Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Chapter**

**9**

**Supporting Mobile Devices**

* [Chapter Introduction](javascript://)
* **9-1**[Types of Mobile Devices](javascript://)
* **9-2**[Mobile Device Operating Systems](javascript://)
  + **9-2a**[Android Managed by Google](javascript://)
  + **9-2b**[iOS by Apple](javascript://)
  + **9-2c**[Windows Mobile by Microsoft](javascript://)
  + **9-2d**[Chrome OS by Google](javascript://)
  + **9-2e**[Comparing Open Source and Closed Source Operating Systems](javascript://)
* **9-3**[Configuring and Syncing a Mobile Device](javascript://)
  + **9-3a**[Mobile Device LAN/WAN Connections](javascript://)
  + **9-3b**[Mobile Device Accessories and Their PAN Connections](javascript://)
  + **9-3c**[Configuring Mobile Device Email](javascript://)
  + **9-3d**[Syncing and Backing Up Mobile Devices](javascript://)
* **9-4**[Securing a Mobile Device](javascript://)
  + **9-4a**[Device Access Controls](javascript://)
  + **9-4b**[Software Security](javascript://)
  + **9-4c**[Mobile Security in Corporate Environments](javascript://)
  + **9-4d**[Common Mobile Device Malware Symptoms](javascript://)
  + **9-4e**[Mobile Device Malware Removal](javascript://)
* **9-5**[The Internet of Things (IoT)](javascript://)
  + **9-5a**[IoT Wireless Technologies](javascript://)
  + **9-5b**[Setting Up a Smart Home](javascript://)
* **9-6**[Troubleshooting Mobile Devices](javascript://)
  + **9-6a**[Troubleshooting Techniques](javascript://)
  + **9-6b**[Common Problems and Solutions](javascript://)
* **9-7**[Chapter Review](javascript://)
  + **9-7a**[Chapter Summary](javascript://)
  + **9-7b**[Key Terms](javascript://)
  + **9-7c**[Thinking Critically](javascript://)
  + **9-7d**[Hands-On Projects](javascript://)
  + **9-7e**[Real Problems, Real Solutions](javascript://)
  + **9-7f**[Exam Tips](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After completing this chapter, you will be able to:

* Describe various types of mobile devices
* Identify and use significant features of Android, iOS, Windows Mobile, and Chrome OS mobile operating systems
* Configure wired and wireless connections on mobile devices
* Synchronize and secure content on mobile devices
* Install and configure IoT devices
* Troubleshoot common problems with mobile devices

Previous chapters have focused on supporting personal computers. This chapter moves on to discuss operating systems on mobile devices such as smartphones and tablets. As mobile devices become more common, many people use them to surf the web, access email, and manage apps and data. This chapter is intended to show you how to support a device that you might not own or normally use. Technicians are often expected to do such things! As an IT support technician, you need to know about the operating systems and hardware used with mobile devices and how to help a user configure and troubleshoot these devices.

Many employees expect to be able to use their mobile devices to access, synchronize, and edit data on the corporate network. Therefore, to protect this data, corporations require that employee mobile devices be secured and that data, settings, and apps be synchronized to other storage locations. In this chapter, you learn how you can synchronize content on mobile devices to a personal computer or to storage in the cloud (on the Internet). You learn how to secure mobile devices. You also learn about some connection technologies specific to the Internet of Things, which includes many non-computing devices such as door locks and security cameras. Finally, in this chapter, you learn about tools and resources available for troubleshooting mobile operating systems.

**A+ Exam Tip**

Much of the content in this chapter applies to both the A+ Core 1 220-1001 exam and the A+ Core 2 220-1002 exam.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-1**Types of Mobile Devices

**A+ Core 1**

* 1.4

Compare and contrast characteristics of various types of other mobile devices.

Mobile devices vary considerably by size, functionality, available connection types, and primary purpose(s), not to mention cost. Here’s a list of the mobile devices that you might be called on to support as an IT support technician:

* ***Smartphone.*** A [**smartphone**](javascript://) is primarily a cell phone that also includes abilities to send text messages with photos, videos, or other multimedia content attached; surf the web; manage email; play games; take photos and videos; and download and use small apps. Most smartphones use touch screens for input (see [Figure 9-1](javascript://)) and a few have a physical keyboard plus a touch screen. Many smartphones allow for voice input.

**Figure 9-1**

Most smartphones don’t have a physical keyboard and use a touch screen with an on-screen keyboard for input



Source: [iStockphoto.com/Hocus-focus](http://istockphoto.com/Hocus-focus" \t "_blank)

* ***Tablets and lightweight laptops.*** A [**tablet**](javascript://) is a computing device with a touch screen that is larger than a smartphone and has functions similar to a smartphone. As you can see in [Figure 9-2](javascript://), it might come with a detachable keyboard or a stylus. Most tablets can connect to Wi-Fi networks and use Bluetooth or NFC (Near Field Communication), which you’ll learn about later in this chapter, to wirelessly connect to nearby devices. Some tablets have the ability to use a cellular network for data transmissions and phone calls. Installed apps, such as Skype, can make voice phone calls, send text, and make video calls. When a tablet can be used to make a phone call, the distinction between a smartphone and a tablet is almost nonexistent, except for size.

**Figure 9-2**

Tablets are larger than smartphones and smaller than laptops

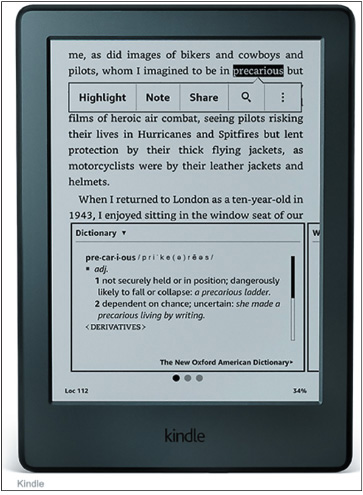


Source: Samsung

* ***E-readers.*** An [**e-reader**](javascript://), as shown in [Figure 9-3](javascript://), is a mobile device that holds digital versions of books, newspapers, magazines, and other printed documents, which are usually downloaded to the device from the web. An e-reader can connect to the Internet using a Wi-Fi wireless connection or a wired connection to a computer that is connected to the Internet. In addition, content can be stored on a flash memory card, which is inserted in the e-reader. Some e-readers, such as Amazon’s Kindle Fire, have other apps that allow for surfing the web, playing games, handling email, and more. Devices such as these blur the line between e-readers and tablets.

**Figure 9-3**

An e-reader includes tools optimized for reading, making notes, and looking up definitions of words



Source: [amazon.com](http://amazon.com/" \t "_blank)

* ***GPS***. A **GPS (Global Positioning System)** feature is often embedded in many mobile devices, including smartphones, smart watches, tablets, and even automobiles, making it possible to identify the device’s location in relation to multiple satellites in orbit around the Earth. Dedicated GPS devices are also available from Garmin ([garmin.com](http://garmin.com/" \t "_blank)), TomTom ([tomtom.com](http://tomtom.com/" \t "_blank)), and a few others. A mobile device determines its location by using Bluetooth and GPS information as well as crowd-sourced Wi-Fi and cellular databases built from anonymous, encrypted, geo-tagged locations of Wi-Fi hotspots and cell towers.
* ***Wearable technology devices.*** [**Wearable technology devices**](javascript://), including smart watches (see [Figure 9-4](javascript://)), wristbands, arm bands, eyeglasses, headsets, clothing, tracking tags, and even action cameras can be used as computing devices to make phone calls, send text messages, transmit data, and/or check email. Wearable technology often includes [**fitness monitoring**](javascript://) capability where the device can measure heart rate, calculate calories burned, count pool laps or miles jogged or biked, and a host of other activities. These devices can sync up with a computer for power and communication, similar to how other mobile devices work. Many people believe smart watches will eventually replace smartphones as the personal communication device of choice.

**Figure 9-4**

The app screen on a smart watch by Apple, Inc.



Source: [iStockphoto.com](http://istockphoto.com/" \t "_blank)/Mutlu Kurtbas

* ***VR/AR headsets***. A special type of wearable technology, **virtual reality (VR) headsets**, can help a user feel immersed in a virtual experience even to the point of moving physically through 3D space. Devices are used primarily for extreme gaming experiences, and are also used in military and medical training. The two main categories of VR headsets are mobile, which is basically a headset shell to hold a smartphone behind the lenses, or tethered, which requires a wired connection to a robust computer. Mobile VR headsets are inexpensive (as low as $30) and, accordingly, the experience leaves much to be desired. Tethered VR headsets, such as the Oculus Rift in [Figure 9-5](javascript://), are much more expensive (around $400) and often come with a variety of accessories to maximize the VR experience. Microsoft has also developed a line of [**augmented reality (AR) headsets**](javascript://) with native compatibility to Windows 10 that tend to fall in the middle ground between mobile and tethered VR headsets.

**Figure 9-5**

The Oculus Rift communicates with a computer through a wired connection



Source: [amazon.com](http://amazon.com/" \t "_blank)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-2**Mobile Device Operating Systems

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

* 4.6

Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.

The operating system for a mobile device is installed at the factory. Here are the four most popular ones:

* [**Android**](javascript://) OS by Google ([android.com](http://android.com/" \t "_blank)) is based on Linux and is used on various smartphones and tablets. At the time of this writing, Android is the most popular OS for smartphones in the world. Nearly 80 percent of smartphones sold today use Android. Combining both smartphones and tablets, Android holds over 70 percent of the worldwide market.
* [**iOS**](javascript://) by Apple ([apple.com](http://apple.com/" \t "_blank)) is based on macOS and is currently used on the iPhone and iPad. Almost 20 percent of smartphones sold today are made by Apple and use iOS, and over 20 percent of smartphones and tablets combined use iOS.
* [**Windows 10 Mobile**](javascript://) by Microsoft ([microsoft.com](http://microsoft.com/" \t "_blank)) is based on Windows 10 and is used on various smartphones. (Tablets use the 32-bit version of the same Windows 10 operating system used on desktop and laptop systems.) About half a percent of smartphones sold today use Windows 10 Mobile or one of its predecessors, such as Windows Phone 8.1.
* [**Chrome OS**](javascript://) by Google is built on the open source Chromium OS ([chromium.org](http://chromium.org/" \t "_blank)). [**Open source**](javascript://) means the source code for the operating system is available for free and anyone can modify and redistribute the source code. Chrome OS is designed solely for use on Google’s Chromebook ([google.com/chromebook](http://google.com/chromebook" \t "_blank)), which is available from many different manufacturers as a lightweight laptop, a tablet, or a convertible laptop-tablet. Chrome OS looks and works like the familiar Chrome browser and relies heavily on web-based apps and storage. While technically a desktop OS, Chrome OS on Chromebooks bridges both the desktop and mobile markets, and it’s rising in popularity due to increased availability of compatible apps, decreasing prices, quick response times in the OS, and reliable security features.

**Notes**

You can see current statistics for specific markets and operating systems at [gs.statcounter.com/os-market-share](http://gs.statcounter.com/os-market-share" \t "_blank). The chart can be edited for a variety of different factors, including device type, OS version, geographic market, and time frame.

**A+ Exam Tip**

The A+ Core 2 exam expects you to understand the similarities and differences among the Android, iOS, Windows Mobile, and Chrome OS operating systems used with mobile devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2aAndroid Managed by Google

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

The Android operating system is based on the Linux OS and uses a Linux kernel. Linux and Android are both open source. Google ([google.com](http://google.com/" \t "_blank) and [android.com](http://android.com/" \t "_blank)) manages but does not own Android, and assumes a leadership role in development, quality control, and distributions of the Android OS and Android apps. Ongoing development of the Android OS code by Google and other contributors is released to the public as open source code.

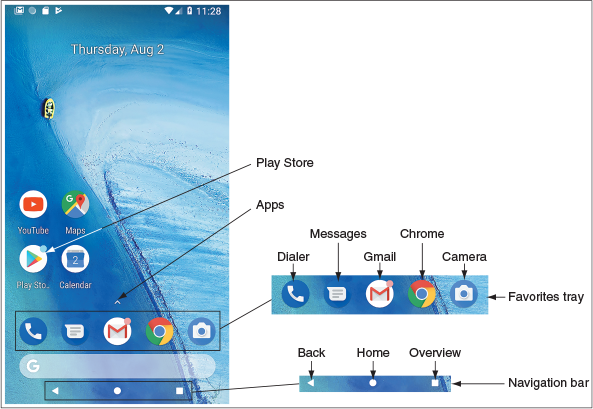
### Get to Know an Android Device

Releases of Android are named after desserts and include Honeycomb (version 3.x), Ice Cream Sandwich (version 4.0.x), Jelly Bean (version 4.1-4.3.x), KitKat (version 4.4+), Lollipop (version 5.0-5.1.1), Marshmallow (version 6.0), Nougat (versions 7.0 and 7.1), Oreo (versions 8.0 and 8.1), and the recently released Pie (version 9.0). Future releases of Android will follow in alphabetic order. At the time of this writing, most new phones and tablets ship with Oreo installed, although Android Pie is released on some phone models.

Android’s graphical user interface (GUI) starts with multiple home screens and supports windows, panes, and 3D graphics. The Android OS can use an embedded browser, manage a database using SQLite, and connect to Wi-Fi, Bluetooth, and cellular networks. Most current Android mobile devices have a power button and volume control buttons on the side, and no physical buttons on the front of the device. However, three soft buttons on the navigation bar at the bottom of the screen include back (goes back to the previous screen), home (goes directly to the home screen), and overview (shows all running apps—swipe an app to the side to close it). See [Figure 9-6](javascript://).

**Figure 9-6**

This Nexus smartphone has the Android Oreo OS installed



Enlarge Image

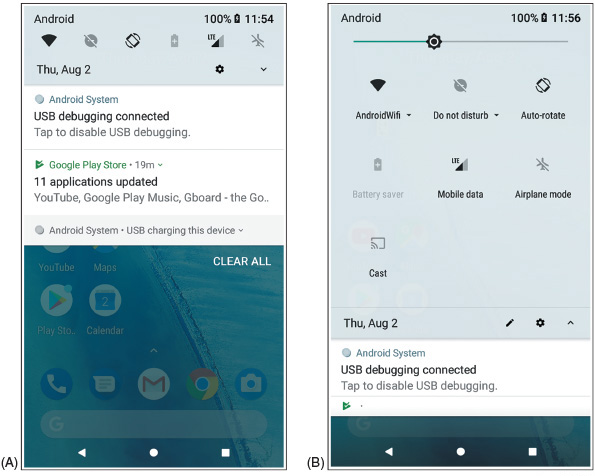
Source: Android

On Android phones, up to five apps or groups of apps can be pinned to the [**favorites tray**](javascript://) just above the navigation bar. Apps in the favorites tray stay put as you move from home screen to home screen by swiping left or right. Tap the small arrow above the favorites tray or swipe up anywhere on the screen to access the [**app drawer**](javascript://), which lists and manages all apps installed on the phone. Press and hold an app in the app drawer to add it to an existing home screen or to add more home screens.

[**Notifications**](javascript://) provide alerts and related information about apps and social media. Notifications are accessed by swiping down from the top of the screen, as shown in [Figure 9-7A](javascript://). The notifications shade provides access to the quick settings panel, such as Wi-Fi, Bluetooth, and Brightness. Tap the **Settings** gear icon near the upper-right corner to open the Settings app (see [Figure 9-7B](javascript://)), or tap the **back** button in the navigation bar to return to the home screen.

**Figure 9-7**

(A) The notifications shade includes quick access to the Settings app; (B) swipe down again to access quick settings on the notifications shade



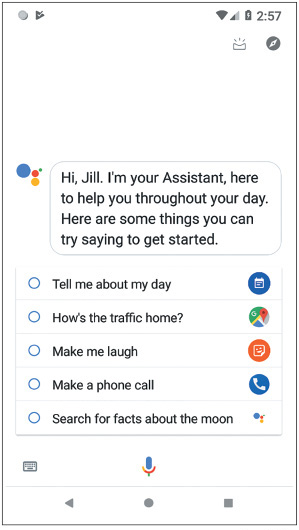
Enlarge Image

Source: Android

A [**digital assistant**](javascript://) service or app, also called a personal assistant, responds to a user’s voice commands with a personable, conversational interaction to perform tasks and retrieve information. Popular examples are Apple’s Siri ([apple.com](http://apple.com/" \t "_blank)), Amazon’s Alexa ([amazon.com](http://amazon.com/" \t "_blank)), Microsoft’s Cortana ([microsoft.com](http://microsoft.com/" \t "_blank)), and the Google Assistant ([assistant.google.com](http://assistant.google.com/" \t "_blank)). Google Assistant can be accessed on most Android devices with the voice command “Ok Google” or “Hey Google,” or by touching and holding the Home button. See [Figure 9-8](javascript://). Give Google Assistant voice commands to send a message, start a phone call, look up information, and do many other tasks.

**Figure 9-8**

Google Assistant responds to voice commands



Source: Android

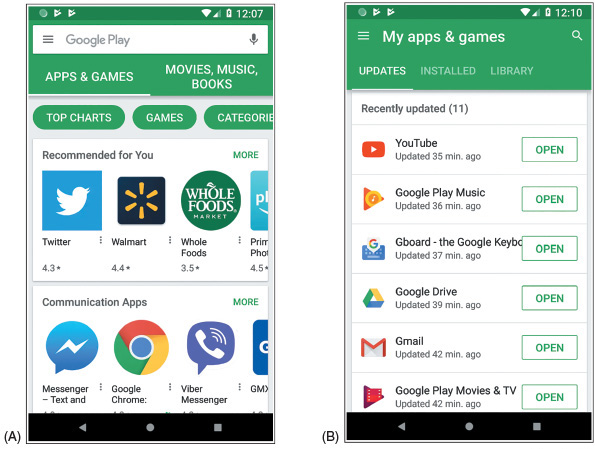
### Android Apps

Android apps are sold or freely distributed from any source or vendor. For example, you can open the Chrome browser and download an app from a website, such as the Amazon Appstore for Android at [amazon.com](http://amazon.com/" \t "_blank) or directly from the website of a developer. However, the official source for apps is [**Google Play**](javascript://) at [play.google.com](http://play.google.com/" \t "_blank). A [**Google account**](javascript://) is required to download content from Google Play and can be associated with any valid email address.

To download an app using the Play Store app, tap the **Play Store** app on the home screen. (If you don’t see the app icon on the home screen, tap the **app drawer** and then tap **Play Store**.) The app takes you to Google Play, where you can search for apps, games, movies, music, e-books, and magazines (see [Figure 9-9A](javascript://)). You can also use the Play Store app to manage updates to installed apps, as shown in [Figure 9-9B](javascript://).

**Figure 9-9**

Use the Play Store app to (A) search Google Play for apps, music, e-books, movies, and more that you can download, as well as (B) updates to installed apps



Enlarge Image

Source: Android

To develop Android apps, an app developer can download Android Studio to his computer from [developer.android.com](http://developer.android.com/" \t "_blank). Included in the download are Android SDK tools and an Android emulator. An [**SDK (Software Development Kit)**](javascript://) is a group of tools that developers use to write apps, and an Android [**emulator**](javascript://) 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. Android Studio is free and is released as open source. In a project at the end of this chapter, you’ll download and install Android Studio and then use it to create virtual Android devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2biOS by Apple

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

Apple, Inc. ([apple.com](http://apple.com/" \t "_blank)) develops, manufactures, and sells the Apple [**iPhone**](javascript://) (a smartphone) and [**iPad**](javascript://) (a handheld tablet). Both of these devices use the iOS operating system, also developed and owned by Apple. iOS is based on [**macOS**](javascript://), the operating system used by Apple desktop and laptop computers. The latest release at the time of this writing is iOS 12. Apple maintains strict standards on its products, which means iOS is exceptionally stable and bug free. Apple’s iOS is also a very easy and intuitive operating system to use. As with macOS, iOS makes heavy use of icons.

### Get to Know an iOS Device

Because Apple is the sole owner and distributor of iOS, the only devices that use it are Apple devices (currently the iPhone and iPad). iPhones and iPads each have a physical [**Side button**](javascript://) on the upper-right side of the device. All iPads and older models of iPhones have a [**Home button**](javascript://) on the bottom front, but the newer iPhone X (pronounced iPhone ten) models don’t have a Home button (see [Figure 9-10](javascript://)). The iOS user interface as it appears on an iPad is shown in [Figure 9-11](javascript://). Apps can be pinned to the [**dock**](javascript://) at the bottom of the screen.

**Figure 9-10**

The iPhone X series does not have the Home button that comes on all previous models of iPhones

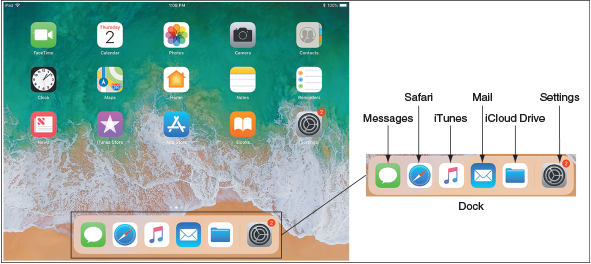


Enlarge Image

Source: [https://www.apple.com/iphone/compare/](https://www.apple.com/iphone/compare/" \t "_blank)

**Figure 9-11**

Access the dock on an iPad by swiping up from the bottom of the screen



Enlarge Image

Source: iOS

Knowing a few simple navigation tips on an iOS device can help you get around a little more easily:

* **Open and close apps.** Tap an app icon to open it. Use the app switcher to switch to a different open app or to close apps. On an iPad, swipe up on the screen or double-click the Home button to show the app switcher and control center on the same screen (see [Figure 9-12](javascript://)). On an older iPhone, double-click the Home button to see the app switcher. On an iPhone X, swipe up from the bottom and briefly hold to see the app switcher, or you can swipe side to side to move among open apps. In the app switcher, swipe up to close an app. Closing apps you’re not using can save battery life.

**Figure 9-12**

Access the app switcher and control center from any screen



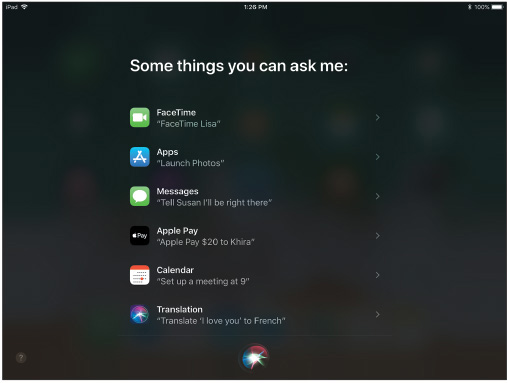
Enlarge Image

Source: iOS

* **Control center**. Use the control center to change basic settings such as brightness, volume, Wi-Fi, and Bluetooth. For the iPad and older iPhones, swipe up to show the control center (see the right side of [Figure 9-12](javascript://) for an iPad). On an iPhone X, swipe down from the upper-right corner to show the control center. Use the Settings app to adjust which settings are available in the control center.
* **Notification screen**. Swipe down from the top of the screen to see the notifications screen. The types of notifications shown and other notification settings can be customized in the Settings app, which you can open from the Home screen by tapping the Settings icon.
* **Delete and move apps**. To delete or move an app icon on the screen, press and hold the icon until all icons start to jiggle. As the icons jiggle, press the **X** beside the icon to delete it. To move an icon, press and drag it to a new location. You can add new home screens by dragging an app icon off the screen to the right. To stop the jiggling, press the Home button on the iPad and older iPhones. For iPhone X, press the **Done** button that appears in the upper-right corner of the screen.
* **Siri**. For iPhone X, press and hold the Side button to open Siri, iOS’s digital assistant service, as shown in [Figure 9-13](javascript://). For all other iPhones and iPads, press and hold the **Home** button to open Siri. Siri was the first of the digital assistant services and has been around long enough to have become quite sophisticated. Siri uses information within the user’s account to provide a customized experience.

**Figure 9-13**

Siri follows voice commands



Source: iOS

### iOS Apps

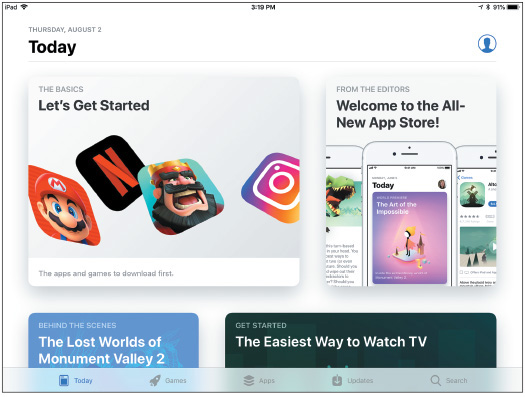
You can get Android apps from many sources, but the only place to go for an iOS app is Apple. Apple is the sole distributor of iOS apps at its [**App Store**](javascript://). Other developers can write apps for the iPhone or iPad, but these apps must be sent to Apple for close scrutiny. If they pass muster, they are distributed by Apple on its website. Apple offers app development tools, including the iOS SDK (Software Development Kit) at [developer.apple.com](http://developer.apple.com/" \t "_blank).

When you first purchase an iPad or iPhone, you activate it by signing into the device with an [**Apple ID**](javascript://), or user account, using a valid email address and password, and associating the account with a credit card number. Here are options for obtaining apps and other content:

* **App Store**. Use the App Store app on your mobile device (see [Figure 9-14](javascript://) for an iPad example) to search, purchase, and download apps, games, e-books, and periodical content such as newspapers and magazines. Some downloads are free.

**Figure 9-14**

Use Apple’s App Store app to download new apps



Source: iOS

* **iTunes**. Use the [**iTunes**](javascript://) Store app to search, purchase, and download media content, including music, movies, TV shows, and podcasts. (Again, some downloads are free.) You also have the option to download and install the iTunes software on a Mac or Windows personal computer. When you connect your mobile device to the computer by way of a USB port, you can use the iTunes software to sync the device to iOS updates downloaded from [iTunes.com](http://itunes.com/" \t "_blank) and to content on your computer, which can be a helpful troubleshooting option, as you’ll see later.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2cWindows Mobile by Microsoft

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

The Windows Mobile operating system by Microsoft is more or less a simplified version of the Windows operating system designed for desktop computers, laptops, and tablets. Windows Mobile and Windows version numbers correspond: Windows Mobile 10 corresponds to Windows 10. One of the biggest differences between Windows and Windows Mobile is that Windows Mobile does not have a desktop screen. Everything is accessed from the Start screen.

### Get to Know a Windows Mobile Device

Most Windows phones have three buttons below the screen (see [Figure 9-15](javascript://)). These buttons might be physical buttons or software buttons. The start button accesses the Start screen, the back button goes back one screen, and the search button opens a Cortana search box. (Recall that Cortana is the Windows digital assistant app.) Also, if you press and hold the **back** button, it displays recent apps. For most phones, these buttons aren’t true software buttons, but they’re also not true physical buttons because they might not work when the OS is malfunctioning.

**Figure 9-15**

Press and hold the search button to activate Cortana, the Windows digital assistant

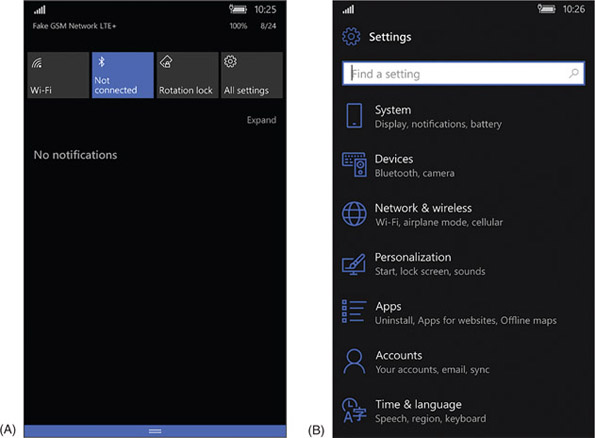


Windows phones rely primarily on the Start screen for accessing apps. Just as with Windows 10, the Start screen is full of live tiles; each represents an app and many show live data on the tile from that app. Here are some tips for getting around Windows Mobile:

* Tap a tile on the Start screen to open its app. Scroll up or down to see more tiles. Press and hold to resize or reposition tiles. On many smartphones, pressing and holding a link functions like right-clicking with a mouse on a Windows desktop computer.
* Swipe down from the very top of the screen to see notifications in the Action Center ([Figure 9-16A](javascript://)), similar to both Android and iOS. Like Android, there is also a Settings icon here to open the Settings app, shown in [Figure 9-16B](javascript://). Settings can also be accessed via the Settings tile on the Start screen.

**Figure 9-16**

(A) Notifications appear in the Action Center; (B) the Settings app provides an extensive toolkit for customizing a Windows smartphone

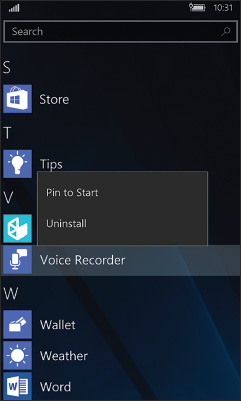


Enlarge Image

* Swipe from the right to see the apps list. Press and hold an app on the list to pin the app to the Start screen (see [Figure 9-17](javascript://)). On the Start screen, you can press and hold the app tile and then change its size and other characteristics. Tap the **Store** tile on the Start screen to find more apps.

**Figure 9-17**

To pin an app to the Start screen, press and hold the app’s icon and then tap Pin to Start



* While a menu is displayed in the Settings app, you can sometimes swipe from the right to see a submenu. Windows Mobile is rich with settings options, making it easier to integrate Windows phones in an enterprise environment.
* Windows Mobile 10 has a digital assistant called Cortana that also customizes the user’s experience.

### Windows Mobile Apps

The availability of apps for Windows mobile devices is much more limited than that for Android or iOS. Windows apps are obtained through the [**Microsoft Store**](javascript://) app. Additionally, like Android apps, Windows Mobile apps can be obtained from third-party websites via the browser on the mobile device.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2dChrome OS by Google

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

Chrome OS is deeply integrated with Google’s Chrome browser: Most of Chrome OS’s native apps open directly in the Chrome browser and rely heavily on having an active Internet connection. While there are some apps that will function offline, such as Gmail, Docs, and Calendar, functionality is limited to data that is temporarily stored on the Chromebook until it can again be synced with the user’s online account. Chrome OS functions exclusively on Chromebooks, although many manufacturers build and sell Chromebooks. See [Figure 9-18](javascript://).

**Figure 9-18**

A Chromebook can be a lightweight laptop, a tablet, or a hybrid laptop-tablet

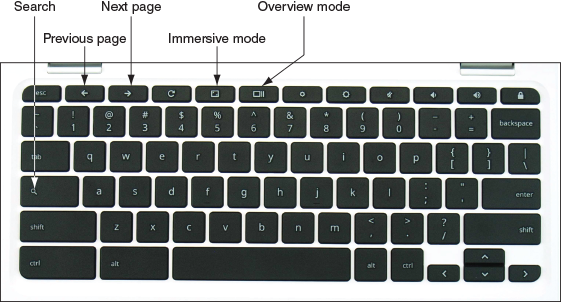


### Get to Know a Chromebook

Chromebooks come with a variety of external ports, depending on the manufacturer and model. Many feature USB and USB-C ports as well as HDMI. Some include SD card slots for adding extra storage space. The keyboard on a Chromebook (see [Figure 9-19](javascript://)) looks similar to the typical laptop keyboard, with a few notable differences. The unique keys mostly run along the top of the keyboard and include these keys: search, previous and next pages, refresh, immersive mode (hides tabs and launcher), and overview mode (shows all open apps). Keyboard shortcuts, a popular feature with Chromebooks, use combinations of key presses to accomplish tasks such as opening a new Chrome window (**ctrl+n**) or tab (**ctrl+t**), taking a screenshot (**ctrl+overview**), locking the screen (**search+L**), and showing all keyboard shortcuts (**ctrl+alt+/**).

**Figure 9-19**

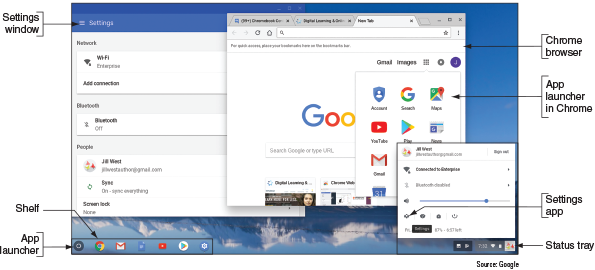
A Chromebook keyboard



[Figure 9-20](javascript://) shows the Chrome OS desktop with the Settings app and Chrome browser open. Also notice the shelf on the bottom left and the open status tray on the bottom right. The app launcher is in the shelf. To open the Settings app, click anywhere in the status tray, which opens the tray, and then click the **Settings app** gear icon in the open status tray.

**Figure 9-20**

The Chrome OS desktop



Enlarge Image

Source: Google

Chrome OS is automatically updated about every six weeks and includes some significant security measures to protect the computer from malware, including built-in virus protection. Google took a four-pronged approach to security with Chrome OS:

* **Sandboxing.** Each tab in the Chrome browser is isolated from the underlying OS and from processes in other tabs.
* **Verified boot.** Similar to the Windows Secure boot, it protects the OS from changes being made to its underlying system files, automatically entering recovery mode if modifications are detected.
* **Power washing.** The user can perform a simple and quick reset to factory settings in the event a malware infection does manage to take hold.
* **Quick updates.** The OS updates itself in the background without user intervention about every six weeks. If an update is needed for a security patch, it can happen within 48 hours.

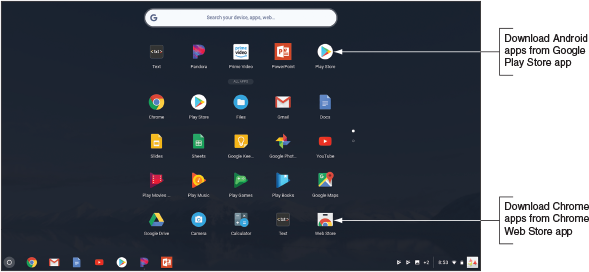
The end effect is a very stable and secure OS that even security professionals rely on when traveling to techie, hacker, or security conferences, where the persistent threat of hacking attacks is an integral part of the overall experience.

### Chrome OS Apps

The Chrome shelf contains icons for important apps; tap an icon to open the app. To view and open any installed app, tap the app launcher icon in the shelf (refer back to [Figure 9-20](javascript://)) and tap an app in the launcher (see [Figure 9-21](javascript://)). Most apps open in the Chrome browser, and several apps offer Chrome extensions that add functionality to the Chrome browser even when the app is not open. Users can get more apps through the Chrome Web Store app, and some newer Chromebooks also support Android apps downloaded through the Google Play Store app.

**Figure 9-21**

Open apps from the Chrome OS app launcher



Enlarge Image

Source: Google

**Caution**

Know that if you download Android apps to the Chromebook and then turn off the Play Store app, you’ll lose all the Android apps’ data and settings from the Chromebook.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2eComparing Open Source and Closed Source Operating Systems

**A+ Core 1**

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

* 4.6

Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.

Open source operating systems (such as Android and Chrome OS) and closed source operating systems (such as iOS and Windows Mobile) have their advantages and disadvantages. Closed source systems are also called vendor-specific or [**commercial license**](javascript://) operating systems. Here are some key points to consider about releasing or not releasing source code:

* Apple carefully guards its iOS source code and internal functions of the OS. Third-party developers of apps have access only to APIs, which are requests to the OS to perform a function, such as to access data provided by the embedded GPS. An app must be tested and approved by Apple before it can be sold in Apple’s online App Store. These policies assure users that apps are high quality. It also assures developers they have a central point of contact for users to buy their apps, and their copyrights are better protected.
* In the interest of openness and innovation, the Android and Chrome OS source code and the development and sale of apps are not as closely guarded. Apps can be purchased or downloaded from Google Play or Chrome Web Store, but they can also be obtained from other sources such as [amazon.com](http://amazon.com/" \t "_blank) or directly from a developer. This freedom comes with a cost because users are not always assured of high-quality, bug-free apps, and developers are not always assured of a convenient market for their apps.
* For Android, because any smartphone or tablet manufacturer can modify the source code, many variations of Android exist. These variations can make it difficult for developers to write apps that are compatible with any given Android platform. These inconsistencies can also make it difficult for users to learn to use new Android devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-3**Configuring and Syncing a Mobile Device

**A+ Core 1**

* 1.5

Given a scenario, connect and configure accessories and ports of other mobile devices.

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 1.7

Given a scenario, use methods to perform mobile device synchronization.

* 2.4

Compare and contrast wireless networking protocols.

* 3.1

Explain basic cable types, features, and their purposes.

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

In this part of the chapter, you learn to configure network connections and to update and back up data, content, and settings on mobile devices. You don’t need to memorize these steps—it’s sufficient to be familiar with the general idea of where these features are located in the OS and how to use them, especially because the specific steps change with almost every new version of any mobile OS. We’ll use examples of both Android and iOS because they’re by far the most popular mobile OSs.

**Notes**

You can follow along with the steps given in the following sections using a real smartphone or tablet (Android or iOS) or you can use an Android emulator. [Real Problem 9-1](javascript://) at the end of this chapter gives you step-by-step instructions to install and configure the free Android Studio, which includes an Android emulator. You can then create emulated Android devices on your screen with real features that work like those on a physical device, including a power button, rotate capability, camera function, and much more.

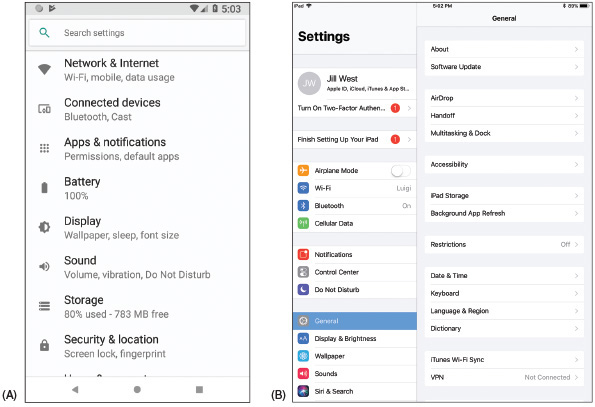
**Notes**

Because the Android operating system is open source, manufacturers can customize the OS and how it works. Therefore, specific step-by-step directions will vary from device to device, even when the devices all use the same Android release. Remember that you don’t need to memorize the steps—just learn general procedures for supporting a variety of mobile devices.

When you are called on to support a device that you don’t own or normally use, it’s helpful to begin by looking for how to change settings. Most of the settings you need to use to support a mobile device are contained in the Settings app. [Figure 9-22](javascript://) shows the Settings apps for Android and iOS. Basically, you can open the Settings app and search through its menus and submenus until you find what you need. If you get stuck, check the user guide for the device, which you can download from the device manufacturer’s website. The user guide is likely to tell you the detailed steps of how to connect to a network, configure email, update the OS, sync and back up settings and data, secure the device, and what to do when things go wrong. So let’s get started.

**Figure 9-22**

(A) The Android Settings app, and (B) the iOS Settings app



Enlarge Image

Source: Android, iOS

**Notes**

Most of us rarely follow step-by-step directions when learning to use a new device until when “all else fails, read the directions.” This part of the chapter can give you an idea of what to look for, and you can likely figure out the specific steps for yourself.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3aMobile Device LAN/WAN Connections

**A+ Core 1**

* 1.5

Given a scenario, connect and configure accessories and ports of other mobile devices.

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 3.9

Given a scenario, install and configure common devices.

A mobile device might have several antennas—primarily Wi-Fi, GPS, Bluetooth, NFC, and cellular. The device uses a Wi-Fi or cellular antenna to connect to a LAN (local area network) or WAN (wide area network) and uses Bluetooth or NFC to connect to a PAN (personal area network). Settings on the device allow you to enable or disable each antenna. Network connections are configured using the Settings app. Let’s look at LAN and WAN network connections first, then we’ll look at technologies used for connecting mobile device accessories in PANs.

**Notes**

You can automatically disable the antennas in a mobile device that can transmit signals by enabling **airplane mode** so that the device can neither transmit nor receive the signals. Many newer devices do not disable the GPS or NFC antennas; GPS only receives and never transmits, and NFC signals don’t reach very far. While airplane mode is on, you can manually enable some wireless connections, such as Bluetooth or Wi-Fi.

**A+ Exam Tip**

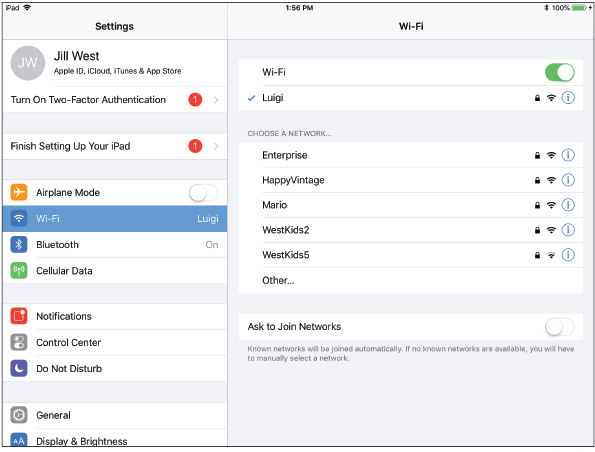
The A+ Core 1 exam might give you a scenario that expects you to decide how to configure a Wi-Fi, cellular data, Bluetooth, or VPN connection on a mobile device.

### Wi-Fi Connection

Most mobile devices have Wi-Fi capability and can connect to a Wi-Fi local wireless network. On the Wi-Fi settings screen, you can add a Wi-Fi connection, manage existing networks, view available Wi-Fi hotspots, see which Wi-Fi network you are connected to, turn Wi-Fi off and on, and decide whether the device should ask the user before joining a Wi-Fi network. When the device is within range of Wi-Fi networks, it displays the list of networks. Select one to connect. If the Wi-Fi network is secured, enter the security key to complete the connection. To change a network’s settings, tap the name of the network (see [Figure 9-23](javascript://)). Searching for a Wi-Fi network can drain battery power. To make a battery charge last longer, disable Wi-Fi when you’re not using it.

**Figure 9-23**

Configure Wi-Fi connection settings



Enlarge Image

Source: iOS

### Tethering and Mobile Hotspots

When a mobile device is connected to the Internet by way of its cellular network, recall from [Chapter 7](javascript://) that you can allow other computers and devices to use this same connection. For example, in [Figure 9-24](javascript://), the smartphone is tethered by USB to a laptop so that the laptop can use the cellular network to connect to the Internet. If the smartphone has Wi-Fi capabilities, it can create its own Wi-Fi hotspot for other computers and devices to connect to wirelessly. An app on the smartphone controls these connections. To use your phone for tethering and for providing mobile hotspots, your carrier subscription must allow it.

**Figure 9-24**

Tether your smartphone to your laptop using a USB cable



### Cellular Data Connection

Smartphones and some laptops, tablets, and wearable mobile devices can connect to a cellular network if they have cellular capability and a subscription to the cellular network carrier. Recall from [Chapter 7](javascript://) that a cellular network provided by a carrier (for example, AT&T or Verizon) is used for voice, text, and data communication. A cellular network uses GSM or CDMA for voice and another layer of technology for data transmissions, such as 3G, 4G, 5G, and LTE. GSM and LTE require a SIM card installed in the device, and CDMA does not use a SIM card unless the network is also using LTE, which does require a SIM card. To make a cellular data connection, you must have a subscription with your carrier that includes a cellular data plan.

Here is information that might be used when a connection is first made to the network:

* The [**IMEI (International Mobile Equipment Identity)**](javascript://) is a unique number that identifies each mobile phone or tablet device worldwide. It’s usually reported within the About menu in the OS, and it might also be printed on a sticker on the device, such as behind the battery.

**Notes**

If your phone gets stolen and you notify your carrier, the carrier can block its use based on the IMEI and alert other carriers to the stolen IMEI. Also, before buying a used phone, check its IMEI against blacklists of stolen phones by doing a Google search on imei blacklist check.

* The [**IMSI (International Mobile Subscriber Identity)**](javascript://) is a unique number that identifies a cellular subscription for a device or subscriber, along with its home country and mobile network. This number is stored on the SIM card for networks that use SIM cards. For networks that don’t use SIM cards, the number is kept in a database maintained by the carrier and is associated with the IMEI.
* The ICCID (Integrated Circuit Card ID) identifies the SIM card if the card is used. To know if a device is using a SIM card, look in the Settings app on the About menu. An ICCID entry indicates a SIM card is present.

**A+ Exam Tip**

The A+ Core 1 exam expects you to identify and distinguish between the IMEI and the IMSI, and might give you a scenario that requires you to enable or disable a cellular data network connection.

When a carrier uses a SIM card, you can sometimes move the card from one device to another and the new device can connect to the carrier’s network. When a carrier does not use a SIM card, you must contact the carrier and request permission to switch devices. If the carrier accepts the new device, the new IMEI will be entered in the carrier’s database.

The carrier typically configures the phone to make calls on its network; however, you might find that you want to disable cellular data at times, or disable cellular roaming. The advantage of disabling cellular data and using Wi-Fi for data transmissions is that these transmissions are not charged against your cellular data subscription plan. Also, Wi-Fi is generally faster than most cellular connections. Disabling roaming can prevent roaming charges on your bill incurred from using other carriers’ cellular networks when you travel outside your home territory.

To disable roaming on an Android device, go to the Network & Internet menu in the Settings app, tap **Mobile network**, then turn off **Mobile data** or **Roaming**. On an iOS device, open the Settings app, tap **Cellular Data**, then turn off **Cellular Data**. Next, tap **Cellular Data Options**, then turn off roaming.

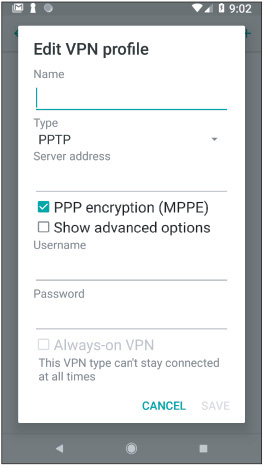
If you have roaming enabled, especially for a CDMA device, you’ll want to keep the [**PRL (Preferred Roaming List)**](javascript://) updated. The PRL is a database file that lists the preferred service providers or radio frequencies your carrier wants the device to use when outside your home network. You can reset or update the list in the Settings app. For Android devices, go to the **System updates** menu and tap **Update PRL**. For an iOS device, open the Settings app, tap **General**, then scroll down and tap **Reset**, **Subscriber Services**, and **Reprovision Account**.

### VPN Connection

Like desktop computers, a mobile device can be configured to communicate information securely over a virtual private network (VPN) connection. To create a VPN connection in the Settings app, tap **VPN** and then add a new VPN connection. Follow directions to complete the connection, which will require you to know the type of encryption protocol used (PPTP, L2TP, or IPsec), the IP address or domain name of the VPN server, and the user name and password to the corporate network. [Figure 9-25](javascript://) shows the configuration options on an Android smartphone. In addition to the built-in Android VPN client shown in the figure, some Android devices also provide proprietary VPN configuration options. To access VPN settings in iOS, open the **Settings** app, tap **General**, and then tap **VPN**.

**Figure 9-25**

Configure a VPN connection



Source: Android

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3bMobile Device Accessories and Their PAN Connections

**A+ Core 1**

* 1.5

Given a scenario, connect and configure accessories and ports of other mobile devices.

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 2.4

Compare and contrast wireless networking protocols.

* 3.1

Explain basic cable types, features, and their purposes.

* 3.9

Given a scenario, install and configure common devices.

You can buy all kinds of accessories for mobile devices, such as wireless keyboards, speakers, earbuds, headsets, game pads, docking stations, printers, extra battery packs and chargers, USB adapters, memory cards (usually the microSD form factor) to expand storage space, credit card readers for accepting payments by credit card, and protective covers for waterproofing. For example, [Figure 9-26](javascript://) shows a car docking station for a smartphone. Using this car dock, the smartphone serves as a GPS device giving driving directions.

**Figure 9-26**

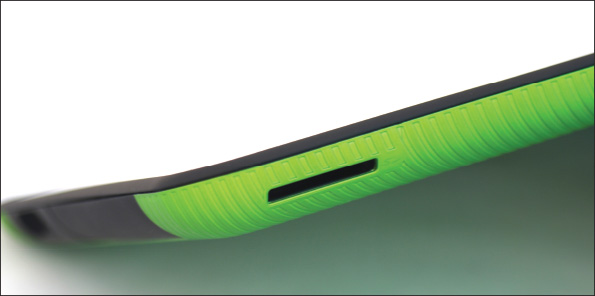
A smartphone and a car docking station



When buying accessories for a mobile device, be sure to check what ports and slots are available on the device. For example, many mobile devices no longer include replaceable batteries. Current iPhones no longer have audio ports—to use a wired headset, you have to plug a dongle into the Lightning port. Some mobile devices have a slot for a memory card, which might be located on the side of the case or inside it; however, Apple mobile devices and many others don’t offer this feature. [Figure 9-27](javascript://) shows a memory card slot on an Android tablet, and [Figure 9-28](javascript://) shows a MicroSD card.

**Figure 9-27**

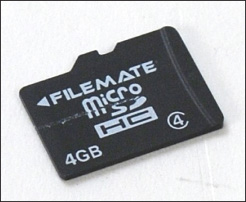
An Android device might provide a memory card slot to allow for extra storage



Enlarge Image

**Figure 9-28**

A mobile device might use a MicroSD card to add extra flash memory storage to the device

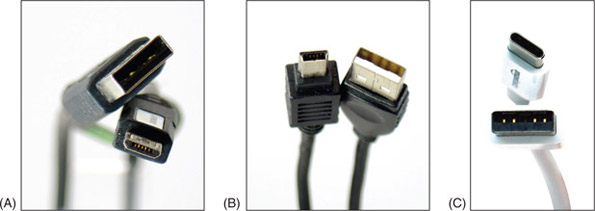


### Wired Connections for Accessories

Smartphones, tablets, and wearable devices can make a wired connection to a computer. This connection can be used to charge the device, download software updates, upload data to the computer, back up data, and restore software or data. The device’s port used for power and communication may be a type of USB port or a proprietary, vendor-specific port. Some USB connectors used for this purpose include **microUSB** (see [Figure 9-29A](javascript://)), the smaller **miniUSB** (see [Figure 9-29B](javascript://)), and the newer **USB-C** (see [Figure 9-29C](javascript://)). Newer Apple iPhones, iPods, and iPads use the proprietary [**Lightning port**](javascript://) and connector for power and communication (see [Figure 9-30](javascript://)).

**Figure 9-29**

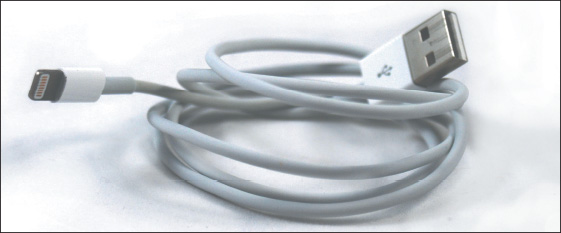
Some mobile devices may connect to a computer’s USB port by way of a (A) microUSB, (B) miniUSB, or (C) USB-C cable



Enlarge Image

**Figure 9-30**

A Lightning cable by Apple, Inc., has a USB connector for the computer end and a Lightning connector for an iPhone or iPad



### Wireless Connections for Accessories

Mobile devices typically have the capability to connect to other nearby wireless devices and accessories using a Bluetooth, IR, or NFC wireless connection:

* **Bluetooth**. **Bluetooth** is a short-range wireless technology to connect two devices in a small PAN. To create a Bluetooth connection, the two devices must be [**paired**](javascript://), a process you’ll learn more about later in this chapter. [Figure 9-31](javascript://) shows an iPad connected to a keyboard using Bluetooth.

**Figure 9-31**

An iPad and a wireless keyboard can connect using Bluetooth



* **Infrared.** [**Infrared (IR)**](javascript://) is a wireless connection that requires an unobstructed “line of sight” between transmitter and receiver, which must be within about 30 m of each other. IR relies on light waves just below the visible red-light portion of the spectrum. This means you can’t see infrared light, but you can feel it as heat. TV or other multimedia devices and a remote control often use an IR wireless interface. Apps on smartphones and tablets that support IR can be used in place of an IR remote control.
* **NFC.** [**Near Field Communication (NFC)**](javascript://) is a wireless technology that establishes a communication link between two NFC devices that are within 10 cm (about 4 inches) of each other. For example, when two smartphones get within close range, they can use NFC to exchange contact information. NFC connections are also used for contactless credit card payments at a store. An NFC tag (see [Figure 9-32](javascript://)) contains a small microchip that can be embedded in just about anything, including a key chain tag, printed flyer, or billboard (see [Figure 9-32](javascript://)). The NFC tag dispenses information to any NFC-enabled smartphone or other device that comes within 4 inches of the tag. Learn more about NFC at [nearfieldcommunication.org](http://nearfieldcommunication.org/" \t "_blank).

**Figure 9-32**

These programmable NFC tags have sticky backs for attaching to a flat surface like a wall, desk, or car dashboard



**Applying Concepts**

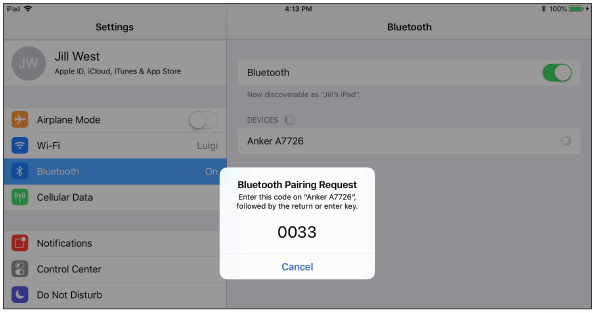
### Pairing Bluetooth Devices

To configure a Bluetooth connection, complete the following steps:

1. Turn on the Bluetooth device, such as a speaker, headset, or keyboard, to which you want to connect your mobile device.
2. Enable Bluetooth on that device and enable pairing mode. Sometimes just turning on Bluetooth enables pairing automatically for a limited period of time. The device might have a pairing button or combination of buttons to enable pairing. When you press this button, a pairing light blinks, indicating the device is ready to receive a Bluetooth connection. This makes the device discoverable, which means it’s transmitting a signal to identify itself to nearby Bluetooth devices.
3. On your mobile device, turn on Bluetooth. The mobile device searches for Bluetooth devices. If it discovers the Bluetooth device, tap it to connect. The two Bluetooth devices now begin the pairing process.
4. The devices might require a code to complete the Bluetooth connection. For example, in [Figure 9-33](javascript://), an iPad and Bluetooth keyboard are pairing. To complete the connection, enter the four-digit code on the keyboard.

**Figure 9-33**

A code is required to pair these two Bluetooth devices



Enlarge Image

Source: iOS

1. Test the connection. For an audio device, play a video or audio recording on the mobile device, and for a keyboard, type into a notes application or text box.

**A+ Exam Tip**

The A+ Core 1 exam might give you a scenario that requires you to pair Bluetooth devices and then test connectivity after the connection is established.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3cConfiguring Mobile Device Email

**A+ Core 1**

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 3.9

Given a scenario, install and configure common devices.

Using a personal computer or mobile device, email can be managed in one of two ways:

* **Using a browser.** In a browser, go to the website of your email provider and manage your email on the website. In this situation, your email is never downloaded to your computer or mobile device, and your messages remain on the email server until you delete them.
* **Using an email client.** An email client application, such as Microsoft Outlook, can be installed on your personal computer or on your mobile device. The app can either download email messages to your device (using the POP3 protocol) or can manage messages on the server (using the IMAP protocol). When the app downloads messages, you can configure the server to continue to store these messages for later use or delete the messages from the server.

Email providers include [**Gmail**](javascript://) (by Google), [**iCloud**](javascript://) (by Apple), [**Yahoo**](javascript://)! (owned by Verizon), or Outlook/Hotmail/Live (Microsoft’s public email services for individuals). Microsoft also offers Exchange, its private enterprise email service that is hosted on corporation or ISP servers, or [**Exchange Online**](javascript://), which is hosted on Microsoft servers. As for apps on your mobile device, Android includes the Gmail app, which can be used with any email provider, and iOS includes its Mail app. In either OS, a different email app can be installed, such as Microsoft Outlook, Google Inbox, Yahoo Mail, or K-9 Mail.

To configure email on a mobile device, open the email app and add an email account directly in the app. Here is the information you’ll need to configure an email app on a mobile device:

* **Your email address and password.** If your email account is with Google, Microsoft, Apple, or Yahoo!, your email address and password are all you need because the OS can automatically set up these accounts.

If your email account is with any other provider, you’ll also need the following information:

* **Names of your incoming and outgoing email servers**. To find this information, check the support page of your email provider’s website. For example, the server you use for incoming mail might be [imap.mycompany.com](http://imap.mycompany.com/" \t "_blank), and the server you use for outgoing mail might be [smtp.mycompany.com](http://smtp.mycompany.com/" \t "_blank). The two servers might have the same name.
* **Type of protocol your incoming server uses**. The incoming server will use POP3 or IMAP4. Using IMAP4, you are managing your email on the server. For example, you can move a message from one folder to another and that change happens on the remote server. Using POP3, the messages are downloaded to your device where you manage them locally. Most POP3 mail servers give you the option to leave the messages on the server or delete them after they are downloaded.
* **Security used**. Most likely, if email is encrypted during transmission, the configuration will happen automatically without your involvement. However, if you have problems, you need to be aware of these possible settings:
  + An IMAP server uses port 143 unless it is secured and using SSL. IMAP over SSL (IMAPS) uses port 993.
  + A POP3 server uses port 110 unless it is secured and using SSL. POP3 over SSL uses port 995.
  + Outgoing email is normally sent using the protocol SMTP. A more secure alternative is [**S/MIME (Secure/Multipurpose Internet Mail Extensions)**](javascript://), which encrypts the email message and includes a digital signature to validate the identity of the sender. This feature is enabled after the email account is set up on the device. The activation process is automated for accounts through Microsoft Exchange and can be set up manually for other types of accounts. Look for this security option on the Advanced settings screen.

**A+ Exam Tip**

The A+ Core 1 exam expects you to know about POP3 and IMAP4, and the SSL and port settings they use, and might require you to use this information in configuring email on a mobile device. Before you sit for the exam, memorize the ports (including secure ports) and protocols discussed in this section and understand how this information is used to configure email on a mobile device. A project at the end of this chapter will give you practice with this process.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3dSyncing and Backing Up Mobile Devices

**A+ Core 1**

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 1.7

Given a scenario, use methods to perform mobile device synchronization.

* 3.9

Given a scenario, install and configure common devices.

**A+ Core 2**

* 1.1

Compare and contrast common operating system types and their purposes.

Synchronization, backup, and restore functions are much simpler now than they were in the past and require almost no attention from the user. Also, compatibility concerns between operating systems are less of an issue now as manufacturers continue to standardize file types and communication protocols. In this part of the chapter, you learn to sync with online accounts or third-party apps, sync with your desktop, update the OS, and back up settings. First, here’s the difference between syncing and backups:

* Syncing mirrors app data and other content among your devices and/or the cloud that use the same Apple or Google account. A photo taken or a calendar event created on one device is available in the cloud and all other devices. As another example, when you sync email, the Gmail app on your phone will show the same email messages and configuration settings as the Gmail interface in your browser on your computer.
* Backups are copies of app data, configuration settings, and other content stored in case you need it to recover from a failed, lost, or corrupted device.

### Sync to the Cloud

Syncing data to the cloud means that you can access your data from any device or any computer with a web browser connected to the Internet. (Google products work best in Google Chrome, of course.) You can sync contacts, application purchases and installations, email, pictures, music, videos, calendars, bookmarks, documents, location data on map apps, social media data, e-books, and even passwords.

**Caution**

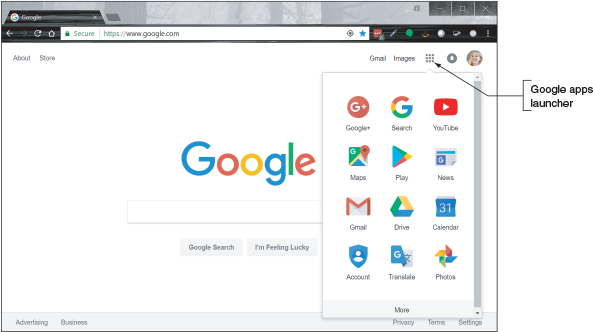
It’s not safe to store passwords in your browser. It’s much more secure to use a password manager app, such as KeePass or LastPass. KeePass stores passwords only on the local computer, which is more secure but less convenient. LastPass can store passwords in the cloud and sync passwords across devices, which is more convenient but less secure.

When you’re signed in to your Google or Apple account, both Google’s cloud and Apple’s iCloud can automatically sync nearly all content created in their OS-native apps across your devices. (You can choose whether to sync only over Wi-Fi so syncing doesn’t use up your cellular data allotment.) Here’s how it works:

* **Google storage in the cloud**. Android syncs Google apps or third-party apps on your device to your Google storage at [google.com](http://google.com/" \t "_blank); the first 15 GB of cloud storage is free. Use the Settings app on your device to manage what is synced. To access your content in the cloud, use any browser to go to [google.com](http://google.com/" \t "_blank) and sign in to your Google account. A [**single sign-on (SSO)**](javascript://), also called mutual authentication for multiple services, gives access to Gmail, Google Drive, Calendar, Contacts, and all other Google apps. Click the **Google apps** icon to select different apps, as shown in [Figure 9-34](javascript://). Many third-party apps can also sync their data through the Google account the mobile device is registered to, although the sync settings might be managed within the app rather than through the device’s Settings app.

**Figure 9-34**

Access Android content at [google.com](http://google.com/" \t "_blank)



Enlarge Image

Source: Google

* **iCloud storage in the cloud**. iOS syncs content to the Apple website at [icloud.com](http://icloud.com/" \t "_blank); the first 5 GB of cloud storage is free. To set up iCloud syncing, go to the **Settings** app on your iPad or iPhone, tap the user name, and tap **iCloud** to go to the screen (see [Figure 9-35](javascript://)) where you can decide which apps and data get synced and manage your iCloud storage.

**Figure 9-35**

Manage iCloud synchronization on a mobile device

Graphical user interface, text, application

Description automatically generated

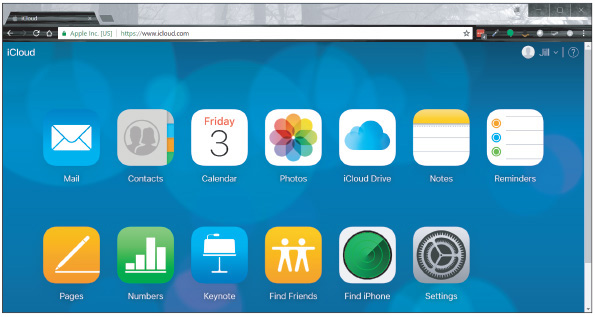
Enlarge Image

Source: iOS

You can access synced data in the cloud from your computer by signing in to your Apple account at [icloud.com](http://icloud.com/" \t "_blank). For example, the Launchpad or home page for your iCloud content (see [Figure 9-36](javascript://)) shows synced apps, including Mail, Contacts, Calendar, iCloud Drive, and Photos.

**Figure 9-36**

Access iOS content at [icloud.com](http://icloud.com/" \t "_blank)



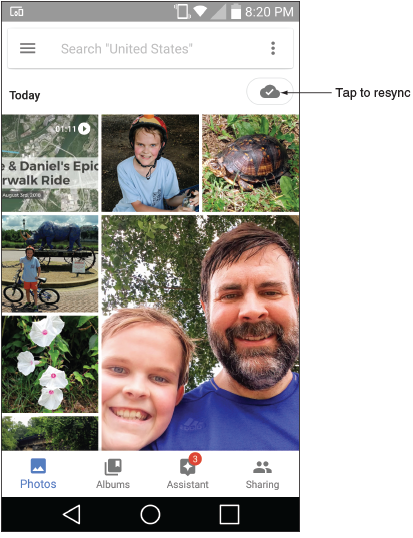
Enlarge Image

Source: [iCloud.com](http://icloud.com/" \t "_blank)

If you notice an account is not syncing correctly, resync information for the account through the app that holds the data. For example, [Figure 9-37](javascript://) shows the Photos app on an Android phone. To resync photos, tap the cloud icon in the upper-right corner of the screen.

**Figure 9-37**

If content fails to sync automatically, resync manually



Enlarge Image

Source: Android

### Sync to the Desktop

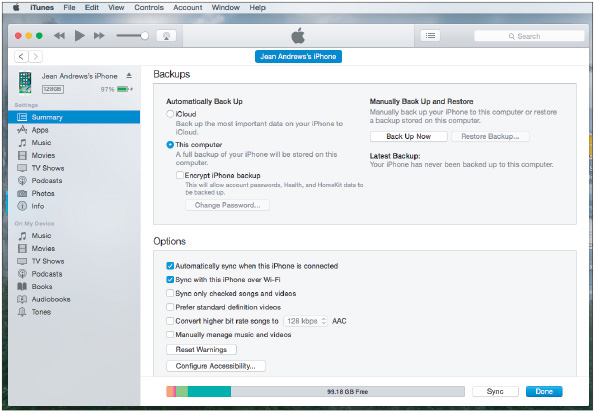
Syncing to the desktop can happen manually as you think to do it or you can set up your device for automatic syncing. The drawbacks of manual syncing are that it’s time consuming and the user must remember to do it on a regular basis. If it’s been six months since the last sync and the phone or tablet dies, the user loses six months’ worth of photos and videos. It can also be challenging to set up syncing to cover all that you might want to sync, such as text messages and third-party app data and settings. Manual or automatic syncing might require you to install software on the computer to manage the syncing.

Here are some manual syncing options:

* **USB connection and File Explorer**. The tried-and-true method for syncing photos and videos from a phone or tablet directly to the desktop is to plug the device into a USB connection with the computer (or a Lightning to USB connection on a Mac) and copy files from the device to the computer. For a Windows computer, you can use File Explorer to copy files from the device to your computer, which preserves the original quality of the media files, unlike some cloud-based sync services, which reduce resolution before storing in the cloud. An advantage of this type of syncing to a computer is that no extra software needs to be installed on your computer.
* **iTunes with iOS**. For iOS devices, you can install iTunes on a computer and use it to sync and back up the mobile device. After you install and start iTunes, connect your mobile device through a USB connection and iTunes will then recognize the device. For example, [Figure 9-38](javascript://) shows the iTunes window on a Mac with backup options at the top right and sync options at the lower right. After selecting the sync or backup settings you want, click **Sync** to sync the device and computer or **Back Up Now** to back up the device to your computer.

**Figure 9-38**

iTunes can sync or back up a mobile device with a Mac or Windows computer



Enlarge Image

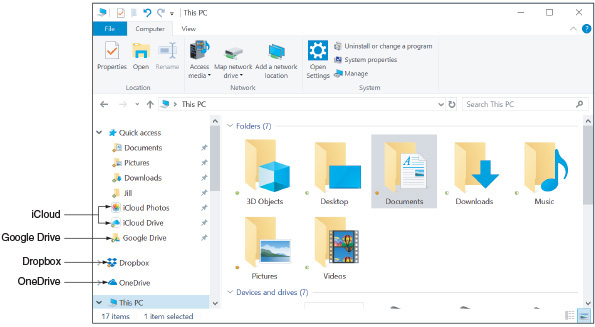
Source: iTunes

The following three options provide automatic syncing to the desktop. Each option requires you to install an application on the computer and configure the sync settings. Before you install the app, make sure the computer meets the minimum hardware and OS requirements needed to support the app:

* **Third-party syncing apps**. OneDrive, Dropbox, and other apps provide cloud-based file storage services and will sync entire folders in the background with no user intervention required to any computer or device that has the app installed and signed in. Make a change on one device and you immediately see it on another or in the cloud. OneDrive, Dropbox, and other syncing apps can install in Android and iOS mobile devices and in Windows and Linux on the desktop. [Figure 9-39](javascript://) shows File Explorer on a Windows 10 computer with synced folders for iCloud Photos, iCloud Drive, Google Drive, Dropbox, and OneDrive, all of which are also installed on one or more of the user’s mobile devices.

**Figure 9-39**

Use synchronization apps to sync files to your Windows computer



Enlarge Image

Sources: iCloud, Google, and Dropbox

* **Backup & Sync app with Android**. Sync an Android device to a Windows or Mac computer using the Backup & Sync app. When you install the app on your computer, it installs a Google Drive folder and can automatically sync files to the mobile device, the computer, and the cloud.
* **iCloud Drive with iOS**. As you know, you can sync app settings and other data on your iOS device to the Apple cloud at [icloud.com](http://icloud.com/" \t "_blank). In addition, when you turn on [**iCloud Drive**](javascript://), the Files app on an iPad or iPhone syncs files across devices and you can share these files with people in your contacts list. You can also install the iCloud Drive app on a computer so that files can sync to your desktop (refer back to [Figure 9-39](javascript://)), which is similar to the way Dropbox works. To turn on iCloud Drive on a device, open the **Settings** app, tap the user name, then tap **iCloud**. Verify that **iCloud Drive** is turned on and syncing the apps you want to sync. If iCloud Drive is installed on your Windows computer, content will also sync there.

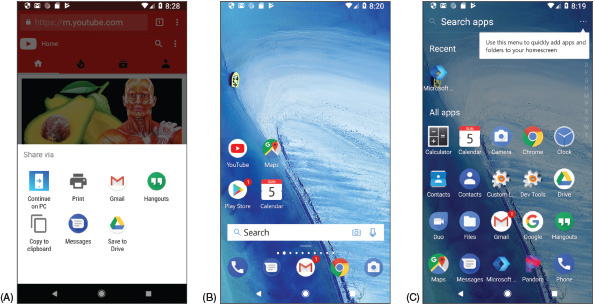
### Sync an Activity with Handoff and Continue on PC

In addition to syncing files and other content, you can sync activity in progress. For example, suppose you’re visiting a webpage on your smartphone, and you want to open that webpage in your desktop’s browser without searching for it again. Or suppose you’re working on a document on one device, and you want to continue your work on the other device. You can transfer the activity from the mobile device to the desktop and back, picking up on one device where you left off on the other.

* **Apple Handoff**. In macOS and iOS, the feature is called Handoff. Enable Handoff in the Settings menu on the iPhone or iPad and in the System Preferences menu on the Mac. When the device and computer are on the same Wi-Fi or Bluetooth network and signed in to the same Apple account, the Handoff icon appears on each device for activities transferrable from the other. Tap or click the icon to pick up an activity from the other device.
* **Microsoft Launcher or Continue on PC**. Windows 10 offers an Android app called Microsoft Launcher or an iOS app called Continue on PC. Both of these apps add a share option, called Continue on PC, into certain activities you perform on your phone and send to a Windows computer (see [Figure 9-40A](javascript://)). Android [**launchers**](javascript://) are apps that can replace Android’s default home screen (called the Pixel Launcher) to add different features and functionality. In the case of Microsoft Launcher, as shown in [Figure 9-40B](javascript://) and [Figure 9-40C](javascript://), the app makes the Android’s home screen look and function more like a Windows Mobile phone, including synchronization with your Windows desktop. Compare the home screen in [Figure 9-40B](javascript://) with the home screen in [Figure 9-6](javascript://) to identify subtle differences. To get started with Windows 10, open the **Settings** app and click **Phone**.

**Figure 9-40**

(A) Tap Continue on PC to pick up an Android activity on your Windows desktop; (B) the Microsoft launcher has made subtle changes to the Android home screen; (C) the launcher’s All apps screen is similar to the Windows Start screen



Enlarge Image

Source: Android

**Notes**

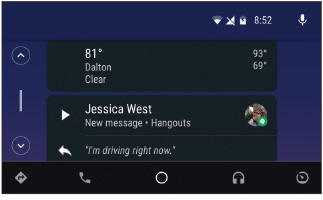
Many apps also include the ability to sync activities between devices, either within one user’s account or between accounts. Google Chrome, for example, syncs browsing history, settings, and bookmarks with all devices signed into Chrome using the same account. Microsoft’s OneNote syncs notes across devices and can sync notes to devices that belong to other people when you share a notebook.

### Sync to an Automobile

Many newer automobiles offer the option to use Bluetooth to pair a smartphone with the car’s computer for easy access to the phone’s music, navigation, and call features through the car’s media screen. While this is not true synchronization because most of the phone’s content stays on the phone and is not stored on the car’s computer, it does allow the user to control the phone through the car’s control panel or touch screen. [Figure 9-41](javascript://) shows information from an Android phone on a Kia Sedona’s touch screen using the Android Auto app. Apple devices use the Apple CarPlay app instead. Both apps include navigation, music, phone, and text message activities to interact with the user directly on the car’s screen.

**Figure 9-41**

Android Auto lets users check the weather, send a Hangouts message, or make a phone call using their vehicle’s touch screen



Source: Android Auto

**Notes**

You can emulate a car’s touch screen in Android Studio for testing apps in the Android Auto interface. You’ll need to download and install the testing tool Desktop Head Unit (DHU) in the SDK Manager, and you’ll need a real smartphone to connect with the DHU (not an emulated one). Learn more at [developer.android.com/training/auto/testing/](http://developer.android.com/training/auto/testing/" \t "_blank).

### Update the OS

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 limitation**](javascript://). 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, although not all devices provide this option.

To see if manual updates can be performed on your device, go to the **Settings** app and tap **About**. On the About screen, tap **System updates**, **Software update**, or a similar item. The device turns to the manufacturer’s website for information and reports any available updates.

Before installing an OS update, you might want to go to the website and read the release instructions about the update, called [**Product Release Instructions (PRI)**](javascript://), which typically describe new features or patches the update provides and how long the update will take. Later, if a device is giving problems after an OS update, check the PRI for information that might help you understand the nature of the problem.

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** in the left pane. On the right side, tap **Software Update**. Any available updates will be reported here and can be installed.

It’s a good idea to back up your mobile device’s files, settings, configurations, and profiles before performing an update. How to back up a device is discussed next.

### Back Up and Recovery

Suppose your mobile device is lost, stolen, or damaged beyond repair. Backups and recovery options need to be in place to prepare for these events. Here are some 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**](javascript://), because each file is backed up individually. File-level backups, however, don’t include your app data or OS settings, such as your Wi-Fi passwords, account profile, or device and app configuration.
* **Partial image-level backup**. A true [**image-level backup**](javascript://) includes everything on the device and can completely restore the device to its previous state. However, a mobile device OS 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 data files 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 a few configurations, such as app installations or third-party app configurations. For this reason, you might need to use an additional method of backing up data and settings for any critical third-party applications.

Generally, you can back up to the cloud or to your computer. Android provides a way to back up to Google Drive:

* **Google Drive backup**. To enable Android’s backup feature, open the **Settings** app, go to **System**, and then tap **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. Your backup data is stored on Google’s servers and is associated with your Google account.
* **Back up to computer**. You need a third-party app or a manufacturer’s app to create a detailed backup of the device configuration and content to your computer.

iOS can back up to a computer using iTunes or to the cloud using iCloud. The best practice is to use both methods:

* **iCloud Backup**. Go to **Settings** and tap the user name, then tap **iCloud**. Scroll down and tap **iCloud Backup**. When you turn on iCloud Backup, it backs up 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**. iCloud backs up app data, call history, device settings, text, photos, and videos unless these items are already included in iCloud syncing.
* **iTunes backup**. Open iTunes on your computer and connect your mobile device to the computer. You might have to enter your device passcode. In iTunes, select your device and click **Back Up Now**.

When deciding whether to back up to the cloud or a computer, consider that cloud backups using Google Drive or iCloud are readily accessible from any computer and happen automatically when you’re connected to Wi-Fi. The disadvantages are that you have less control over security of your data and you have to pay for cloud storage.

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

* **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 to set up the device as a new device. You’ll learn more about resetting a device later in this chapter. For iOS, if you have a backup on your computer and connect the device to your computer, iTunes gives you the option to recover 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 computer and the iTunes app.

**Notes**

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.

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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-4**Securing a Mobile Device

**A+ Core 1**

* 5.5

Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

**A+ Core 2**

* 2.8

Given a scenario, implement methods for securing mobile devices.

* 3.4

Given a scenario, troubleshoot mobile OS and application issues.

* 3.5

Given a scenario, troubleshoot 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 logs, voice mail, text messages, Dropbox, iCloud Drive, Google Maps, Hangouts, 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 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 controlling access to your devices and consider what apps you can use to protect the data. These methods are discussed in this part of the chapter along with BYOD (Bring Your Own Device) policies that might be used in an enterprise environment to secure corporate data stored on a device.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4aDevice Access Controls

**A+ Core 2**

* 2.8

Given a scenario, implement methods for securing mobile devices.

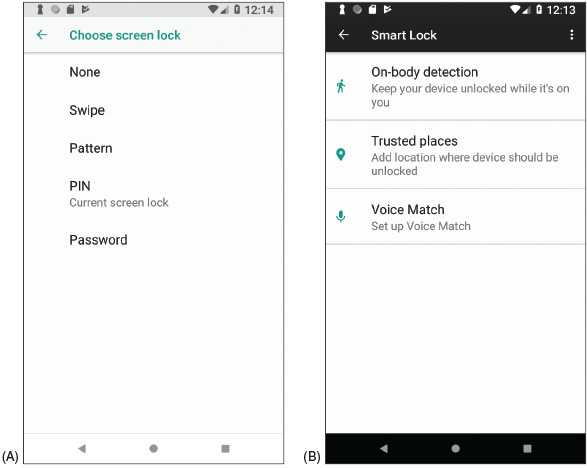
Consider the following lock methods to control access to the device.

* **Screen lock**. 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 lock**. Enter a numeric code with numbers.
  + **Passcode 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.
  + **Face lock**. Use the device’s camera to perform facial recognition.

[Figure 9-42A](javascript://) shows screen lock options on an Android smartphone, including a swipe lock, pattern lock, PIN lock, and passcode lock. Android also allows the user to set exceptions to the screen lock, as shown in [Figure 9-42B](javascript://). Using these options, the smartphone might stay unlocked when it detects it’s being carried or when it detects its location, such as the user’s home or office.

**Figure 9-42**

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



Enlarge Image

Source: Android

**Notes**

Fingerprint and facial recognition are both forms of biometric authentication. [**Biometric authentication**](javascript://) 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.** When you set a screen lock, you can specify that data be erased after a certain number of failed login attempts, or you can simply block further attempts. With iOS, the device locks after six failed attempts and you must wait before you can try again. If the device permanently locks and you’ve created a backup in iTunes, you can sync to the backup to access the phone. Otherwise, you’ll have to use recovery mode, which erases the device. With Android devices, login attempt restriction options vary by manufacturer. You can change the lock code online using the device’s associated Google account on the Find My Device website ([google.com/android/find](http://google.com/android/find" \t "_blank)), which also locates the device.

**Caution**

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

* **Full device encryption.** Both Android and iOS devices offer [**full device encryption**](javascript://), 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 stored on the device, not when it’s in motion or in use. When enabling encryption for the first time, it might take an hour or more to complete the encryption. Also, if the encryption process is interrupted during that time, some or all of the data will be lost.
* **Multifactor authentication**. Smartphones can be used to authenticate to services and networks (for example, email, cloud services, corporate network accounts, VPNs, or even Facebook) as one of the two or more techniques required for [**multifactor authentication**](javascript://). For example, you might first enter a password on a computer as the first authentication and then a code is sent as a text message to your smartphone; you must then enter the code in the computer as the second authentication. Another example might be that you enter a code in a computer that is at a certain location and the system you’re signing in to checks the GPS location of your smartphone to make sure it is near the computer. In addition, [**authenticator applications**](javascript://) can be installed on your smartphone and configured to provide multifactor authentication support for a huge variety of account types. Popular examples are Google Authenticator or Microsoft Authenticator, both of which work on either Android or iOS devices, or an independent competitor like Authy ([authy.com](http://authy.com/" \t "_blank)), which also works in Chrome OS.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4bSoftware Security

**A+ Core 2**

* 2.8

Given a scenario, implement methods for securing mobile devices.

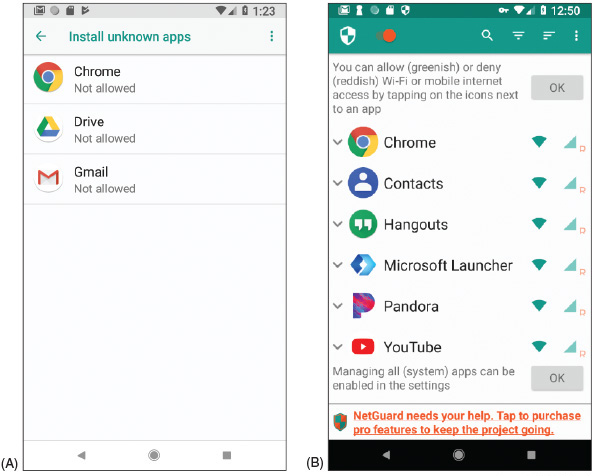
In addition to controlling access to a device, software can help secure data. Most of the methods discussed here require the user to understand the importance of a security measure and how to use it:

* **OS updates and patches.** Apply OS updates and patches to plug up security holes. Android automatically pushes updates to many of its devices, but iOS devices and many other mobile 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.
* **Trusted sources**. iOS devices are limited to installing apps only from Apple’s App Store. Android and Windows devices can download and install apps from other sources, only some of which are trustworthy. [**Trusted sources**](javascript://) generally include well-known app stores, such as Amazon Appstore for Android ([amazon.com/appstore](http://amazon.com/appstore" \t "_blank)) or SlideME ([slideme.org](http://slideme.org/" \t "_blank)). Other trusted sources might include your bank’s website, your employer, or your school, although often their apps are posted in Google Play ([play.google.com](http://play.google.com/" \t "_blank)) as well. Before downloading an app, look for lots of reviewer feedback as one measure of safety.

Android versions before Oreo allow you to limit app sources to only the Google Play Store, which can help reduce the threat of untrusted sources for apps. In the **Settings** app, tap **Security** and make sure that **Unknown sources** is unchecked. Beginning with Oreo, you can decide which apps are allowed to install other apps. To choose, go to **Settings > Apps & notifications > Advanced > Special app access > Install unknown apps** (see [Figure 9-43A](javascript://)). 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 9-43**

(A) Choose which apps can install apps from sources other than the Play Store; (B) choose which apps can access the Internet



Enlarge Image

Source: Android, NetGuard

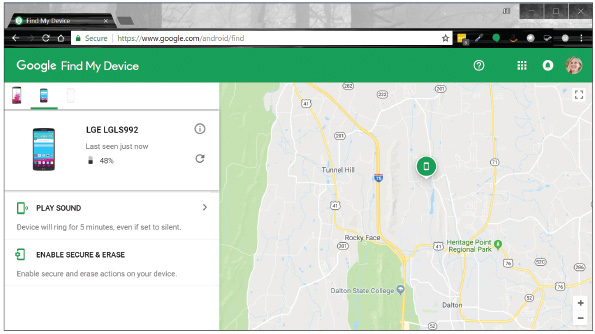
* **Firewalls.** As with Windows computers, a firewall on a mobile device helps control which apps or services can use network connections. When you install an app, you’re required to agree to the permissions it requests in order to get the app. A firewall gives you more control over an app’s network access. For example, a firewall can prevent the Facebook app from sending SMS messages.

Most firewall apps for mobile devices mimic a VPN connection, which forces all network communication to be routed through the firewall. [Figure 9-43B](javascript://) 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.

* **Android locator application and remote wipe**. You can use Find My Device ([google.com/android/find](http://google.com/android/find" \t "_blank)), Android’s built-in [**locator application**](javascript://), to locate your phone on a map, force it to ring at its highest volume, change the device password, or remotely erase all data from the device to protect your privacy, which is called a [**remote wipe**](javascript://). See [Figure 9-44](javascript://). To use the locator app to locate your device or perform a remote wipe, Find My Device must already be turned on in the **Security & location** menu in the Settings app. Third-party locator applications are also available in the Play Store.

**Figure 9-44**

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



Enlarge Image

Source: Google

* **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**, tap **iCloud**, and then turn **Find my iPad** or **Find my iPhone** on or off. 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4cMobile Security in Corporate Environments

**A+ Core 2**

* 2.8

Given a scenario, implement methods for securing mobile devices.

Corporations and schools might provide corporate-owned devices, which are secured and managed by corporate policies and procedures, or the organization might have [**BYOD (Bring Your Own Device)**](javascript://) policies and procedures. With BYOD, an employee or student is allowed to connect his own device to the corporate network. For security purposes, an organization configures the person’s device before allowing it to connect to the network.

Employees or employee groups in an organization are assigned [**security profiles**](javascript://), which are a set of policies and procedures to restrict how a user can access, create, and edit the organization’s resources. [**Profile security requirements**](javascript://) can be partially implemented by configuration requirements placed on BYOD and corporate-owned devices an employee uses. These device requirements, such as full device encryption, remote wipes, location apps, access control, authenticator apps, multifactor authentication, firewalls, anti-malware measures, or use of VPN connections, must be clearly outlined. Users must be educated on how to use them, and they must include assurance that devices continue to meet the baseline requirements.

Part of these requirements will likely include installation of a [**remote backup application**](javascript://), which remotely backs up the device’s data to a company file server. For example, Canopy Remote Backup by Atos ([canopy-cloud.com](http://canopy-cloud.com/" \t "_blank)) provides cloud-based backups for laptops, tablets, and smartphones.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4dCommon Mobile Device Malware Symptoms

**A+ Core 1**

* 5.5

Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

**A+ Core 2**

* 3.4

Given a scenario, troubleshoot mobile OS and application issues.

* 3.5

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

Android and Windows mobile devices are more susceptible to malware than iOS devices because apps can be downloaded from sites other than Google or Microsoft. With iOS devices, apps can be obtained only from the Apple App Store and are therefore more strictly vetted. However, for any mobile device, malware can be introduced by a Trojan that a user accepts (for example, as an email attachment) or by macros embedded in shared documents.

Here are some symptoms that indicate malware might be at work on an Android, iOS, or Windows Mobile device:

* **Power drain, slow data speeds, high resource utilization, leaked personal files or other data, strange text messages, and data transmission over limits.** Battery power draining faster than normal or slow data upload or download speeds can indicate that apps are running in the background to leak your data to online servers. For example, when the XAgent malware app installs on an Apple device with iOS version 7 or below, the app icon is hidden, and the app runs in the background. When you close the app, it restarts. The malware not only uses resources, it steals personal data and makes screenshots, which it sends to a remote command-and-control (C&C) server. A C&C server might send coded text messages back to the phone. If you receive strange text messages, suspect malware. Another indication of malware at work is a spike in data usage charges on your phone bill.
* **Dropped phone calls or weak signal.** Dropped phone calls can happen when malware is interfering and trying to eavesdrop on your conversations or is performing other background activities.
* **Unintended Wi-Fi and Bluetooth connections.** Malicious Wi-Fi hotspots and Bluetooth devices can hijack a device or inject it with malware. When a mobile device connects to a malicious Wi-Fi hotspot, the device can receive a malicious script that repeatedly reboots the device, which makes it unusable. To prevent this type of attack, avoid free Wi-Fi hotspots or use a VPN connection. To prevent a device from pairing with a malicious Bluetooth device, turn off Bluetooth when it’s not in use.
* **Unauthorized account access.** A malicious app can steal passwords and data from other apps and can pretend to be a different app to get access to online accounts. If you suspect an online account has been hacked, consider malware might be on the mobile device that uses this account.
* **Unauthorized location tracking**. Spyware apps installed on a mobile device can report its location to a C&C server.
* **Unauthorized use of camera or microphone.** Unauthorized surveillance is a sure sign of malware. Stalker spyware apps have been known to take photos and send them to a C&C server; send a text alert to a hacker and then add the hacker to a live call; use the microphone to record live conversations and then send the recording to a C&C server; report Facebook, Skype, Viber, and iMessage activity, including passwords and location data; and upload all photos, videos, and text messages to a C&C server.

**Notes**

When is spyware legal? Parents can legally install spyware (politely called monitoring software) on a minor child’s phone, tablet, or computer, and employers can monitor employee devices when they are company owned. One example is FlexiSPY ([flexispy.com](http://flexispy.com/" \t "_blank)), an app that runs in the background to monitor text, email, Facebook and other visited websites, apps, photos, videos, contacts, bookmarks, location tracking, and phone calls. It can also record calls and surrounding sounds. It comes with a mobile viewer app installed on the parent’s or employer’s smartphone.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4eMobile Device Malware Removal

**A+ Core 2**

* 2.8

Given a scenario, implement methods for securing mobile devices.

Here are general steps for removing malware from a mobile device, listed from least to most invasive:

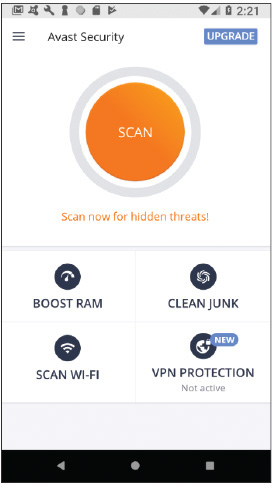
* **Uninstall the offending app.** If you can identify the malware app, close the app and uninstall it. If the app won’t uninstall, you can force stop the app or any background processes that belong to the app. For Android apps running in the background, open the Settings app, tap **Apps**, and tap a running app to force it to stop. Then try again to uninstall the app.
* **Update the OS**. Check to see if any updates are available for the device. For an iOS device, consider using iTunes on your computer to perform the update rather than updating iOS directly from the device.
* **Perform a factory reset**. The most surefire way to remove malware is to back up data and other content, reset the device to its factory default state, and then restore the content from backup. Reset options for Android and iOS are discussed later in this chapter.

After you have removed malware on a mobile device, you will want to keep it clean. Here are a few tips:

* Keep OS updates current.
* Educate users about the importance of privacy settings (for example, disable cookies and turn off Bluetooth when it’s not in use). Also, users should not open email attachments or download shared files from untrusted sources.
* Consider installing an anti-malware app. Apple claims that an iOS device cannot be infected with malware and does not make anti-malware apps available in the App Store. However, you can get an app from the App Store that monitors your device and scans for malware that might be in stored files, but is not installed. For Android and Windows Mobile devices, search online reviews and consider the features offered before deciding on an anti-malware app. An anti-malware app, such as Avast shown in [Figure 9-45](javascript://), can scan apps and files for malware, scan for unauthorized surveillance, monitor security and privacy settings, find the device when it’s lost, lock and remote wipe it, and maintain automatic updates. It might even include a firewall or a VPN feature.

**Figure 9-45**

Avast performs regular scans on an Android device



Source: Avast

**Applying Concepts**

### Rooting and Jailbreaking

To get more control over what can be done with an Android or iOS device, some people 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**](javascript://), and for iOS, the process is called [**jailbreaking**](javascript://). 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 malware. 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, which 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, try the **sudo su root** command, which in Linux allows you root access. If the prompt changes to #, the device is rooted.

**Notes**

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

* **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 Icy 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 using iTunes, the jailbreak will be removed.

Mobile devices and their reliance on wireless communication are closely related to another set of technologies, the Internet of Things or IoT. You might have heard of smart lights, smart TVs, and even smart houses. Let’s take a look at what the IoT is all about and begin exploring the special technologies developed for these purposes.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-5**The Internet of Things (IoT)

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.4

Compare and contrast wireless networking protocols.

There’s some debate on what makes up the [**Internet of Things (IoT)**](javascript://). Most people define IoT to be devices connected to the Internet for a specific purpose, such as a smart thermostat, that normally would not be connected to the Internet. Generally, it’s agreed that traditional computing devices, such as desktops, laptops, and smartphones, or traditional networking devices, such as routers, firewalls, and cable modems, are not IoT devices. However, as the line between “computer” and “Internet-connected non-computer” blurs, this distinction will become less relevant.

**Notes**

For a device to be considered part of the IoT, the device or its controller or bridge must have an IP address. After all, a node can’t connect to the Internet without an IP address.

In this part of the chapter, you learn about the wireless technologies used by IoT devices and how to set up a smart home network of IoT devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5aIoT Wireless Technologies

**A+ Core 1**

* 2.4

Compare and contrast wireless networking protocols.

In most cases, IoT devices are monitored and controlled by wireless connections. Besides Wi-Fi and Bluetooth, Z-Wave and Zigbee are two other wireless technologies commonly used by smart locks, smart light bulbs, and other IoT smart home devices. Here are the primary facts about Z-Wave and Zigbee:

* [**Z-Wave**](javascript://) transmits around the 900-MHz band and requires less power than Wi-Fi. It has a larger range than Bluetooth, reaching a range of up to 100 m in open air (though significantly less inside buildings).
* [**Zigbee**](javascript://) operates in either the 2.4-GHz band or the 900-MHz band, requires less power than Wi-Fi, and generally reaches a range of about 20 m inside but can reach much farther.
* Z-Wave and Zigbee are not compatible. Zigbee is faster than Z-Wave. Z-Wave and Zigbee use encryption and are considered safe from hackers.
* Both Z-Wave and Zigbee devices can connect in a mesh network, which means that devices can “hop” through other devices to reach the destination device. Z-Wave and Zigbee devices don’t inherently use TCP/IP without another protocol at work, such as Z/IP or Zigbee IP, that manages TCP/IP networking.
* Typically, Zigbee and Z-Wave compete about equally for the smart home device wireless standard of choice. Zigbee is the choice for large-scale commercial or industrial use because it is more robust.

**Notes**

When worker honeybees return to their nest, they do a dance that looks like a zig-zag pattern. Zigbee was named after this phenomenon: zig bee.

Another wireless standard used in the IoT industry is [**RFID (radio-frequency identification)**](javascript://), which is traditionally used in small tags that attach to and identify clothing inventory, car keys, bags, luggage, pets, cattle, hospital patients, and much more. An RFID tag contains a microchip and antenna and can be a passive or active tag. Active RFID tags have built-in batteries and transmitters to respond to commands or requests for information. Passive RFID tags, which cost much less, are essentially electronic barcodes that can be read from a few feet away without requiring line-of-sight access. Recently, RFID has been used for real-time IoT inventory management. RFID readers placed in manufacturing plants, warehouses, transportation systems, and stores can track inventory in real time to get products to customers faster and with less overhead.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

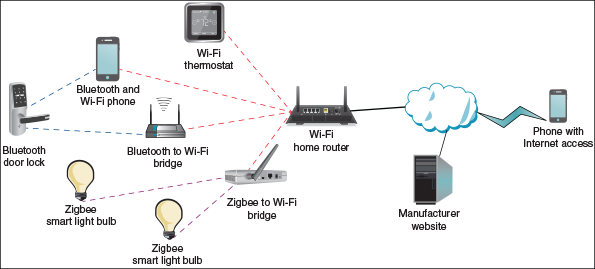
## 9-5bSetting Up a Smart Home

As an IT support technician, you might be called on to set up and support a smart home that uses IoT devices. For the most basic of smart homes, you’ll need:

* **Smartphone or tablet and Wi-Fi home network with Internet access**. Use a smartphone or tablet to set up and control smart devices by way of the device manufacturer’s app you install on the phone or tablet. Internet access is often required to use the app.
* **Smart home devices**. Examples are smart light bulbs, thermostats, security cameras, door locks, doorbells, refrigerators, televisions, and sound systems. Smart devices can be controlled by the manufacturer’s app installed on a phone or tablet. Some smart devices, such as a smart thermostat by Nest ([nest.com](http://nest.com/" \t "_blank)), can connect directly to a Wi-Fi network via an embedded Wi-Fi radio (see [Figure 9-46](javascript://)). Alternately, devices such as a door lock or thermostat might use Bluetooth to communicate with a phone or tablet within Bluetooth range or might use a bridge to connect to the Wi-Fi network. Other devices, such as smart light bulbs or a door lock, might use Zigbee, Z-Wave, or another wireless technology that the phone or tablet does not use. Such devices require a bridge device to connect them to the Wi-Fi network, as shown in [Figure 9-46](javascript://).

**Figure 9-46**

IoT devices connected to a smart home network may use a variety of wireless technologies



Enlarge Image

For smart devices to truly be IoT devices, you must be able to control them over the Internet. For that to happen, they must connect directly or through a bridge to a home Wi-Fi network that has Internet access. Notice in [Figure 9-46](javascript://) that the manufacturer’s website is involved when managing many IoT devices. For example, [Figure 9-47](javascript://) shows the webpage where two exterior webcams and two thermostats by Nest ([nest.com](http://nest.com/" \t "_blank)) can be monitored and managed from anywhere on the web.

**Figure 9-47**

IoT device manufacturers provide websites to manage their devices



Enlarge Image

Source: [nest.com](http://nest.com/" \t "_blank)

You can enhance a smart home network with smart speakers and controller hubs:

* **Smart speaker**. A [**smart speaker**](javascript://) includes digital assistant software that is voice activated. Amazon, Google, and Apple offer competing smart speakers, which connect by Wi-Fi to the Internet and include a search engine. For example, you can command a smart speaker to play music available over Pandora radio on the web. You can also ask it to tell you the capital of Myanmar. When you sign in to your Amazon, Google, or Apple account on the web, you can set up smart devices so that a smart speaker can turn them on or off and tell you information the devices provide. For example, you can ask a smart speaker with a screen, such as an Echo Show, to show you the live feed from a security camera at your front door. Here are three options for smart speakers:
  + **Alexa and Echo devices by Amazon**. An Echo smart speaker is voice activated and may include a screen. The embedded digital assistant is called Alexa. You can say, “Alexa, turn on the lights,” and the app does it. One low-end Echo product is the Echo Dot shown in [Figure 9-48](javascript://). You’ll need the Alexa app on an Android or iOS device to set up an Echo device.

**Figure 9-48**

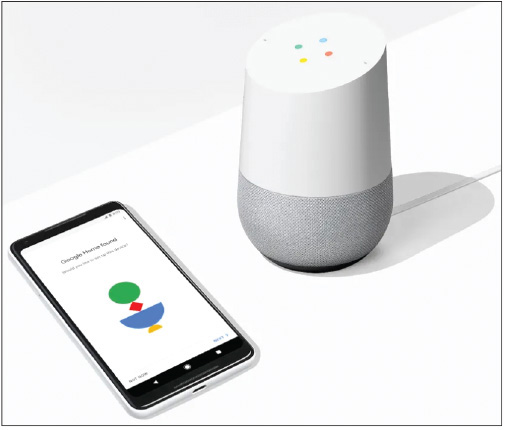
The orange light indicates the Echo Dot is on but not connected to a Wi-Fi network



* + **Google Assistant and Google Home**. Google Assistant is an app on an Android phone and is also embedded in a Google Home smart speaker. You control Google Assistant by starting with the spoken command “OK Google.” You set up the Google Home smart speaker using an app on your phone (see [Figure 9-49](javascript://)). You can also install the Google Assistant app on an iPhone or iPad so it can control smart devices set up to use the app.

**Figure 9-49**

Use a smartphone to set up a Google Home smart speaker



Source: [google.com](http://google.com/" \t "_blank)

* + **Siri and HomePod by Apple**. Siri is the digital assistant included with an iPhone or iPad and is also embedded in a HomePod smart speaker. A HomePod is set up using an iPhone or iPad.
* **Controller hub**. A smart speaker can access the web and turn Wi-Fi-connected smart devices on or off, but for a completely automated smart home experience, you need a controller hub. A [**controller hub**](javascript://), also called a smart home hub, can control smart devices that use different manufacturer apps and different wireless technologies, such as Wi-Fi, Bluetooth, Zigbee, or Z-Wave, to create an integrated smart home experience. For example, you can use a controller hub to coordinate dinner: When you approach your home, the garage door opens, the range turns on to warm up the soup, the room temperature is raised, and the kitchen lights are turned on. Two examples of hubs are Wink Hub ([wink.com](http://wink.com/" \t "_blank)) and Samsung SmartThings ([smartthings.com](http://smartthings.com/" \t "_blank)). In addition, software hubs such as Yonomi ([yonomi.co](http://yonomi.co/" \t "_blank)) install as apps on smartphones and tablets.

Some people start a smart home by installing one or two smart devices controlled from a smartphone. Later they add a smart speaker and other smart devices to manage lighting, climate, convenience features, security, and entertainment. They also add controller hubs to make all the devices work together.

**Applying Concepts**

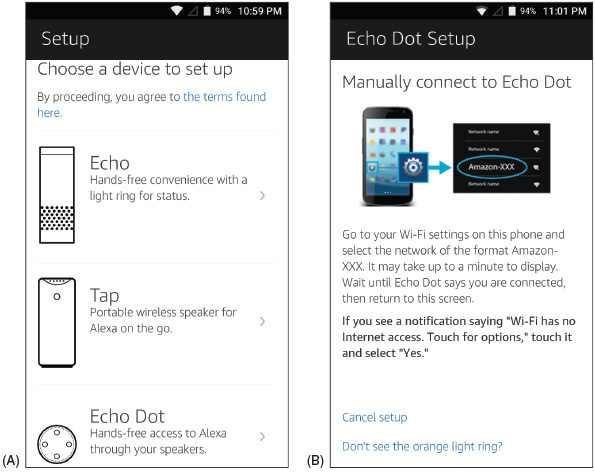
### Setting Up a Digital Assistant and Smart Speaker

One significant goal of manufacturers of IoT smart home devices is to make them easy to set up and connect to the home’s Wi-Fi network. However, the steps for setting up these devices vary somewhat among manufacturers, their products, and product models. Here, we’ll look at the general steps for configuring an Echo Dot from Amazon; you should use the more specific steps from your product’s manufacturer.

1. The Echo Dot and Alexa are set up and controlled from the Alexa app on a smartphone. Download and install the Alexa app first and sign in to your Amazon account. After Alexa is set up, you can also control Alexa from your Amazon account at [amazon.com](http://amazon.com/" \t "_blank).
2. Plug the Echo Dot into a wall outlet. After it powers up and the light turns orange, it’s ready to be paired with a smartphone. Refer back to [Figure 9-48](javascript://).
3. On the smartphone in the Alexa app, choose the Echo Dot from the device setup menu (see [Figure 9-50A](javascript://)).

**Figure 9-50**

(A) Choose the Echo Dot in the setup options; (B) connect the phone to the Dot’s Wi-Fi hotspot



Enlarge Image

Source: [amazon.com](http://amazon.com/" \t "_blank)

1. Echo Dot provides its own Wi-Fi hotspot to do the initial setup for another Wi-Fi network. First, connect the phone to the Dot’s Wi-Fi hotspot (see [Figure 9-50B](javascript://)). You can then configure the Dot to connect to your home’s Wi-Fi network.
2. Once the Dot is communicating with your local network, it’s ready to respond to voice commands. Use the wake word “Alexa” to activate the Dot, then say your command or request. You can change the wake word in the Alexa app. If you’re setting up a smart home network, you’re ready to add smart home devices to your Alexa account.

**Notes**

Some people like to use Alexa when traveling. In late 2018, Amazon introduced Echo Auto, which connects to your smartphone and vehicle for the Alexa experience on the road. Be aware, however, that Echo Auto uses data on your smartphone’s cellular data plan.

**Applying Concepts**

### Setting Up an IoT Smart Home Device

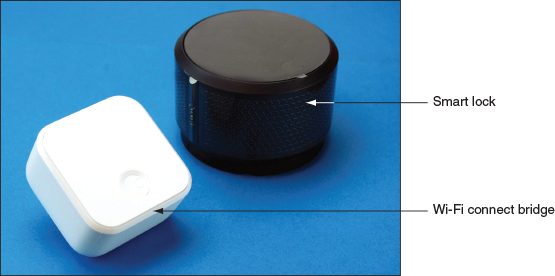
The following general steps apply to setting up many types of IoT devices:

1. Download the manufacturer’s app.
2. Open the app to follow the instructions for installation and configuration and to control the device from your smartphone. You might also need to install a bridge for devices that don’t use Wi-Fi.
3. To control the device with voice communication, enable the smart home device in your digital assistant account.

Using these general steps, we’re adding a smart door lock, the August Smart Lock Pro (see [Figure 9-51](javascript://)), to a smart home network. This smart lock by default is controlled via Bluetooth by your smartphone within Bluetooth range. In addition, we’re installing the August Connect, which is a bridge to connect the smart lock to your home Wi-Fi network so that you can control the smart lock from anywhere on the Internet or through a smart speaker such as Alexa.

**Figure 9-51**

The August Smart Lock Pro automatically unlocks or locks as the user’s Bluetooth-enabled smartphone moves closer or farther away

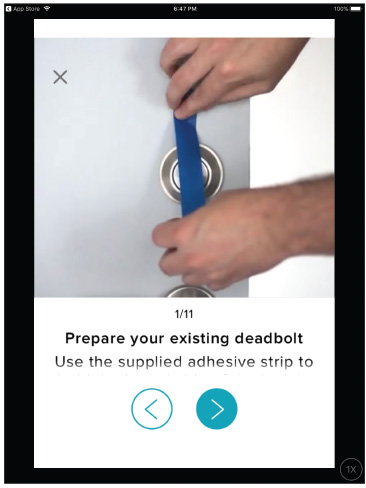


The steps above are general steps; you should follow the more specific directions provided by your device’s manufacturer:

1. Smart home device manufacturers usually provide their own app to control the device. Download and install the August Home app on your smartphone and create an account. This process might include security measures such as providing a photo of yourself, verifying your phone number with a texted security code, and verifying your email with an emailed security code.
2. Set up your smart lock in the app. The August Home app gives step-by-step video instruction for the lock installation (see [Figure 9-52](javascript://)). You can also search YouTube for demonstrations of this process for your device. A good video for the August Smart Lock is posted by Silver Eagle Locksmith at [youtube.com/watch?v=omrbvCVOcI8](http://youtube.com/watch?v=omrbvCVOcI8" \t "_blank).

**Figure 9-52**

Install the smart lock on existing deadbolt hardware



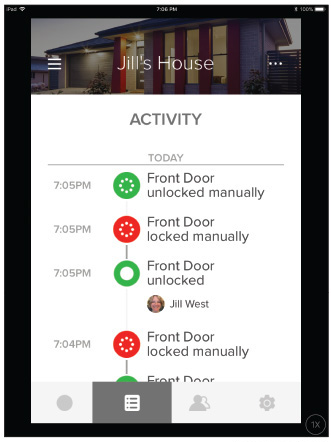
Source: August Home Inc.

1. With your smartphone within Bluetooth range of the door lock, the app will connect to the lock via Bluetooth and continue setup. You can name your house and the specific location of the lock, such as “Front Door.” The app might also install a firmware update at this time.
2. Calibrate the lock if instructed to do so. This involves setting the lock to “locked” and “unlocked” multiple times so the detectors inside the lock know how far to turn the latch.
3. Next, if you’re using an iPhone or iPad, you have the option to link the lock to HomeKit, which is the software used by HomePod, Apple’s smart speaker that works with Siri. We’re going to use Alexa, so we skip this step.
4. August Connect is a small box, called a bridge, that is mounted near the door lock and connects to the lock via Bluetooth and to your Wi-Fi home network so that you can control the lock from your smartphone anywhere on the Internet. To install the Connect, make sure your smartphone is connected to the home Wi-Fi network, then plug the Connect into a wall outlet near the lock’s location. The app detects the Connect and configures it for your home Wi-Fi network.

You can now control the lock from anywhere using the August Home app, and you can view a log of the lock’s activity, as shown in [Figure 9-53](javascript://). However, we want to also link it to the Alexa app.

**Figure 9-53**

See the lock’s recent activity, including which users have locked or unlocked the door

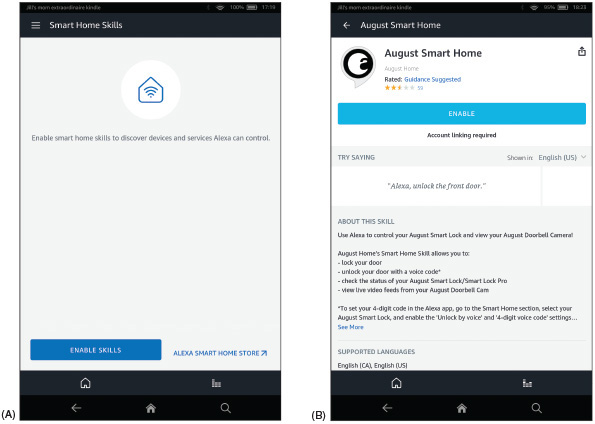


Source: August Home Inc.

1. Alexa relies on “skills” to add functionality to an Alexa account. Think about skills as apps within the Alexa app. To add smart home devices to Alexa, use the Alexa app to first enable Smart Home Skills (see [Figure 9-54A](javascript://)), then enable the August Smart Home skill (see [Figure 9-54B](javascript://)).

**Figure 9-54**

Using the Alexa app, (A) enable Smart Home Skills; (B) enable the August Smart Home skill



Enlarge Image

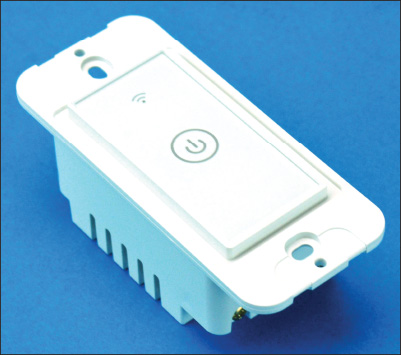
Source: [amazon.com](http://amazon.com/" \t "_blank)

1. After you link your August account and give Alexa permission to manage the lock, Alexa will discover the lock. Alexa will now respond to voice commands such as, “Alexa, tell August to lock the front door” and “Alexa, tell August to unlock the front door,” in which case you’ll also need to tell Alexa your PIN.

Let’s look at a couple more examples of IoT smart devices. The smart light switch by Meross ([meross.com](http://meross.com/" \t "_blank)), shown in [Figure 9-55](javascript://), uses Wi-Fi and the Meross app and can be controlled by Amazon Alexa or Google Assistant. The Honeywell wireless thermostat in [Figure 9-56](javascript://) uses Honeywell proprietary RedLINK wireless transmissions and can communicate with a Wi-Fi network via the RedLINK-to-Wi-Fi bridge, also shown in the figure, so that it can interact with Honeywell’s Total Comfort Care app. Both devices can also link to Amazon Alexa or Google Assistant.

**Figure 9-55**

Install this smart light switch to remotely control a room’s light, fan, or electric outlets



**Figure 9-56**

Use your phone, an Echo Dot, or a Google Home smart speaker to control this wireless thermostat



Enlarge Image

The setup for both the Wi-Fi smart light switch and the thermostat using RedLINK wireless is similar to how the Bluetooth thermostat was set up:

1. Install the app.
2. Install the device in the app. If the device does not use Wi-Fi, install an optional bridge device.
3. Connect the device to a smart speaker.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-6**Troubleshooting Mobile Devices

**A+ Core 1**

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 5.5

Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

**A+ Core 2**

* 3.4

Given a scenario, troubleshoot mobile OS and application issues.

* 3.5

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

As an IT support technician for mobile devices, know that they contain few [**field replaceable units (FRU)**](javascript://), or hardware that can be replaced by field technicians. The cost of replacement, including parts and labor, generally exceeds the value of fixing the device. Although it is possible to replace the screens in some mobile devices, a support technician is generally not expected to take the time to do so.

There are, however, many problems with a device that you can troubleshoot using tools within the OS. When learning to troubleshoot any OS or device, remember the web is a great source of information. Depend on the [support.google.com/googleplay](http://support.google.com/googleplay" \t "_blank) and [support.apple.com](http://support.apple.com/" \t "_blank) 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 many common symptoms and problems and what to do about them.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-6aTroubleshooting Techniques

**A+ Core 1**

* 5.5

Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

**A+ Core 2**

* 3.4

Given a scenario, troubleshoot mobile OS and application issues.

* 3.5

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

The following steps are ordered to solve a problem while making the least 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. Too many open apps can shorten battery life and slow down device performance. 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) and reboot the device (also called a hard boot).
3. Update, repair, or reinstall the OS, or recover the system from the last backup.
4. Start over by resetting the device to its factory state (all data and settings are lost).

Earlier in the chapter, you learned how to close, uninstall, and reinstall an app. Let’s look at the last three steps in a little more detail. For more specific instructions, search the website of the device manufacturer.

### Restart or Reboot the Device

A restart powers down the device and restarts it, which is similar to a Windows restart. A reboot, also called a hard boot, is similar to a Windows shutdown and performs a full clean boot. First try a restart, and if that doesn’t fix the problem, try a hard boot:

1. **Restart the device, also called a soft boot.** To restart an Android device, press and hold the power button, and select **restart**. To restart an iOS device, press and hold the Side button and slide the power-off message to the right. To turn the device back on, press and hold the Android power button or iOS Side button. Power cycling a smartphone every few days is a good idea to keep the phone functioning at peak efficiency.
2. **Reboot the device using a hard boot.** When the menus in a device don’t work or the device freezes entirely, a full clean boot might help. For most Android devices, hold down the power button and volume-down button at the same time. (Check Android device manufacturers for details.) To reboot an iPhone X, hold down either volume button and the Side button until the Apple logo appears; for an iPad or older iPhone, press and hold the Side button and the Home button.

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:

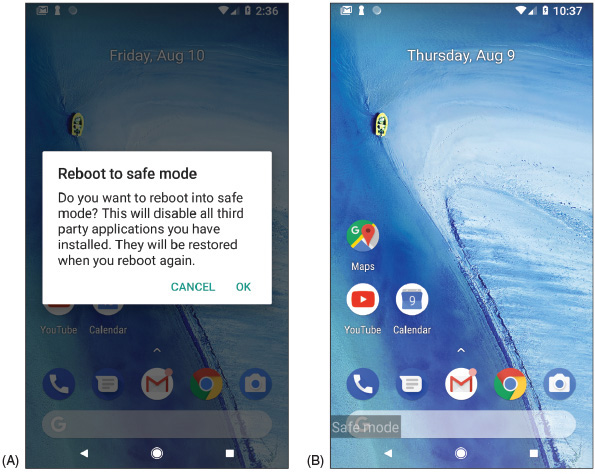
1. **Back up content and settings.** Before you try any of the techniques in this section, first try to back up data and settings using one or more of the methods discussed earlier in the chapter.
2. **Update the OS.** Try installing any updates, if available.

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. Be aware, however, that booting to Safe Mode might result in the loss of some settings, such as synchronization 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 9-57A](javascript://) appears. Tap **OK** to restart the phone in Safe Mode, as shown in [Figure 9-57B](javascript://). 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 9-57**

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



Enlarge Image

Source: Android

1. **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.

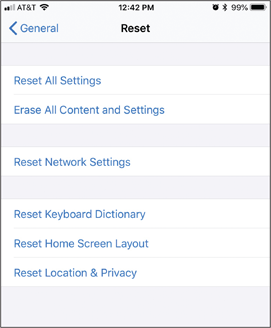
Several troubleshooting apps have been developed to help resolve Android problems. Most of these apps work only if they have already been installed before the problem occurs. If you have not already installed a troubleshooting app, your best resource at this point is to do a Google search on the problem 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 **Reset**. On the Reset screen (see [Figure 9-58](javascript://)), tap **Reset All Settings**.

**Figure 9-58**

The Reset screen on an iPhone

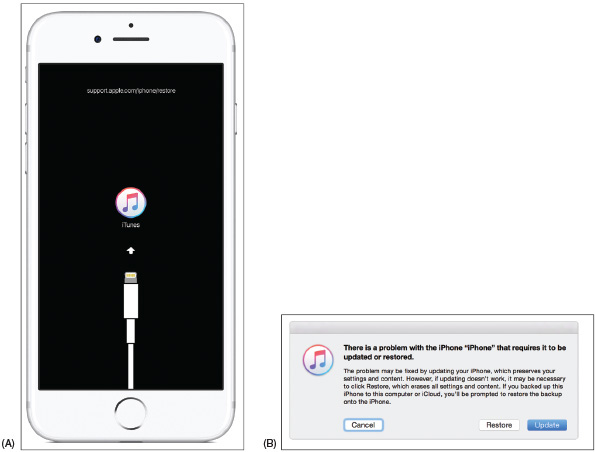


Source: iOS

1. **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 9-58](javascript://)). Then tap **Restore** and **iCloud backup**. You’ll need to sign in to iCloud.
   * **Restore the device from iTunes.** If you have used iTunes to back up the device, connect the device to your computer, start **iTunes**, and click **Restore Backup**. Refer back to [Figure 9-38](javascript://). In the figure, notice the option is grayed out because there is no iTunes backup for this connected iPhone.
2. **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 iTunes to try to reinstall iOS without losing your data. (You can use iTunes on any 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 iTunes. For an iPhone X or iPhone 8, 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 9-59A](javascript://)). For older iPhones or iPads, press and hold the Home button and Side button. Follow the directions until you see the screen shown in [Figure 9-59B](javascript://), and then click **Update**. The latest version of iOS that works on your device should install and keep your data.

**Figure 9-59**

Use recovery mode with iTunes to reinstall iOS on an iOS device that will not start



Enlarge Image

Source: [https://support.apple.com/en-us/HT201412](https://support.apple.com/en-us/HT201412" \t "_blank)

### 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.

1. **Factory reset from the Settings app.** In Android, open the **Settings** app, tap **System**, 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**.
2. **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.
3. **Factory reset and restore from iTunes backup (iOS only).** If an iOS device won’t turn on and you’ve already tried to reinstall iOS using iTunes, as discussed above, you can perform a factory reset using iTunes. Connect the device to a computer that has iTunes installed and go to recovery mode in iTunes, as you learned to do earlier. Then click **Restore** (see [Figure 9-59B](javascript://)). All data and settings on the device are erased and iOS is reinstalled. If you have previously used iTunes on 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.

**Notes**

If you have forgotten your iOS passcode, you are given six attempts to enter it before the device is disabled. You will need to use iTunes to reinstall iOS and you will lose all your data and settings unless you have an iTunes backup to restore the device from backup. If you have backed up to iCloud and you sign into iOS for the first time with your Apple ID, 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 below, or take the device to the place of purchase for repair.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-6bCommon Problems and Solutions

**A+ Core 1**

* 1.6

Given a scenario, configure basic mobile device network connectivity and application support.

* 5.5

Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

**A+ Core 2**

* 3.4

Given a scenario, troubleshoot mobile OS and application issues.

* 3.5

Given a scenario, troubleshoot mobile OS and application security 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:

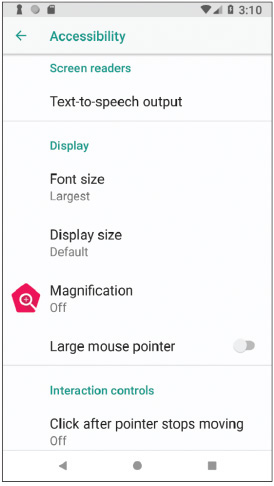
* **Short battery life or power drain**. Too many apps or malware running in the background will drain the battery quickly, as will Wi-Fi, Bluetooth, or other wireless technologies. Disable wireless connections and close apps when you’re not using them to save battery juice. Consider that malware might be at work; how to address malware is covered earlier in the chapter. If the battery charge still lasts an extremely short time, try exchanging the AC adapter (charger). 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.
* **Inaccurate touch screen response**. A cover on the screen can result in inaccurate touch screen responses. Also, accessibility settings can alter a touch screen’s performance. Check accessibility settings in the Settings app. Hold duration is a particular suspect, as are touch location assistance and screen auto-rotate.
* **Touch screen nonresponsive**. Here are some tips to try when a touch screen is giving you problems:
  + Clean the screen with a soft, lint-free cloth.
  + Don’t use the touch screen when your hands are wet or you are wearing gloves.
  + Restart the device.
  + Remove any plastic sheet or film protecting the touch screen. Some screen protectors are too thick and interfere with the touch screen interface, or bubbles and debris under the screen protector can cause problems. Use a screen protector that is approved for your device and carefully follow instructions for installing it. Turn on the screen protector’s touch sensitivity setting if available.
  + 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.
* **No sound or distorted sound from speakers**. This might seem obvious, but first make sure the volume is turned up by pressing the device’s physical **Up** volume button. Also, the problem could be that the sound output for the device is being misdirected. Check to see if Bluetooth is on; if it is, turn it off to make sure the device is not inadvertently connected to a Bluetooth headset or car stereo system. Also check Accessibility settings. Some of the Accessibility audio settings can interfere with normal operation of the device’s built-in speaker system.
* **Dim display**. Try increasing the brightness. This is especially helpful when trying to view the screen in bright daylight, but increasing the brightness level will also drain the battery more quickly. For Android, open the notifications shade, then slide the brightness slider to the right to brighten the screen. Make sure the Auto option is not selected so that you have more control over the screen’s brightness level.

For the iPad and older iPhones, swipe up to show the control center; on an iPhone X, swipe down from the upper-right corner to show the control center. In the control center, you can adjust the screen brightness.

Sometimes individual apps will control the screen brightness separately from the OS, so also check brightness settings within an app. Also check color and contrast settings on the accessibility menu in the Settings app (for Android, see [Figure 9-60](javascript://)).

**Figure 9-60**

Accessibility settings can make a mobile device act in unexpected ways

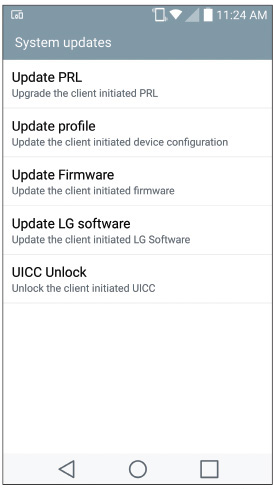


Source: Android

* **Cannot broadcast to external monitor**. Many mobile devices can wirelessly mirror, or [**cast**](javascript://), their displays to a TV, monitor, projector, or to a dongle attached to one of these display devices. Android devices rely on Miracast technology, while iOS devices use AirPlay. When troubleshooting, first confirm that both devices are turned on (and not in sleep mode), placed closely enough to each other, casting is enabled where needed, and devices are connected to the same Wi-Fi network. You can also check for available updates on each device. Next, consider sources of interference, such as crowded Wi-Fi bands, and check that the Wi-Fi router is set to prioritize Wi-Fi multimedia (WMM) traffic. A VPN app on the device sometimes disables the casting feature because of the way cast technology seems to pose a threat to VPN security. It might be necessary to uninstall third-party VPN apps for casting to work properly.
* **Bluetooth connectivity issues**. Turn the Bluetooth radio off and then back on again. Devices typically limit the time they’re available for pairing, so reactivating Bluetooth restarts the pairing process. In Bluetooth settings, you might be able to adjust the visibility timeout so devices have more time to discover each other. You can also delete all known Bluetooth devices in the Settings app to try the pairing process from the beginning. Sometimes an OS update will cause issues with Wi-Fi network connectivity or Bluetooth pairings. In this case, reset network settings in the Settings app. This restores network settings to factory defaults, and then you can attempt pairing again.
* **Wi-Fi connectivity problems**. Intermittent connectivity problems or no wireless connectivity might be caused by problems with the signal that is being broadcast from the router or access point. First make sure the access point and router are working correctly, that they’re positioned closely enough to each other, that the Wi-Fi network you want to connect to is visible to the device (not hidden), and that you’re using the correct security key. For Wi-Fi issues on the device side, first start with Wi-Fi settings in the Settings app for the network to which you’re trying to connect. Try renewing the IP address, and if that doesn’t work, tell the device to forget the network and then retry connecting to the network. Finally, try resetting the network settings. By default, many mobile devices stop attempting to reconnect to a weak Wi-Fi signal to conserve battery power, but you can sometimes change this setting so the device will attempt to maintain a connection even with a weak signal.
* **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**](javascript://), which manages the cellular, Wi-Fi, and Bluetooth radios. This is sometimes referred to as a [**baseband update**](javascript://). 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, usually that option will be available in the Settings app (see [Figure 9-61](javascript://)) in the same place as the OS update option. You might also be able to download software from the device’s manufacturer that can apply updates to the device through a USB connection with your computer. Examples are iTunes ([apple.com/itunes](http://apple.com/itunes" \t "_blank)) for Apple devices, LG PC Suite ([lg.com/us/support/software-firmware-drivers](http://lg.com/us/support/software-firmware-drivers" \t "_blank)) for LG devices, and HTC Sync Manager ([htc.com/us/software/htc-sync-manager](http://htc.com/us/software/htc-sync-manager" \t "_blank)) for HTC devices. These apps can also be used for synchronization and backup functions. Be careful when applying a firmware update, as a failed update can “brick” the device, which means to make it useless.

**Figure 9-61**

This LG phone lists several options for applying updates

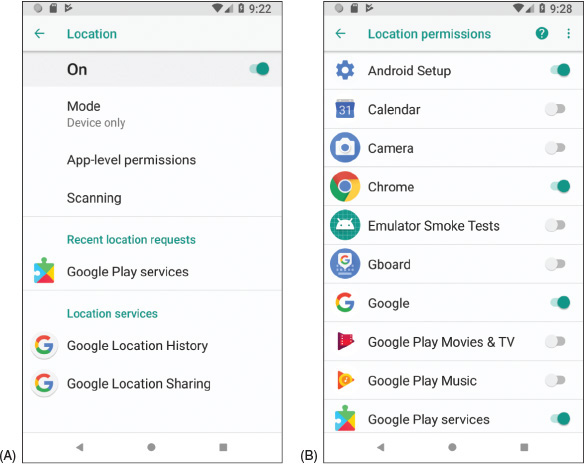


Source: Android

* **GPS not functioning**. **[Geotracking](javascript://)**, which is the identification of a device’s location to track the device’s movements, relies heavily on GPS location information. For example, Siri checks the device’s current location before recommending Italian restaurants in the area. Many apps can only access this information if Location services are enabled on the device (however, emergency calls can use location information even if Location services are not enabled). If an app is having trouble accessing location-specific information, check the Location services settings in the Settings app, as shown in [Figure 9-62](javascript://).

**Figure 9-62**

(A) Manage Location services in the Settings app, and (B) fine-tune which apps can use Location services



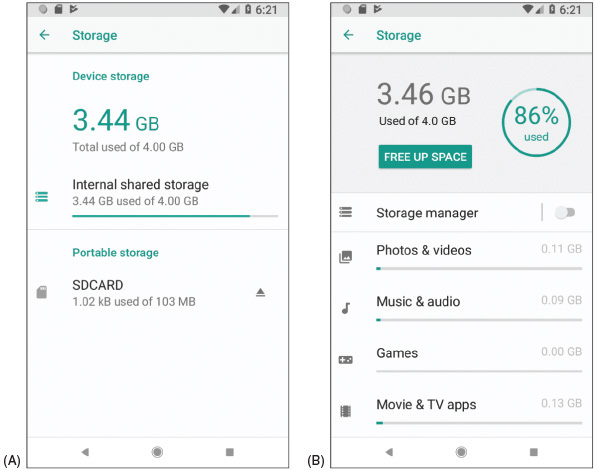
Enlarge Image

Source: Android

* **Unable to decrypt email**. Email encryption is done using a public key and a private key. You distribute your public key to those who want to send you encrypted email and you keep the private key on your device. If your device is unable to decrypt email, most likely you’ll need to generate a new public key and private key and then distribute your new public key to those who send you encrypted email. Search the website of the email app you are using for encryption to find instructions for setting up new public and private keys and for other tips on troubleshooting decrypting problems.
* **Apps not loading**. When apps load slowly or not at all, a hot or failing battery might be the problem. Having too many apps open at once will use up memory and 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. The Settings app displays how much storage space is available (see [Figure 9-63A](javascript://)) and what content can be removed (see [Figure 9-63B](javascript://)). 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.

**Figure 9-63**

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



Enlarge Image

Source: Android

* **App log errors**. Some apps maintain logs of errors that can be useful to technical support staff for the app. When helping you troubleshoot a problem, an app support technician might give you specific steps for accessing those logs.
* **Frozen system**. Consider that the battery may be low. Try recharging the battery for at least an hour. Then follow directions given earlier to reboot the device using a hard boot. If that doesn’t work, move on to reinstall the OS, recover the system from backup, and finally reset the device to its factory state.
* **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](http://accounts.google.com/" \t "_blank) and search for additional methods and tools to unlock your device.

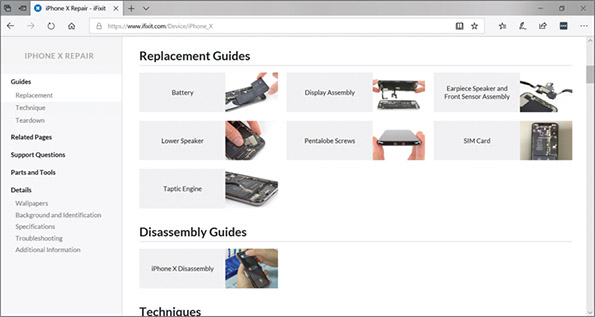
If you have forgotten the passcode for an iOS device, Apple advises that your only solution is to reset the device, which erases all data and settings, and then restore the device from a backup. You can restore from a backup stored in iTunes on your computer or from iCloud.

* **Overheating**. For a true overheating problem where the device is too hot to touch safely, power off and replace the device. However, all devices can get fairly warm if the display is left on for too long, if the surrounding environment is particularly hot, if the device is sitting on a blanket or other soft surface, if the case is not properly vented, if the battery is going bad, or if the device remains plugged in to a power source for a long period of time. Don’t use a mobile device for too long in direct sunlight, turn off the display when you’re not using it, and close apps that you’re not using. This will also help conserve battery power.

If you know where the battery is located inside a mobile device, check for heat originating from that area of the device. If the area is hot, replacing the battery might be your solution. First check if the phone is under warranty. If the phone is not under warranty, open the case and examine the battery for damage. Is it swollen or warped? If so, replace the battery. For most mobile devices, you can find teardown instructions, videos, tools, and replacement parts for purchase online at various websites, such as [ifixit.com](http://ifixit.com/" \t "_blank) (see [Figure 9-64](javascript://)). If the phone is under warranty, you might be able to tell if the battery is swollen or warped by laying the phone on a flat surface. If the phone itself appears warped, take it in for repair.

**Figure 9-64**

At [ifixit.com](http://ifixit.com/" \t "_blank), you can find instructions and purchase tools or parts to replace an iPhone battery



Enlarge Image

Source: [ifixit.com](http://ifixit.com/" \t "_blank)

**Notes**

Some Android smartphones provide information about the device when you enter **\*#\*#4636#\*#\*** in the phone’s dialer keypad. In the screen that appears, select **Battery Information**. If the Battery Health screen reports “unknown,” suspect a bad battery. The screen also reports the temperature of the battery, which should be less than .

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-7a**Chapter Summary**

### Types of Mobile Devices

* Mobile devices an IT support technician might be called on to service include smartphones, tablets, lightweight laptops, e-readers, GPS devices, and wearable technology devices such as smart watches, fitness monitors, and VR or AR headsets.

### Mobile Device Operating Systems

* The most popular operating systems used on mobile devices include Android by Google, iOS by Apple, Windows and Windows Mobile by Microsoft, and Chrome OS by Google.
* Android is an open source OS, and anyone can develop and sell Android apps or variations in the Android OS. Google is the major distributor of Android and Android apps are available on its Google Play website.
* iOS by Apple is used only on Apple devices, including the iPhone and iPad. Apps for iOS are distributed solely by Apple.
* Windows Mobile by Microsoft installs on smartphones and uses the same version numbers as Windows for desktops, laptops, and tablets.
* Chrome OS is designed solely for use on Google’s Chromebook, which is a tablet, lightweight laptop, or convertible laptop-tablet available from many different manufacturers. Chrome OS relies heavily on the Chrome browser and an active Internet connection. Chrome OS apps are distributed through the Chrome Web Store, and apps for the newer Chromebooks are distributed from the Google Play Store.

### Configuring and Syncing a Mobile Device

* A mobile device might have several antennas for wireless connections—primarily Wi-Fi, GPS, Bluetooth, NFC, and cellular. The device uses a Wi-Fi or cellular antenna to connect to a LAN (local area network), a WAN (wide area network), or to create its own hotspot, and it uses Bluetooth or NFC to connect to a PAN (personal area network). A wired connection might use a microUSB, miniUSB, USB-C, or proprietary port, such as the Lightning port by Apple, for syncing with a computer or tethering to provide the computer with cellular WAN access.
* Email can be accessed on a mobile device through a browser or an email client. Email providers include Gmail (by Google), iCloud (by Apple), Yahoo! (owned by Verizon), or Outlook/Hotmail/Live (Microsoft’s public email services for individuals). Microsoft also offers Exchange, its private enterprise email service that is hosted on corporation or ISP servers, or Exchange Online, which is hosted on Microsoft servers.
* Syncing mirrors app data and other content among your devices and/or the cloud that use the same Apple or Google account. Backups are copies of app data, configuration settings, and other content in case you need it to recover from a failed, lost, or corrupted device.

### Securing a Mobile Device

* 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. You can also use the mobile device as an authentication factor to increase security for access to other services and networks.
* Secure mobile device data and resources by regularly updating and patching the OS, using an anti-malware app, getting apps only from trusted sources, implementing a firewall, and configuring a locator app and the ability to remote wipe the device.
* In corporate environments, profile security might require the use of full device encryption, remote backups, remote wipes, access control to the device, firewalls, anti-malware measures, and VPN connections to protect company resources on the mobile device.
* Symptoms of malware on mobile devices include slow performance, short battery life, power drain, slow data speeds, leaked personal files or data, data transmission over limits, signal drops, weak signal, unintended Wi-Fi connections, unintended Bluetooth pairing, unauthorized account access, unauthorized location tracking, unauthorized camera or microphone activation, and high resource utilization.
* To remediate an infected device, uninstall the offending app, update the OS, and/or do a factory reset on the device.

### The Internet of Things (IoT)

* The IoT is made up of any device connected to a network or to the Internet, including a plethora of devices from thermostats and light switches to security cameras and door locks, but not including traditional computing devices, such as desktops, laptops, and smartphones, or traditional networking devices, such as routers, firewalls, and cable modems.
* Wireless technologies used by IoT devices include Wi-Fi, Bluetooth, Z-Wave, and Zigbee. RFID is used to passively or actively track items and inventory, such as shipped packages, clothing inventory, hospital patients, and your car keys, and can be used in an automated IoT inventory system.
* Zigbee is faster and more robust than Z-Wave and is better suited for industrial and large-scale commercial use.
* A smart home requires a Wi-Fi network with Internet access, a smartphone or tablet, smart home devices, and optional smart speakers, controller hubs, and bridges.

### Troubleshooting Mobile Devices

* To troubleshoot a mobile device using tools in the OS, you can close running apps, uninstall and reinstall an app, reboot the device, update the OS, reset all settings (iOS only), use Safe Mode (Android only), use Recovery mode, or perform a factory reset.
* To address specific, common symptoms on a mobile device, you might need to check accessibility settings, replace the battery if it’s not under warranty, change the way a device is used, remove protective coverings that are causing interference, check wired or wireless connection configurations, adjust device settings, or consult with tech support for the device manufacturer or app.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-7b**Key Terms**

For explanations of key terms, see the Glossary for this text.

* **airplane mode**
* [**Android**](javascript://)
* [**app drawer**](javascript://)
* [**App Store**](javascript://)
* [**Apple ID**](javascript://)
* [**AR (augmented reality) headset**](javascript://)
* [**authenticator application**](javascript://)
* [**baseband update**](javascript://)
* [**biometric authentication**](javascript://)
* **Bluetooth**
* [**BYOD (Bring Your Own Device)**](javascript://)
* [**cast**](javascript://)
* [**Chrome OS**](javascript://)
* [**commercial license**](javascript://)
* [**controller hub**](javascript://)
* [**digital assistant**](javascript://)
* [**dock**](javascript://)
* [**emulator**](javascript://)
* [**end-of-life limitation**](javascript://)
* [**e-reader**](javascript://)
* [**Exchange Online**](javascript://)
* [**favorites tray**](javascript://)
* [**file-level backup**](javascript://)
* [**fitness monitoring**](javascript://)
* [**FRU (field replaceable unit)**](javascript://)
* [**full device encryption**](javascript://)
* [**geotracking**](javascript://)
* [**Gmail**](javascript://)
* [**Google account**](javascript://)
* [**Google Play**](javascript://)
* **GPS (Global Positioning System)**
* [**Home button**](javascript://)
* [**iCloud**](javascript://)
* [**iCloud Drive**](javascript://)
* [**image-level backup**](javascript://)
* [**IMEI (International Mobile Equipment Identity)**](javascript://)
* [**IMSI (International Mobile Subscriber Identity)**](javascript://)
* [**iOS**](javascript://)
* [**IoT (Internet of Things)**](javascript://)
* [**iPad**](javascript://)
* [**iPhone**](javascript://)
* [**IR (infrared)**](javascript://)
* [**iTunes**](javascript://)
* [**jailbreaking**](javascript://)
* [**launcher**](javascript://)
* [**Lightning port**](javascript://)
* [**locator application**](javascript://)
* [**macOS**](javascript://)
* [**Microsoft Store**](javascript://)
* **microUSB**
* **miniUSB**
* [**multifactor authentication**](javascript://)
* [**NFC (Near Field Communication)**](javascript://)
* [**notification**](javascript://)
* [**open source**](javascript://)
* [**paired**](javascript://)
* [**PRI (Product Release Instructions)**](javascript://)
* [**PRL (Preferred Roaming List)**](javascript://)
* [**profile security requirements**](javascript://)
* [**radio firmware**](javascript://)
* [**remote backup application**](javascript://)
* [**remote wipe**](javascript://)
* [**RFID (radio-frequency identification)**](javascript://)
* [**rooting**](javascript://)
* [**SDK (Software Development Kit)**](javascript://)
* [**security profile**](javascript://)
* [**Side button**](javascript://)
* [**smartphone**](javascript://)
* [**smart speaker**](javascript://)
* [**S/MIME (Secure/Multipurpose Internet Mail Extensions)**](javascript://)
* [**SSO (single sign-on)**](javascript://)
* [**tablet**](javascript://)
* [**trusted source**](javascript://)
* **USB-C**
* **VR (virtual reality) headset**
* [**wearable technology device**](javascript://)
* [**Windows 10 Mobile**](javascript://)
* [**Yahoo!**](javascript://)
* [**Zigbee**](javascript://)
* [**Z-Wave**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-7c**Thinking Critically**

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use content from other chapters and the web.

1. Which of these network connections would allow your smartphone to sync your photos to your online account? Choose all that apply.
   1. Wi-Fi
   2. Bluetooth
   3. GPS
   4. Cellular
2. While visiting a coffee shop, you see a poster advertising a concert for a music group you’d love to see. You notice there’s an NFC tag at the bottom with additional information about the concert. Which of the following devices would likely be able to read the NFC tag?
   1. GPS
   2. Smartphone
   3. E-reader
   4. VR headset
3. Which of the following mobile device OSs are open source? Choose all that apply.
   1. iOS
   2. Windows 10 Mobile
   3. Chrome OS
   4. Android
4. A smart speaker has no screen or keypad for changing its settings. Order three steps to configure the speaker.
   1. Connect the smartphone to the speaker’s Wi-Fi hotspot.
   2. Download the speaker’s app to a smartphone.
   3. Enter the password to the home Wi-Fi network.
   4. Enter the password to the speaker’s Wi-Fi hotspot.
5. Which Chromebook security feature ensures that malware can’t change the OS’s system files?
   1. Quick updates
   2. Power washing
   3. Sandboxing
   4. Verified boot
6. You work for a company that provides dozens of the same smartphone model for its employees. While troubleshooting one smartphone that won’t connect to the cellular network, you call the provider’s tech support number for some assistance. The technician asks for the device’s IMEI. What is she trying to determine?
   1. The OS version on the phone
   2. The specific device you’re calling about
   3. The SIM card installed in the device
   4. The IP address of the phone on the cellular provider’s data network
7. Which encryption protocols might be used to secure a VPN connection? Choose all that apply.
   1. L2TP
   2. SSH
   3. PPTP
   4. IPsec
8. You’re at the store to buy a car charger for your dad’s iPhone. There are several options with many different types of connectors. Which of these connectors should you choose?
   1. USB-C
   2. microUSB
   3. Lightning
   4. VGA
9. Place the following information in the correct fields in [Figure 9-65](javascript://) to add an email account to a smartphone using port 143 for the incoming mail server and port 25 for the outgoing mail server (not all information will be used):

* + [imap-mail.sample.com](http://imap-mail.sample.com/" \t "_blank)
  + p@ssw0rd

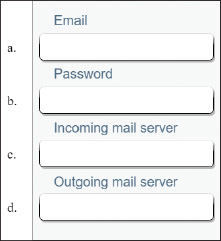
* + [pop-mail.sample.com](http://pop-mail.sample.com/" \t "_blank)

* + [mjones@sample.com](http://mjones@sample.com/" \t "_blank)

* + [smtp-mail.sample.com](http://smtp-mail.sample.com/" \t "_blank)
  + Mary Jones

**Figure 9-65**

Configure email for a smartphone



1. Congratulations! You just bought a new-to-you car, and it comes with a media system that can sync with your iPhone. You’re concerned about data usage on your cell phone, so before you go pick up your car, you decide to download the necessary app at home while you’re connected to Wi-Fi. What app do you need to download?
2. You’re traveling across the country for a much-anticipated vacation. When you get there, your smartphone seems to be having trouble connecting to the local cellular network. You call the provider, and the technician suggests you update the PRL. Why might this help? Where would you find this option on your Android smartphone to perform the update?
3. Your company has recently been hired to install a smart security system for a large office building. The system will include security cameras, voice-controlled lights, smart locks, and smart thermostats. Some of the security cameras will be installed outdoors throughout the parking lot. Which wireless IoT protocol should your company use for the installation?
   1. Wi-Fi because it is always encrypted
   2. Zigbee because it is always encrypted
   3. Z-Wave because it is the fastest wireless standard
   4. Bluetooth because it is easiest to configure
4. You’re trying to cast a video presentation from your tablet to a projector for a training session with some new hires. Although you tested it successfully yesterday, today the connection is not cooperating. You’ve closed apps you’re not using, and you’ve checked that the projector and the tablet are working otherwise. Of the following troubleshooting steps, which should you try first? Second?
   1. Restart the projector.
   2. Restart the tablet.
   3. Reinstall the presentation app.
   4. Verify that you have Internet access on the tablet.
5. An app that cost you $4.99 is missing from your Android. What is the best way to restore the missing app?
   1. Go to backup storage and perform a restore to recover the lost app.
   2. Purchase the app again.
   3. Go to the Play Store where you bought the app and install it again.
   4. Go to the Settings app and perform an application restore.
6. Suppose you and your friend want to exchange lecture notes taken during class. She has an iPhone and you have an iPad. What is the easiest way to do the exchange?
   1. Copy the files to an SD card and move the SD card to each device.
   2. Drop the files in OneDrive and share notebooks with each other.
   3. Send a text to each other with the files attached.
   4. Transfer the files through an AirDrop connection.
7. 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?
   1. Set up the Google account on your tablet that you used to buy apps on your phone and then download the apps.
   2. Buy the apps a second time from your tablet.
   3. Back up the apps on your phone to your SD card and then move the SD card to your tablet and transfer the apps.
   4. Call Google support and ask them to merge the two Google accounts into one.
8. Of the 10 devices shown earlier in [Figure 9-46](javascript://), how many of them are assigned IP addresses?
   1. Four: two phones, a web server, and a router
   2. Three: two phones and a web server
   3. Seven: a thermostat, a router, two phones, two bridges, and a web server
   4. All 10 are assigned IP addresses.

Go to pg.

[**help**](javascript://)