If you have not already installed a troubleshooting app, your best resource at this point is to do a Google search on the problem and depend as much as possible on the device manufacturer's website.

For iOS devices, you have several options for repairing and restoring your system, which are listed beginning with the least invasive:

1. **Reset all iOS settings.** To erase settings, open the **Settings** app and tap **General** and then **Reset**. On the Reset screen (see Figure 18-19), tap **Reset All Settings**.

Figure 18-19

The reset screen on an iPhone



2. **Restore from backup.** Use one of these methods to restore from backup:

    - **Restore the device from iCloud.** If you have an iCloud backup, open the **Settings** app and tap **General**, **Reset**, and **Erase All Content and Settings** (see Figure 18-19). Then tap **Restore** and **iCloud backup**. You'll need to sign in to iCloud.
    - **Restore the device from a Mac or from iTunes in Windows.** If you have used a Mac or iTunes in Windows to back up the device, connect the device to your computer, start Finder on the Mac or iTunes in Windows, and click **Restore iPhone**. Refer back to Figure 18-6.

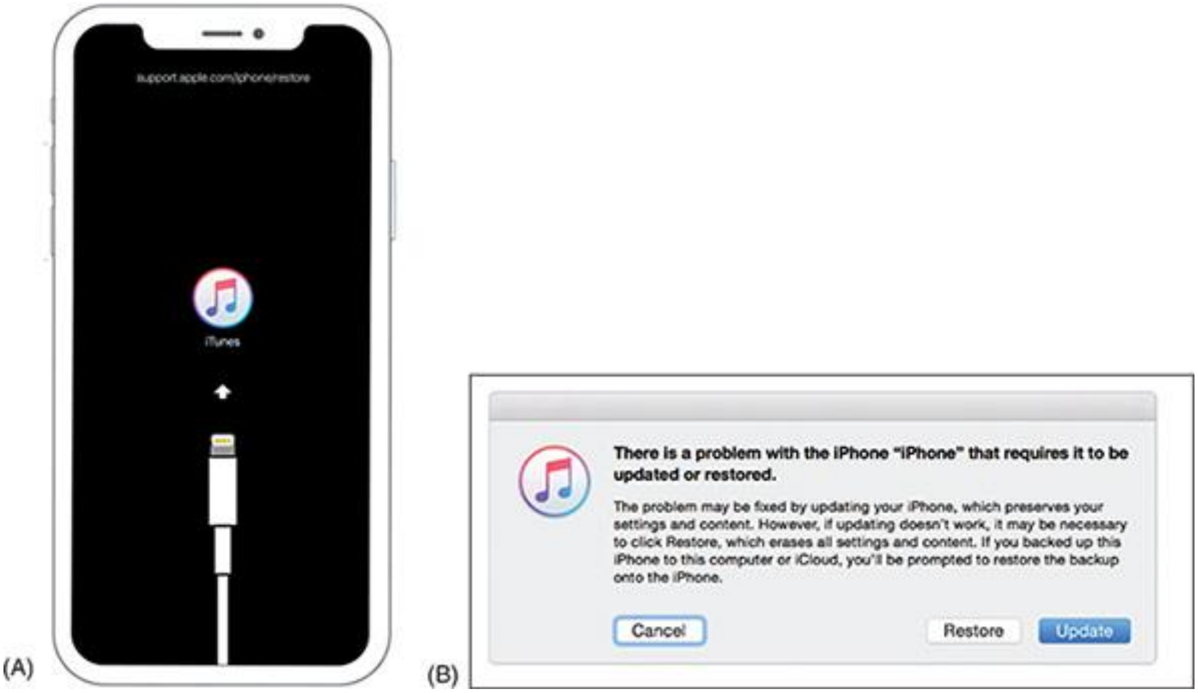
3. **Reinstall iOS.** If an iOS device won't turn on or start up, first consider that the battery might be dead. Try to charge it for at least an hour. If you still can't turn it on, you can use a Mac or iTunes in Windows to try to reinstall iOS without losing your data. (You can use any Mac or iTunes on any Windows computer, even if you have not previously used it to back up your device.)

    - If necessary, download and install iTunes. Make sure iTunes is updated, and then close it.
    - Connect the iPhone or iPad to the computer and start the Mac Finder or iTunes in Windows. Check the Apple website (support.apple.com) for the correct keys to press to put the device in Recovery Mode. For iPhone 8 or later, press and release the volume-up button followed by the volume-down button, and then press and hold the Slide button until you see the Recovery Mode screen (see Figure 18-20A). For newer iPads, press and hold the top button and volume down button at

the same time. For older iPhones or iPads, press and hold the power button and volume down button at the same time. Follow the directions until you see the screen shown in Figure 18-20B, and then click **Update**. The latest version of iOS that works on your device should install, keeping your existing data.

Figure 18-20

Use Recovery Mode on a Mac or with iTunes in Windows to reinstall iOS on an iOS device that will not start



There is a problem with the iPhone "iPhone" that requires it to be updated or restored.

The problem may be fixed by updating your iPhone, which preserves your settings and content. However, if updating doesn't work, it may be necessary to click Restore, which erases all settings and content. If you backed up this iPhone to this computer or iCloud, you'll be prompted to restore the backup onto the iPhone.

Start Over with a Factory Reset

As a last resort, you can perform a factory reset. The reset erases all data and settings and resets the device to its original factory default state. You can then apply a backup if you have one, so try to back up all data and settings before performing the reset, if possible. Here are your options:

- **Factory reset from the Settings app.** In Android, open the **Settings** app, tap **System**, tap **Advanced**, tap **Reset options**, and then tap **Erase all data (factory reset)**. In iOS, open the **Settings** app, and then tap **General** and **Reset**. On the Reset screen, tap **Erase All Content and Settings**.
- **Factory reset from a hard boot (Android only).** If you cannot start Android or cannot get to the Settings app after a reboot, you can perform a factory reset from a hard boot. For most Android devices, hold down the power button and volume-down button at the same time until you see the Android bootloader menu. Select **Recovery**

Mode, and then check the device manufacturer's website for other options on the Recovery Mode screen that you can try before a full factory reset. If you decide that you have no other options, select **Factory reset** on the Recovery Mode screen.

- **Factory reset and restore from a Mac or iTunes backup (iOS only).** If an iOS device won't turn on and you've already tried to reinstall iOS using a Mac or iTunes in Windows, as discussed earlier, you can use the computer to perform a factory reset. Connect the device to a Mac or Windows computer with iTunes installed, and then put the device in Recovery Mode, as you learned to do earlier. Then click **Restore** (see Figure 18-20B). All data and settings on the device are erased, and iOS is reinstalled. If you have previously used this computer to back up your device, the device is restored from the backup. If you have an iCloud backup, you will be given the opportunity to restore from iCloud the first time you sign on to the device with your Apple ID.

Note 7

If you have backed up to iCloud and you sign into iOS for the first time with your Apple ID on a new or factory reset device, you are given the chance to restore the device from the iCloud backup.

If you've tried the previous steps and your device is still not working properly, search for more troubleshooting tips online, review the list of common problems in the next section, or take the device to the place of purchase for repair.

18-3bCommon Problems and Solutions

Core 2 Objective

- 3.4

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

Several common problems with mobile devices can be addressed with a little understanding of what has gone wrong behind the scenes. Here's a description of how to handle some common problems:

- **Short battery life or power drain.** Too many apps or malware running in the background will drain the battery quickly, as will Wi-Fi, Bluetooth, or other wireless technologies. Disable wireless connections and close apps when you're not using them to save battery juice. Consider that malware might be at work. If the battery charge still lasts an extremely short time, try exchanging the charger cable. If that doesn't work, exchange the battery unless the device is under warranty. Many Android devices have replaceable batteries, so if a battery is performing poorly, consider replacing it.

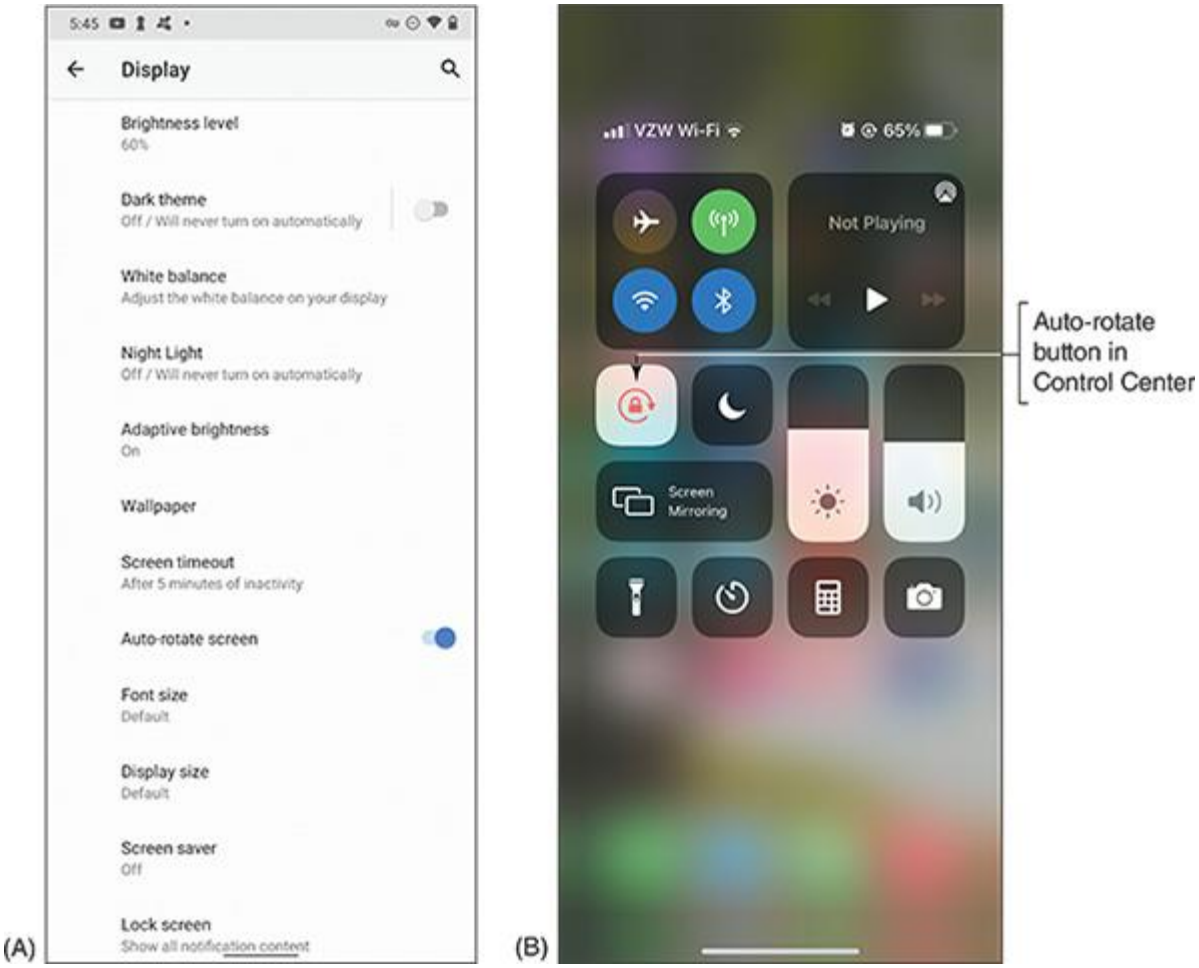
Core to Core

How to deal with malware on mobile devices is covered in the Core 1 module "Supporting Mobile Devices."

- **Screen does not autorotate.** Try these things:
  - In the Android Settings app, check the Display screen to verify auto-rotate is turned on (see Figure 18-21A).
  - For Apple devices, swipe from the upper-right corner to open the Control Center (see Figure 18-21B), and check the auto-rotate button.
  - Don't touch the screen when you're rotating it.
  - Update the OS, and restart the device.
  - If you recently installed a third-party app when the touch screen became unresponsive, try uninstalling that app. Sometimes third-party apps can cause a touch screen to freeze.

Figure 18-21

Verify auto-rotate is turned on with (A) an Android phone and (B) an iPhone



5:45

Display

Brightness level
60%

Dark theme
Off / Will never turn on automatically

White balance
Adjust the white balance on your display

Night Light
Off / Will never turn on automatically

Adaptive brightness
On

Wallpaper

Screen timeout
After 5 minutes of inactivity

Auto-rotate screen

Font size
Default

Display size
Default

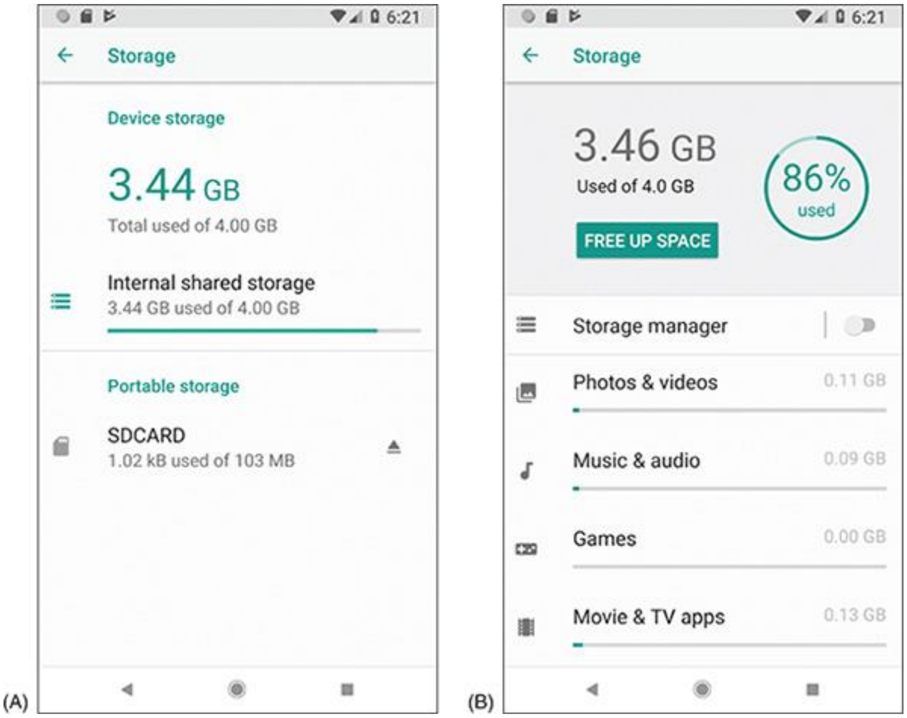
Screen saver
Off

Lock screen
Show all notification content

- **OS fails to update.** Try these things:
  - The OS might fail to update if there's not enough free space on the device to download and install the update. The Settings app on an Android device displays how much storage space is available (see Figure 18-22A) and what content can be removed (see Figure 18-22B). If free space is needed, try uninstalling some unneeded apps or moving some data to the cloud.

Figure 18-22

(A) Android reports how storage is used and (B) makes suggestions to free up some storage space



(A)

Storage

Device storage

3.44 GB

Total used of 4.00 GB

Internal shared storage
3.44 GB used of 4.00 GB

Portable storage

SDCARD
1.02 kB used of 103 MB

(B)

Storage

3.46 GB

Used of 4.0 GB

FREE UP SPACE

86% used

Storage manager

Photos & videos 0.11 GB

Music & audio 0.09 GB

Games 0.00 GB

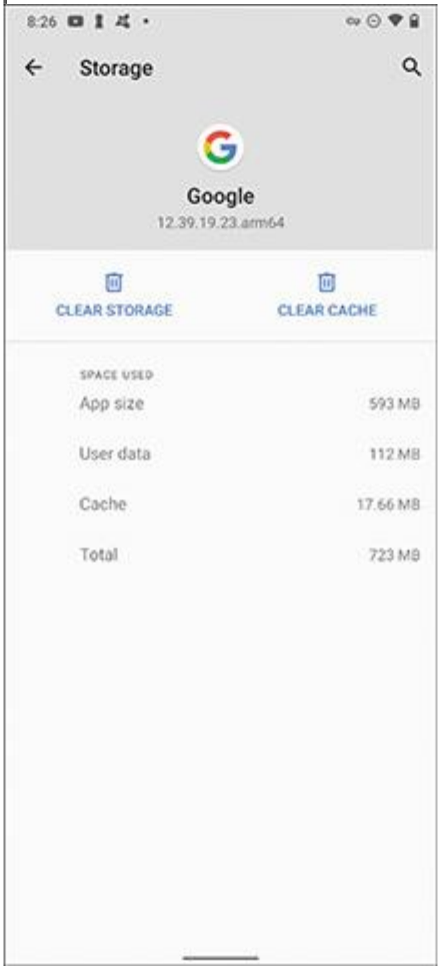
Movie & TV apps 0.13 GB

  - Make sure the battery is charged and the network connection is good.
  - Try a different network. Restart the device, and try again.
  - For iOS, you can try removing a failed update and updating the OS again. To remove an update, go to **Settings**, **General**, and **iPhone Storage**; tap the update; and tap **Delete Update**. Then try the update again. To use iTunes to update the OS, plug in the Apple device to your computer, open **iTunes** in Windows or Finder on a Mac, locate your device, and click **Check for Updates**. Refer back to Figure 18-6.
- **Apps fail to launch or are slow to respond.** Check and try these things:
  - When apps are slow to respond, slow to launch, or won’t launch at all, a hot or failing battery might be the problem. Having too many apps open at once will use up memory, which can also slow down overall performance. Close apps you’re not using, clean cached data, and disable live wallpapers.
  - Try to update the app, or uninstall it and install it again.
  - The device might be short on storage space; uninstall unused apps and delete files that are no longer needed.
  - Consider downloading an app to clean up storage space or monitor how apps are using memory.
  - Consider performing a factory reset, and start over by installing only the apps you actually use.

- **Apps crash, fail to close, or fail to update.** Apps might crash or fail to close or update when an app is corrupted, storage is low, or the Wi-Fi network or cellular signal is slow or unstable. Try these things:
    - Free up some storage, and try a different network.
    - Make sure the OS is up to date.
    - For Android apps failing to update, try clearing the Google cache: In Settings, go to **Apps & notifications**, **Google**, and **Storage & cache**, and tap **CLEAR CACHE**. See Figure 18-23. If the problem persists, force stop the Google app.

Figure 18-23

Clearing the Google cache might solve the problem of apps failing to update



12.39.19.23.arm64

SPACE USED

App size	593 MB
User data	112 MB
Cache	17.66 MB
Total	723 MB

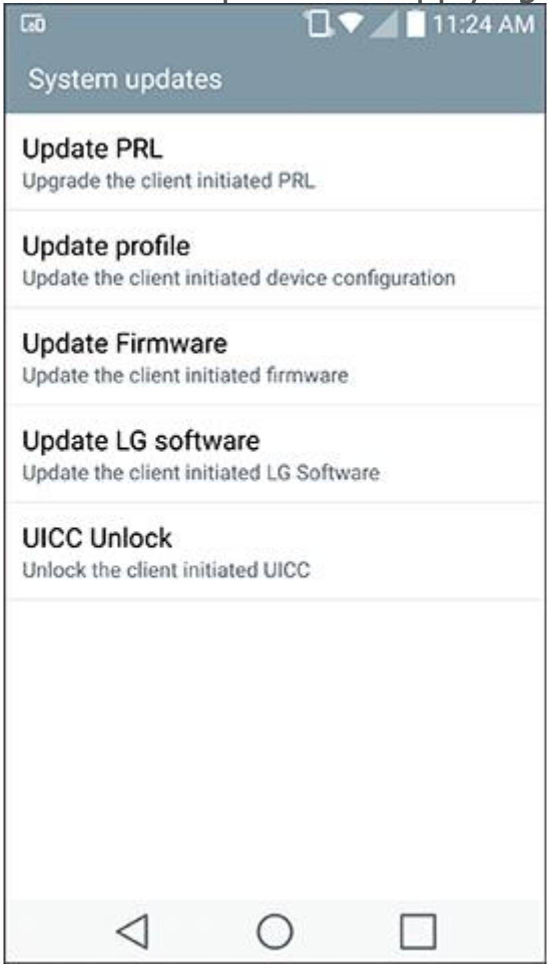
- **Random reboots.** Random reboots are usually caused by bad apps, overheating, corrupted OS, or defective hardware. First try uninstalling any suspected apps and updating the OS. For Android, go to the Play Store, and update all apps: Tap your profile icon, tap **Manage apps & device** and **Update all**. For iOS, in Settings, tap **App Store** and turn on **App Updates**.

How to deal with overheating is covered in the Core 1 module “Supporting Mobile Devices.”

- **Signal drop/weak signal.** Sometimes updating the device’s firmware can solve problems with dropped calls or network connections due to a weak signal because the update might apply to the radio firmware, which manages the cellular, Wi-Fi, and Bluetooth radios. This is sometimes referred to as a **baseband update**. For most of today’s mobile devices, firmware updates are pushed out by the manufacturer at the same time as OS updates. If your device allows for managing firmware updates separately, that option will usually be available in the Settings app (see Figure 18-24) in the same place as the OS update option. You might also be able to download firmware updates directly from the device manufacturer (for example, for LG devices, go to lg.com/us/support/software-firmware-drivers). Be careful when applying a firmware update because a failed update can “brick” the device, which means to make it useless.

Figure 18-24

This LG phone lists several options for applying updates



System updates

Update PRL
Upgrade the client initiated PRL

Update profile
Update the client initiated device configuration

Update Firmware
Update the client initiated firmware

Update LG software
Update the client initiated LG Software

UICC Unlock
Unlock the client initiated UICC

- **System lockout.** If a device is locked because of too many failed attempts to sign in (such as when a child has attempted to unlock your device or you have forgotten the passcode), wait until the timer on the device counts down, and try to sign in again. With Android devices, you might also be able to sign in using your Google account and the password associated with the device. After you have entered the account and password, you must reset your passcode or screen swipe pattern. If you still can't unlock the device, know that Google offers many solutions to this problem. Go to accounts.google.com, and search for additional methods and tools to unlock your device.

If you have forgotten the passcode for an iOS device, Apple advises that your only solution is to reset the device, which erases all data and settings, and then restore the device from a backup. You can restore from a backup stored on your computer or from iCloud.

Connectivity Issues

Connectivity issues might arise with Bluetooth, Wi-Fi, and NFC on both Android and Apple devices. You might also face issues with Apple AirDrop connections.

✓ Exam Tip

The A+ Core 1 and A+ Core 2 exams both expect you to know how to troubleshoot mobile device connectivity problems with Bluetooth, Wi-Fi, NFC, and AirDrop connections.

⇆ Core to Core

Connectivity issues with mobile devices are covered in the Core 1 module "Supporting Mobile Devices" and are not repeated in this module.

Security Concerns

Common symptoms that malware is at work on a device, indicating that the security features in place have been breached, include the following:

- Excessive power drain
- Sluggish response time
- Slow data speeds and high network traffic
- Unauthorized account access or leaked personal data or other data
- Strange text messages or phone calls
- High number of ads
- Data-usage limit notifications
- Fake security warnings
- Unexpected app behavior
- Limited or no Internet connectivity
- Dropped phone calls or weak signal
- Unintended Wi-Fi and Bluetooth connections
- Unauthorized use of camera or microphone

✓ **Exam Tip**

The A+ Core 1 and A+ Core 2 exams both expect you to know how to recognize malware might be at work on a mobile device and how to remove the malware.

⇆ **Core to Core**

How to recognize and remove malware is covered in the Core 1 module “Supporting Mobile Devices” and is not repeated in this module.

18-4a Module Summary

Backing Up Mobile Devices

- Currently, the most popular operating systems used on mobile devices are Android by Google and iOS and iPadOS by Apple.
- A mobile OS can be updated until it ages out of manufacturer updates based on end-of-life (EOL) limitations.
- Mobile apps are usually developed using development tools provided by Google and Apple in a software development kit (SDK).
- Backups for mobile data include file-level backups and full and partial image-level backups, which can be made to a local computer or to the cloud.

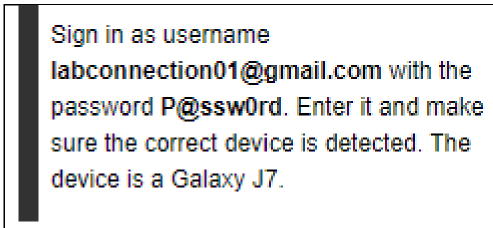
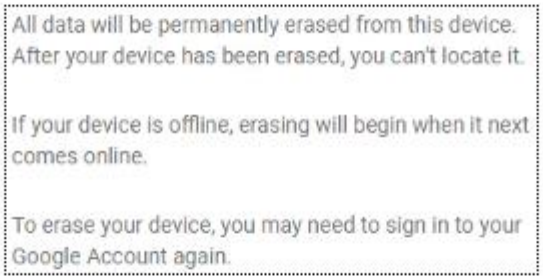
Securing Mobile Devices

- Secure mobile device data and resources by regularly updating and patching the OS, using an anti-malware app with the Android OS, implementing a firewall, configuring a locator app and the ability to remote wipe the device, and getting apps only from trusted sources.
- Control access to a mobile device by restricting failed login attempts, encrypting the device, and configuring a screen lock, such as a swipe lock, PIN lock, passcode lock, pattern lock, fingerprint lock, or face lock.
- Allowing root access to an Android device or jailbreaking an Apple device can expose the device to bootlegged apps, spoofing apps, or apps from untrustworthy sources.
- In corporate environments, a security profile might require the use of full device encryption, remote backups, remote wipes, access control to the device, authenticator apps, multifactor authentication, firewalls, anti-malware measures, and VPN connections to protect company resources on the mobile device.

Troubleshooting Mobile Devices

- To troubleshoot a mobile device using tools in the OS, you can close running apps, uninstall and reinstall an app, restart or reboot the device, update the OS, reset all settings (iOS only), use Safe Mode (Android only), use Recovery Mode and restore from backup, or perform a factory reset.

- To address specific, common symptoms on a mobile device, you might need to replace the battery if it's not under warranty, adjust device settings, update the OS, uninstall or update problem apps, free up space on the device, clear the Google cache, update firmware, reset the device, or consult with tech support for the device manufacturer or app.
- Symptoms of malware on mobile devices include excessive power drain, slow performance, slow data speeds, high network traffic, leaked personal files or data, data transmission over limits, strange text messages or phone calls, signal drops, weak signal, unintended Wi-Fi connections, unintended Bluetooth pairing, unauthorized account access, unauthorized location tracking, and unauthorized camera or microphone activation.

 Sign in as username **labconnection01@gmail.com** with the password **P@ssw0rd**. Enter it and make sure the correct device is detected. The device is a Galaxy J7.	 All data will be permanently erased from this device. After your device has been erased, you can't locate it. If your device is offline, erasing will begin when it next comes online. To erase your device, you may need to sign in to your Google Account again. Google.com/android/find

Which of the following is the best reason to replace a mobile device with a new one in a corporate environment?

○ a. The device has only a single camera, and MDM requires a minimum of two cameras for two-factor authentication.

○ b. The device does not have an SD card slot required for MDM management tools.

○ c. The latest version of Android the device can support has reached its EOL limitation.

○ d. The device will not update to the latest version of Android.

An app that cost you $4.99 is missing from your Android. What is the best way to restore the missing app?

○ a. Go to backup storage and perform a restore to recover the lost app.

○ b. Go to the Play Store where you bought the app and install it again.

○ c. Go to the Settings app and perform an application restore.

○ d. Purchase the app again.

Suppose you and your friend want to exchange lecture notes taken during class. Your friend has an iPhone, and you have an iPad. What is the easiest way to make the exchange?

○ a. Copy the files to an SD card, and move the SD card to each device.

○ b. Send a text to each other with the files attached.

○ c. Drop the files in OneDrive, and share notebooks with each other.

● d. Transfer the files through an AirDrop connection.

You have set up your Android phone using one Google account and your Android tablet using a second Google account. Now you would like to download the apps you purchased on your phone to your tablet. What is the best way to do this?

○ a. On your tablet, set up the Google account that you used to buy apps on your phone, and then download the apps.

○ b. Buy the apps a second time from your tablet.

○ c. Back up the apps on your phone to your SD card, and then move the SD card to your tablet and transfer the apps.

○ d. Call Google support and ask them to merge the two Google accounts into one.

What is one effective way to implement a VPN connection on your Android device?

○ a. Enable Android Firewall in the Settings app on your device.

○ b. VPN connections are not important to secure the device because all Wi-Fi and cellular transmissions are encrypted in Android.

○ c. Install a firewall app that includes a VPN connection in its services.

○ d. Subscribe to a website service that provides mobile device firewalls.

Before allowing apps from untrusted sources to be installed on your Android device, what should you do? (Choose all that apply.)

○ a. Install a firewall app.

○ b. Install an anti-malware app.

○ c. Use Android settings to allow apps from untrusted source.

○ d. All of the answers are correct.

Android apps are contained in an Android package kit, which has what file extension?

○ a. .and

○ b. .apk

○ c. .exe

○ d. .apx

What is a potential security risk when enabling Developer mode in Android?

○ a. Malicious software might reach your device when it is connected to a computer via a USB cable.

○ b. Android updates can install without your knowledge.

○ c. A video game might contain malware that can reach the Android root level of your mobile device.

○ d. Malicious software can easily download and install from the web without your knowledge.

How can you configure an iPhone so it can download and install any app from any website on the Internet?

○ a. Go to the Apps Store, and download and install the AllApps app.

○ b. Go to Settings, General, and then set the iPhone to allow apps from untrusted sources.

○ c. Use an app to jailbreak the iPhone.

○ d. Use Finder on a Mac computer to reset the iPhone.

When is it appropriate to use iTunes to restore an iPad from backup?

○ a. When the backup has been created on a Windows computer

○ b. When the backup has been created on a Mac computer

○ c. When the backup has been created in iCloud

○ d. All of the answers are correct.

Where is the biometric data for an Android facial recognition lock or fingerprint lock kept?

○ a. On the Android device and in the cloud

○ b. Only on the Android device

○ c. On the Android device and with any backups of data

○ d. Only in the Google cloud

Which of the following are true about Android Safe Mode? (Choose all that apply.)

☑ a. Only apps native to the Android installation can run in Android Safe Mode.

☑ b. A Safe Mode flag displays somewhere on the screen.

☑ c. Safe Mode helps you eliminate third-party apps as the source of a problem.

☑ d. To exit Safe Mode, restart the device normally.

Your friend has an iPhone that refused to start, and you helped them use a Mac computer to perform a factory reset. They had previously backed up the phone to iCloud. How do you instruct your friend to restore the phone from the iCloud backup?

○ a. Turn the phone on, and set it up without the backup. After the phone is operational, use the Settings app to restore from backup.

○ b. Turn on the phone, enter their Apple ID, and step through the questions to restore the phone from the iCloud backup.

○ c. Take the phone to an Apple service center, and ask them to help restore the phone from the iCloud backup.

○ d. Reconnect the phone to the Mac computer, and use the Finder window to restore the phone from the iCloud backup.

What is the most effective thing you can do to prevent a mobile device battery from draining too quickly?

○ a. Close the browser app.

○ b. Turn off Wi-Fi when Wi-Fi is not available.

○ c. Enable airplane mode.

○ d. Turn off your mobile hotspot.

A friend is having problems with their iPhone randomly rebooting. When you examine the phone, you notice the Cydia app installed. What do you recommend your friend try first to fix the problem?

○ a. Update the OS to eliminate the jailbreak.

○ b. Restore the iPhone to factory state to remove the malware.

○ c. Restore the iPhone to factory state to eliminate the jailbreak.

○ d. Update the Cydia app to eliminate the random reboots.

Exercise 1 - Securing a Mobile Device

Mobile devices may contain sensitive data of a user. It is essential that the mobile device is secured to prevent the device from being accessed when lost or stolen.

Different features are available that can be enabled to lock the device.

These methods include:

- Facial recognition
- PIN codes
- Fingerprint
- Pattern
- Swipe

In this exercise, different methods will be explored for securing a mobile device.

Task 1 - Exploring the Screen Lock Feature for a Mobile Device

A screen lock feature is available on most mobile devices to ensure there is no unauthorized access to a device.

Note: *Adding a password to the lock screen of the device will ensure that unauthorized users can not access the device if the device is lost or stolen*

Note: *Selecting the* ***Hide sensitive content*** *option will ensure that when the device is locked, it will not display any notifications such as messages or emails on the lock screen, protecting the user's privacy.*

Note: ***A password was set for the screen lock of the device. There are different options available for the screen lock feature. This includes Swipe where the screen is locked by swiping to the left or the right of the screen to lock the device. This method will not secure the device and only lock or unlock it. The other two options are*** *Pattern* ***or*** *PIN,* ***where the device can be unlocked by a PIN specified by the user or a specific pattern on the device's lock screen.***

Task 2 - Explore Additional Security Settings for a Mobile Device

Several additional security features are available to secure a mobile device when lost or stolen.

Note: ***The*** *Play Protect* ***feature can be used to scan the device for malicious applications, thus protecting the data on the device.***

Note: ***It is essential to keep the operating system of a mobile device up to date to ensure the latest security patches are installed on the device. If it is not updated regularly, the device will become vulnerable to cyber security threats.***

Note: ***Due to restrictions in the lab environment, the location for the mobile device can not be enabled. In a real-world scenario, the device's location will be enabled, which can then be used to determine its location if it is lost or stolen. Enabling this feature will also ensure applications on the device can use the location of the device to enable specific features for the applications.***

Note: ***Due to restrictions in the lab, the encryption of the device is not possible. In a real-world scenario, a mobile device's hard drive can be encrypted to prevent unauthorized access if the device is lost or stolen.***

Which one of the following Screen lock options is not secure?

○ PIN

○ Swipe

○ Password

○ Pattern

What is the reason for encrypting a mobile device's hard drive? [Choose all that apply]

□ Prevent unauthorized access to the data on the device

□ Prevent the device from being unlocked with a password or PIN

□ Prevent the device's hard drive from being accessed when lost or stolen

□ Prevent the access to the location of the device when lost or stolen

Which mobile security feature ensures that the device will not be vulnerable to attacks?

○ Location

● Security Update

○ Lock Screen

○ Encryption

Exercise 1 - Mobile OS and Application Issues

As more and more people are using cross mobile devices, it means that you as IT professional will have to actually learn a little bit more about it. Let's find out what we need to do next.

Welcome back to our show. We are now diving into the realm of mobile operating systems and application issues.

And this is a little bit trickier than what we would normally see in terms of regular desktops or even laptops. Because we're now moving into this realm where West, there's so many different manufacturers out there and all of the actual operating systems seem to be a little bit different.

But there are still some things that actually united together, but we'll still find issues that we have to deal with, right?

Most definitely, and that's a good point. We talk about Android, we talk about iOS, we talk about the iPad OS, just a variation on iOS, right?

But when it comes down to it at the end of the day, when you look at Android, Android is the one that has a little bit more modularity into it. And the fact that people who release it out on their devices, they might make slight modifications to it and things might be just called a little bit different.

But for the most part, you're gonna see that a lot of the settings that you're gonna find when it comes to troubleshooting OS issues and application issues, for the most part are gonna be in the same location, even if they're just named slightly different. So we're gonna look at our Android devices, we're gonna talk a little bit about some of the things that we need to be able to troubleshoot when it comes to applications and some of those issues.

All right, so West let's go ahead and divide this up and let's begin with different application issues. What we normally talking about there?

All right, sure, so when it comes to application issues, right, one of the things that we want our end users at the end of the day wanna be able to do is they wanna be able to use their devices.

And they wanna be able to use the applications that are on those devices, whether it means that they can use them at work or they can use them while they're traveling, there can be a variety. So one of the first things we'll tackle is, let's start talking about some of these application issues and some of the different types of application issues that you could encounter, right?

Again, these are more of the common ones. Remember, it's not a completely exhaustive list and I always encourage you to study more and study so that you can be successful. So one of the first ones that we have is what's known as a fails to launch, right? If try to launch an application and that application doesn't launch, it fails to launch, there are a couple of things that you can do.

One of the things that might actually happen is the application itself might be disabled. Other things to keep in mind is the fact that you have permissions that are required for certain applications functionality to work. And if an application doesn't work, let's say for one that uses location data, and that's its primary permission that you need but you disable that, the application will not launch and it will not be able to work.

Or the permissions could be blocked too, right? So in Android we have a couple of different types, right, of when we allow these permissions. We actually have what's known as privileged bracketing where we could say, hey, allow it this time, when the application's working, all the time. Or maybe it came up and you said, I don't use that application, we said block it.

Well, at that point the application is not gonna work again. So let me show you enough talking about this, let's look at our applications. We're in our Android phone right here, and what we're gonna do is we're gonna get into our Settings. And I want you to look at the App location, right?

You can scroll down and you can see a variety of different things here in Settings. But I want you to look at apps itself because the apps give you the ability to view the application permissions, right? And some of the permissions and also gather some information about the applications as well.

So for instance, let's see if there's any permissions associated with calculator. Well, it doesn't look like we have much here in the use or permissions, no permissions are required. But notice if I choose disable, the calculator is not gonna launch, right? But this one doesn't have any permission.

So let's go ahead, and I have let's see if DevInfo is in here somewhere. There we go, DevInfo I know it because it requires to be able to look down into your operating system and check your hardware. So you can see that there are certain level permissions, right?

I have denied this application permissions here. So if this application does need permissions and no permissions are allowed, then its functionality, it might cause it not to launch. So that's one of the things Ronnie and those are some of the things that you can do when it comes to maybe modifying the permissions to ensure that it does work appropriately.

Right now, West sometimes, even though it's not the idea here that it won't launch, but what if an application just stays open and it fails to close?

That's another possibility, right? There's a couple of ways that we could do this. If it is one of these ones that you think maybe it's consuming resources and you need to shut it down, you could use this little three stacked bar here.

And what this would do is it would give you the ability to close all the applications down at once if you wanted to. But sometimes Ronnie they get a little tricky and they don't really play nice. So sometimes what we have to do, going back into the Settings, going back to apps themselves and let's go ahead, I'm gonna choose that DevInfo.

And the reason I say that Ronnie, because I know I installed that, that wasn't one that was on this phone in the beginning. So let me go ahead and just kinda scroll down to it. We'll find it again, DevInfo here, all right? And sometimes, I'll tell you what, let's go ahead and let me launch DevInfo App and then we'll go back to that same location because you can't stop something if it isn't started.

So we'll go ahead, we'll go back to our Home button, back to home. We'll go back into Settings and back into Apps, all right? And now what we're gonna do is we're gonna go, and I want you to keep in mind too, see that guest has no Internet access?

That might be something that we have to tackle here coming up soon. But we'll go ahead, we'll go back to that DevInfo. All right, and notice that it's running and if it fails to close, right, this is the big thing. If an application fails to close then what you can do is you can actually force stop it.

And what it'll do is it's kinda like task killing Windows or a kill command if you will, if you're in Linux and it says shut that application down.

Yeah, so that's actually really good especially when these apps kinda do end up failing to close and staying open there.

But how is that different from, let's say, like an application crash then?

Okay, so an application crash can happen for a couple of reasons. It could be literally running that the installation, the APK didn't install correctly. And if that happens then you might have to actually have to uninstall the application and reinstall the application too.

But remember, one of the things I want you to keep in mind is that is the most intrusive of the options. So that might wanna be one of the ones you wanna do last. Here's something else you can do if the application seems to be crashing. You have inside of your application and I really haven't moved from the DevInfo app that we have here Ronnie.

There is this Storage and Cache option, and sometimes if an application doesn't wanna act right, right? The first thing you can do is you can clear the cache, right? You clear the cache and that's just that temporary information you utilize to make the performance of this application a little faster.

However, if that doesn't work, you can go a little bit farther. Now when you clear data, you have to be careful because if you have any user account information and you're signed in, take down your user information before you sign it out. Because you wanna be able to sign back in as whatever the user account for that application could be.

And we could say, okay, this is gonna clean the slate and we can relaunch the application. And if at that point it doesn't actually fix the problem, chances are you're just gonna have to uninstall the application and you're gonna have to reinstall it. Fresh installation kinda like spring cleaning might help that application get back off of its knees, if you will.

Yeah, now I've also seen this happen to me too in terms of updating an app.

Mm-hm.

For example, on my iPad, every once in a while it will show me apps that actually need to be updated. I go and click on it and it just says, hey, it failed to actually update.

Mm-hm.

So what are some things I can do about that?

Sure, sometimes you have applications that are paid applications, they rely on a certain account. So for instance, if I'm gonna be logging into Google Play and I'm gonna be downloading that application from Google Play, I might be required To only run that application on a certain amount of devices and maybe I've hit that device max and you go to download it and you go to update it and it doesn't update.

So check your account information, check your licensing information as far as the devices go to as well. Keep in mind that like I said for instance here if you have an application that fails to update, check your account credentials. So for instance if I go back into settings and we go back up here where are my accounts?

There we go, user accounts user and google accounts make sure that your user account is right for the application that you're trying to update because it isn't uncommon for some devices if you have a shared device that you have to have multiple accounts are you logged into the right account?

That might be why it's not updating. And then one of the most simple fixes, do you have network connectivity? If you don't have network connectivity it's hard to reach out and pull down the updates over the air there. So definitely check your network connections too.

Yeah, and I've also seen where I simply just go ahead and do the airplane mode for a few seconds and then turn that off and turn it back on and everything kinda starts to update and actually works the way that we need to.

So along with this Wes there are sometimes where I know that my wife will actually hand me her phone saying everything is running slow as well. What happens when something like that? What can we do about that?

Sure, so when we talk about something that is slow to respond, remember you can have multiple applications open and see right here we have this little stacked icon, that little stacked icon allows you to find the applications that maybe you have in a hibernated mode.

Keep in mind that they're still consuming some of your system resources, they're just in a hibernated state and they're not actively writing information to the storage device within the mobile device. So you might have to literally just do a close all and then re launch the application and see if that causes the application to run a little bit better.

However, if it doesn't remember those same options that we use for crashing applications can also be used for applications that are maybe a little hesitant to run at an optimal performance like they should.

You know it's kind of amazing that sometimes we don't think about these things, but if you hand a regular user who doesn't check these things and then they're saying it's really acting slower than I thought it should.

Normally the applications where you've actually run so many of them, it's actually really stacked up in the RAM pretty hard and sometimes a reboot may be required if they don't know that. And so usually that's what I'd say it's just reboot the thing that actually works,. You know Ronnie that's a valid point and it's a valid troubleshooting methodology when it comes to any mobile device or any software applications, Sometimes it just doesn't free up in memory and a simple reboot will clear that out and flush that memory out.

Now Wes I know with my phone, I'll wake up sometimes and it says, hey, it's time to update the android device itself or the operating system but that can also fail to right?

It can too, let me show you I've actually got one kind of waiting here I'm gonna update this a little bit later.

I didn't want to do it because it could take a while here and I certainly don't want you all to have to wait while we do a long update here. But and you know I kind of take it for granted because I've been on the phone so much, you know these phones.

So I'm going to settings right here and you can kinda see that little notification icon is coming up and it's letting me know that there is a system update that I need to do. And it's asking me if I wanna install it, I'm just gonna install it later, I'm not gonna install it now.

Let's see if they will, they give me any, no they won't give me any information on it, but again, this is an overall system update and this differs a little bit right. Because one of the one of the questions Ronnie asked first was application updates. Application updates come from the google play store, a lot of times these mobile devices you get your system updates from the mobile carriers.

So you have to be careful on that because remember ones coming from google in this case could be the app store if you're an IOS but your system update is gonna be coming from your carrier a lot of times. And that's something that you need to pay attention to because it updates things like the firmware, the base band radio, if you're using PRLS or preferred roaming list, it updates all of that information.

So keep in mind that if it does fail you need to pay, you might have to actually reach out to your carrier and find out why but definitely check your network connections too. All right, so Wes let's talk about this question that most people will ask, do I need to update it?

Yes, yes, you need to update, if you are in a business sense, If you're in a home sense, don't update, that's okay. It's the security vulnerabilities that you have on your network that you need to worry about. I would update because of the security updates alone. Just the security updates.

It does a lot of times give you new functionality fixes, old bugs and stuff but the big thing is when you're in a business environment, security is key and you should be updating your phones.

Right now if you're ever not sure like whether or not it is a security update Wes if we go back to that screen where he actually does show this right underneath you actually see a link there for release notes.

Yeah.

And that should show you what things are actually talking about anytime you see the word like update security. I think it's probably a good reason to do it.

Most definitely because remember your security updates, they are fixing the potential exploits, the vulnerabilities within your mobile devices and those mobile devices are you're gonna bring into your business networks.

So that means by association you're now making your business network vulnerable to if you're using those devices within the company networks. Yeah, so Wes sometimes though it used to happen a lot more often. The very fact is mobile devices used to eat batteries pretty heftly here. So what are some of the things that we can do to help extend the idea of our battery life?

Sure, so some of the things that could happen, I mean we can't overlook that you might have to replace your AC adaptor. I've know that, I've done that before because they get pulled on a lot and that little piece that connects whether it's a micro USB or a lot today.

It's either a lightning or a USB C connector. The connector itself can get worn out. I know that one I have on my phone right now I've got a galaxy note and the little charging ports is actually kind of damaged. So I've gotta really, really be careful. I've actually put it on the charger and set it down and didn't realize it actually wasn't connected so it never charged.

And again, that's my fault. So we can't look past things like the AC adapter needs to be replaced. You might have physical damage to the phone too, so it could be potential damage like that. You might have to repair a charging ports. The other thing too, you might wanna dim your screen, right?

You have, if you swipe down from the top, right, you have the option to actually dim the screen up a little bit. Now what it doesn't show you here is because this is software. But can you see how I'm dimming the screen right? If you dim the screen, that could be something that can preserve your battery life too.

You heard Ronnie mention airplane mode. I know that there's times when I know that I'm not connected and I don't really need to be sending any mobile data. So I'll actually turn on airplane mode just to disable the radios to save my battery life too. I like what you said about the reset, I'm gonna use that resetting your radios too.

Another thing that you have as well in here and let me swipe over I believe. Let's see here there it is battery saver. So keep in mind that you also have the option, it's on AC Power right now. So that battery option is not gonna turn on and if I disconnected from the computer you won't be able to see it.

So you also have the battery saving mode to that could cause problems too. At the end of the day just pay attention to if the battery savers on. I know I've used this a lot and it really does save the the overall battery life. And well like like we say, at the end of the day your battery just might be dying and it might be time to either get it repaired or actually use the warranty on your phone and if it's still in warranty have them replace it.

Yeah, It's amazing because we used to swap batteries out of mobile phones all the time. But today I don't remember the last time I ever heard him but

I tell you I took one out of a a a a cheaper Samsung. It was an A02 Samsung and it was actually, it had some tape that they had fused it to the side wall of the back of the battery.

So you had to use a heating gun very, very careful to liquefy the glue to be able to pull. The lithium ion battery, and that's another thing, even though this episode isn't about safety. If you are changing batteries, please make sure that you dispose of these appropriately cuz they are caustic and they are something that is toxic.

Now Wes I haven't really experienced this one, but you have randomly reboots, what happens there?

Is sure if your phone goes into these random reboots a lot of times, it's gonna be damage potential damage to the phone. Sometimes there is nothing you can do about it, if you noticed that in the normal troubleshooting process, right?

If if Ronnie came to me and he said, hey, wes you're telling me that you're getting random reboots, right. One of the first things he would ask me in the troubleshooting process is, hey, what has changed since you've noticed that this problem has happened? And I said Ronny, I recently installed an application that monitors all of my hardware and now after that part has after that's been installed, it's doing this random reboot.

So that might be an indicator that maybe I need to uninstall the application. And that's one of the reasons we wanna make sure that we install applications from trusted locations because, they are digitally certified. We can verify the publisher and they go through trusted installation sources and they've been tested.

If you go through untested sources, you don't untrusted sources. You don't really know that they're gonna interact with the hardware the way they should. The other thing that you can do and this is probably the most intrusive thing to do. So try some of these other steps that we've talked about before you do this,ultimately you can do a factory reset.

If you do a factory reset, and you bring it back to that earlier point in time and you notice that the reboots are gone. Then you know that it's a software issue that was causing the problem before you factory reset it. If you factory reset it, you still have this issue, I'm gonna say that chances are it's very likely that you've got damage to the mobile device.

All right, well that's the last thing that you have us to address here is the idea of connectivity issues, what are some of the things we need to check.

And sure, so when it, when it comes to connection issues it's so easy if you, if you like me and you have fat fingers like me, you're typing on the phone, you accidentally swipe down, you turn the radio off.

I've actually turned on airplane mode and not known it, not for a procedure that would actually fix the potential issue with the application of the radios themselves. So some of the connectivity issues again, just check your settings. So here let's go ahead and we'll go back into settings, all right.

And then from settings we just go ahead and swipe up and we'll see we've got wifi here, and we can look at the available networks, we can see what our preferences are. Turning on wifi automatically open network notification apps and let me get back in there, because there's also some advanced options too, avoid bad wifi connections.

So you've got a lot of information that you need to just pay attention to come in in the settings, when it comes to your wireless communications. Also with you with Bluetooth, no, I can't pair right now with Bluetooth and Bluetooth is turned off If you turn it on.

Remember you have to be in a pairing mode and you have to find the new device to pair, so definitely pay attention to that. This phone by the way doesn't have near field communication, it doesn't support things like Apple Pay and google pay. If you will think that maybe you're using near field communication maybe like an Apple Pay and that's not working.

Check your NFC settings inside of the phone as well, I wish I could show them to you here but we do not have them. And last but not least there is a really great technology, I really wish we had it was as good in android as it is in IOS and Apple devices.

We have airdrop, if airdrop gives you a connection issue, pay attention to the other device, make sure that you can find it and make sure that airdrop is turned on. It might just be a simple flip of a switch, that might be causing the connectivity issues, these are some of the issues that I would also face.

One of the last ones Ronnie that is in the list that I didn't really wanna make a big deal about if the screen won't auto rotate. That's another thing thing that can cause problems here, so notice that you have this auto rotate option here. And just make sure that it's turned on or off, if you want it to rotate, turn it on, if you don't want it to rotate, then turn it off.

So either way one or the other, just a simple setting that you can change. These are some of the most mobile os and application issues that I'd be able to identify keep in mind it's not an exhaustive list. And we always encourage you to study more, but if you can get these under your belt and you're sitting that certification exam or if you're helping your end users you should be doing good alright.

Wes well that's a lot of great information for us to actually ponder over as we might be supporting users in all the things that they're doing. If not just family members, the very fact is we should be ready to actually help somebody if they need to.

Exercise 2 - Mobile OS and Application Security Issues

It really should, one of the big things when it comes to security in general is that we should be encrypting our devices.

We should be requiring devices to have lock screens that require us to enter some kind of pin or maybe even biometrics to get back in. But there are some other security concerns that maybe we don't think about. And one of the things that I want to talk about really are some of these security concerns that we have in when it comes to just being in a corporate network.

If you're not in a corporate network, then some of these might not even be issues that we even face. And what am I talking about? Well, some of the security concerns that we have to talk about are trusted installation sources. And that shouldn't be something that is new to you if you've been in a Windows Environment.

If you've been in a Mac environment, a Linux environment. You have to know where the software is coming from. Is the software that you're downloading? Is it coming from a reputable source? Can we verify that that software actually came from that vendor? So for instance on my desktop here next to we got our mobile device right here.

But next to our mobile device, I've got this little f droid APK. APK, your android package, if you will. APKs are the installer files inside of android and one of the things that they call out is generically they say the android package source. Well, let me kind of maybe tell you around the jargon of that.

What does that mean? That's your installer files. It means wherever your installer files come from, trust the source of where you get them. So how do we do that? Well, that means that if I decide that I want to get applications for my android device, I'm gonna go to a place like the play store.

Why? Well, because the play store here and I'm not gonna wait for this to launch up, it'll launch up in the background, because if we look at the play store. One of the things that we're going to notice is that if we get down into settings and we look at our applications here, let me scroll down.

I went past my apps. One of the things that we'll see every time an application is downloaded from the google play store. It is run through what is known as Google Play Protect and that means that it's going to be scanned for the certificate that verifies the publisher and where it came from and that it has maintained its integrity and its in the state that we expected.

This is APK over here. Is it somebody that we trust? Is the application going to install the way we wanted to install? Is it going to cause any issues if you will with our device? Well if we don't trust the source and we can't verify the source, then we really don't know that.

And that really is one of the biggest security concerns when it comes to installing applications within your mobile devices is where are those applications coming from? So go to the app store for IOS, iPad OS, if you will, your app store from Mac OS. And I know we're not really talking about laptops here, but if you're in the android world, make sure you go to something like Google Play, make sure you trust the installation sources, the applications that you're going to run on your devices because they have been tested.

A lot of times your administrators can vet them ahead of time because they can go to the vendor, they can see where it came from, find out what it does, what permissions it needs. And they can compare that back to a security policy and they can either allow it or they can deny it.

But at the end of the day, if you're gonna use your device in corporate resources, you need to remember that these kind of APKs that we can't verify. They could cause security concerns.

Now, speaking of that though, what happens if we choose to just run it anyways?

Well, there's a couple of things that could happen too, one of the things that could happen is it might not follow the best practices that Google puts out there when it comes to development of these APKs. Is it going to say, hey, we're requesting these permissions or is it gonna say we're taking these permissions.

The application when installed we're just gonna take the permissions. How about this? If it's a bootleg application like that, is it going to spoof itself? And when it installs, it looks like something like an antivirus software and it tells you you're infected. We call that scare ware. And again, we don't have a way to vet those.

But when you go to trusted sources, you can have people like Google people like Apple, if you will, they are vetting these applications, they are verifying that the applications don't cause damage. And if it's known that they do, guess what, they remove them from the Apple store, they remove them from Google Play and customers are made aware of the fact.

Yeah, it's kind of neat when you go to the Google Play Store. Generally, most app will tell you what permissions that they're actually seeking to run. And if you end up, let's say for instance, you download some particular app, I always recommend you at least check those permissions because you might find out that whatever app you downloaded, you don't know why it's actually asking for permission to get access to your microphone or to your camera or to anything else.

But you're saying, hey, this is a simple application, but why is it accessing my camera? There's no need for it too. And so to me, even the Google Play Store at least tells me those things. Whereas the Bootleg, like what you said here, may not actually end up doing that for us.

Now, Wes at this point, is it really easy to go ahead and actually be able to just install these bootleg things.

You can, if you enable installing from untrusted sources, you can bypass them, you can go into something and you can do even more than what probably your phone wasn't made for the average consumer to do through something like developer mode.

You have what are known as developer options. Now, if I go down all the way to the bottom here and I go into system, you'll notice that developer options are here. I didn't get to developer options by default. I actually had to enable it. And where is the build here?

Let's see here about the phone and there's the build number and I believe, notice it says you're already a developer and it's giving me this little warning, Ronnie, saying there's no need to do that. You're already done that. But when you select the build time, I believe it's five times you turn on what's known as developer options and these developer options give you options that aren't really for the average end user, they're for developers to do testing.

And these could potentially cause security vulnerabilities. If you are in a testing environment, then developer options should be used inside of a mobile device that is sandbox is isolated from your corporate and company network. Again, if you're in a home environment and you're not using this in any kind of corporate sense, it's not a problem.

Because inherently developer options don't have a lot of the security problems that we think, but they could lead to them. I can connect this device to a computer, I could run drivers against it. I could potentially do things reverse engineer stuff. So there could be some security vulnerabilities that your company might have to deal with and that's why sometimes in mobile device management solutions, they might not allow developer options to be turned on.

Yeah, it actually makes a lot of sense there because nobody really wants you messing around with that device and potentially causing it to become a security issue as well. Now Wes, people used to actually take their phones and do what they call routing or jail breaking. What's that about?

Sure. So Ronnie, if we think about our kernel or our Linux kernel, that really is underneath the hood of an android operating system, at the end of the day it's a Linux kernel that is running down there below everything that we see with our applications, graphical user interface, multi-touch screens.

Well, I want you to think a root user access. Root user access is typically locked on these phones and that's because there's not a lot of things that you need to do that requires super user access or even more than super user access. Route access, administrative privileges. So when you root the phone, what are you doing?

Well, when you route a phone, you're bypassing and modifying the bootloader and then once you modify the bootloader, which by the way if you don't root it is protected by security techniques or security technologies like knocks which actually protects the firmware in the operating system as well. But if you root that then what you do is you're bypassing some of those security techniques, those security implementations and you can install customized ROMs.

Think about installing a windows operating system that you didn't get from Windows, you got from some back alleys torn, you can't verify where it actually came from, is it illegal or is it illegal? Well, I don't know. So the problem with this is that when you install some of these aftermarket ROMs, think of it as just technical jargon for I can install whatever operating system on my android device that the some of the developers out there have made.

Well the problem is it's very very difficult for your systems administrators that are trying to protect and secure those devices if you have root access, that means any protections that they put in place, you could just turn around and wipe and they're not in place anymore. That isn't a risk that a lot of companies want to take.

In fact that's not a risk a lot of carriers want to take too, like for instance, you might have a phone that is carrier locked and they do not want you to root it because of the fact that they want to be able to sell you their products and they want you to stay on their networks.

But inside of a corporate environment, it's more about the fact that now we don't know if those security checks and balances that we know we can vet if we look at android documentation, the open source documentation for android, we look at the applications that are installed from trusted sources, no longer can we vet any of that.

So it becomes a major security vulnerability. You might hear the term jail breaking and IOS and iPad OS, and that's the same type of thing where you get those extra level of privilege is kind of like a root level privilege. And the problem with that is it can give the consumer or the employee depending on what your context is.

The ability to override security settings that your security team, if you will, or your IT team put in place to make sure that the productivity applications that they use, you use to access their resources are secure. We can bypass those. So that's one of the reasons. And in fact, this is a big thing inside of mobile device management solutions like Microsoft Endpoint Manager where they will disable that.

They will say no, if that that device is jail broken or if that device has root level access, we don't even allow it on our network. So it is a security vulnerability that companies take very seriously.

So Wes, how does someone actually be able to see, what are the symptoms if something like that were to happen?

Sure. And there's a variety of symptoms that we could see just talking about some of them. You could see high network utilization, high network traffic. And if you've downloaded an application, kind of like Ronnie said, it didn't ask us for the permissions. We think the permissions were what it needs my camera.

Why does it need my camera? It's a calculator. Everything about that. Why does it need access to my contact list if it's a calculator. Now, I'm not talking about the calculator that's built in that one that we've used in the past, but maybe I download a third party one because I like the skin color, the avatar that's in it.

I want it to be flashy. So this could be a problem. So check your application utilization and if you can find the application that is utilizing the majority of your data, then you can shut it down and potentially uninstall it. If you have data limit notifications here, let me show you here.

So for instance, you can get in here to where you get into your WiFi. And you know what, let's go a little bit different. Let's talk mobile networks. That's what we need. Notice that there's this data usage. And you could potentially do a data cap on this. And you could say, hey, I don't want you using any more than two gigs of our three gig data plan.

Well, that's gonna cause, if you will, when you start to hit that limit, some notifications to pop up and it doesn't necessarily mean that there's something wrong with your phone. But it could cause the availability of other applications that require on data utilization to stop working.

Yeah, this is actually kind of interesting here because sometimes when we do end up getting an application on our phone and we don't realize that it actually is communicating constantly actually over, then a notification like this would be very helpful for us.

Most definitely. Another one Ronnie, they talk about limited Internet connectivity, limited Internet connectivity could be because you have your mobile data turned off. So for instance if I pull down from the top here and I scroll over, let me pull it down a little bit farther there, you will notice that in here we will have our mobile data now.

It might not say mobile data. Mine says mobile data on my Samsung. This one doesn't. This TCL says cellular data. If that's turned off, you're not gonna be able to access the Internet. And that could be a problem. So the other thing too, if you have limited Internet connectivity, I would also check those data caps too.

Well, what happens if you have no, you don't have any network connectivity. You will check your network settings and double check permissions as well that you don't have an application that is maybe using that network connection that shouldn't be using that connection that also by association could cause you a high amount of network traffic.

So sometimes these are all shaking hands together and it's just a matter of troubleshooting and going through these pieces one by one and correlating them back with, for instance, application permissions.

There's a lot of apps though that we also end up downloading maybe even from the Google Play Store.

If not even sideloading apps that require you to do either in app purchases or they actually have a higher number of ads.

Most definitely. And that's the difference sometimes just between freeware and pay wear. Right? Something or even shareware, shareware where we share it out for you and we give you a limited trial run.

But once that trial is over, you have reduced functionality or maybe, like Ronnie said, you just have a whole bunch of applications. It could just be the difference between a paid subscription based model or it's free and you have to use the ads to have the free version.

One of the things I would do is that if it becomes a nuisance you can find whatever the offending app is and if those applications or those ads become too much, you can just uninstall that application.

Yeah, there's no doubt because that becomes very annoying trying to use it and then your middle of something and all of a sudden like, hey, it's time to actually post an AD here while you're trying to do it as well.

So Wes, there's also times where we may actually even see fake ad or fake notifications security warnings.

Sure. And we've probably heard of these before. This is that scare ware that's out there. You download that application and you download it from an untrusted source and it starts to warn you that you have a gazillion viruses, technical terminology there.

You have a whole bunch of viruses on your phone and if you'll pay them money, they'd be more than happy to take those viruses off of your phone. Sometimes those applications and of themselves are some type of piece of malware and they can pave the way for additional attacks later down the way.

So the best thing I would say is that if you think you have something like that, go ahead and go to a trusted installation source and download a piece of anti-malware software and run scans against your phone and find out if it finds the locations where maybe a piece of malware is sitting that's causing these fake warnings, if you will, with the fake security warnings.

Yeah, along with that, when we start talking about the very fact that we might download something and it actually does a behavior that we weren't sure of.

Sure. And that again, could be like we were talking about, it could be the permissions issue. It could just be a corrupted installation.

Honestly it might not be any security vulnerability but it can manifest itself as being a security vulnerability. So it's going to be up to you as a tech to make sure that you go through your troubleshooting process. And make sure that you are installing trusted APKs on your mobile devices, trusted installation sources, go to the mobile application stores that are verified.

A lot of times when you download an application they're already running some kind of antimalware software against it, checking it, reaching out to a certificate repository, finding out if we can verify that that application is what it's supposed to be.

Lastly, you also addressed the idea that we may end up having data leaked.

Data leak can happen, that could be because of an application even though the attacks aren't as common, it doesn't mean that they're not out there. We have things like blue jacking and blue snarfing that could cause that problem. So if you do think you have data that's leaking off the device, I would disable any unused connections, if you're not using Bluetooth, disable it.

Because you have to remember that Bluetooth, even though later revisions of Bluetooth have gotten very power friendly. It used to be we would disable it because if we kept it on for five minutes our battery would be dead. But that's not the case today. They have very low energy Bluetooth.

So, a lot of people don't think about having that radio on and just leaving it because it doesn't actually cheer through their battery because battery lives are getting better. But the problem is it opens you up for a potential vulnerability and exploit that somebody if you're sitting at, maybe you're sitting at a hotel and you've jumped on their WiFi hotspot.

Maybe they're connecting through WFfi. Maybe it's not Bluetooth at all. So just remember be mindful of your location where you are and also be mindful of permissions as well as the radios that you have turned on. At the end of the day if you're not using it, turn it off.

If you turn it off, then what you've done is you've closed that gap to be able to leak that personal data. At the end of the day we don't want your data or the company's data falling in unauthorized hands.

Alright Wes, well that's a lot of great information when it comes down to these particular issues that we still have to deal with on a daily basis sometimes, but you should be monitoring and you should of course be training users to make sure that they're looking out for things like this as we actually proceed on in our IT career.

Which of the following may cause an application to fail to launch on a mobile device?

○ The mobile device is charging

● Certain permissions have been disabled

○ You have not used the application for a long time

○ Your friend is also using the application on their mobile device

Which of the following can you do if an application crashes? [Choose all that apply]

□ Clear the cache

□ Clear the application data

□ Uninstall and reinstall the application

□ Ignore the issue

Which of the following may help to prolong the battery life? [Choose all that apply]

□ Turning on airplane mode

□ Dimming the screen

□ Turning on battery-saving mode

□ Playing games on your device

For which of the following reasons is root user access usually locked on phones?

○ To prevent you from using the phone

○ To prevent you from downloading apps from a trusted source

○ It will allow you to disable permission on all apps

● You don’t usually need to do things on phones that require administrator access

Which of the following will help prevent viruses from being downloaded onto your mobile device?

□ Download all files that are sent to you via an attachment

□ Only download apps from a trusted installation source

□ Install anti-malware software on your device

□ Install spam software on your device