CONNECT & SECURE YOUR iPHONE & iPAD

Covers iOS 13.1 & iPadOS 13.1

BY GLENN FLEISHMAN

Click here to buy the full 185-page “Connect and Secure Your iPhone and iPad” for only $20!
Welcome

Welcome to *Connect and Secure Your iPhone and iPad*, version 1.0.2, written by Glenn Fleishman, published September 24, 2019, by Aperiodical LLC.

This book describes how to use your iPhone and iPod touch with iOS 13 and iPad with iPadOS 13 on Wi-Fi and cellular/mobile networks securely, making connections with ease while protecting your data and your privacy. It also covers Bluetooth, tracking an Apple mobile device, the Apple Watch, managing passwords, Safari’s cookie protections, Personal Hotspot and Instant Hotspot, two-factor authentication with an Apple ID, Sign in with Apple, using AirDrop and AirPlay, and solving connection problems.

Visit the updates page to check for new versions and re-download any of the ebook files. Use the password *horsefly*. Sign up for the announcement email list, and you’ll be notified about free updates to this edition of the book, as well as receive a note and a discount coupon when I release future editions covering newer versions of iOS and iPadOS. I will not sell, rent, or share your information.


If you have the ebook edition and want to share it with a friend, I ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Aperiodical LLC is a tiny independent publishing company—just Glenn!

Copyright ©2019 Aperiodical LLC. All rights reserved. More copyright info on page 184.

Click here to buy the full 185-page “Connect and Secure Your iPhone and iPad” for only $20!
The book is divided into three major sections:

*Networking* should be simple, and security should be automatic. And money should grow on trees. Despite how intuitive it is to pick up and use an iPhone or iPad, requiring little thought as to how it connects to a cellular or Wi-Fi network, it becomes complex as soon as you drill down to any details. This is especially true when connectivity fails, and you try to troubleshoot.

*Privacy* deserves the attention it’s now getting. Your information is your own to choose how it’s shared, whether it’s your location, your food preference, or your address and phone number. iOS and iPadOS provide tools that enhance your ability to control that.

*Security* is an even denser area. Apple makes its default choices reasonably secure, but to ensure real protection for your data—when you select and use passwords, while your bits are traveling through the æther, or in the event that your device is stolen—you need to know how it all works.

**Note:** Apple split iOS into two parts in its latest release. iOS is now the name of the operating system that runs an iPhone or iPod touch, while iPadOS naturally powers the iPad. Because nearly everything covered in this book remains identical across both systems, I will frequently refer to them collectively as “the OS” to avoid repetition.
## TABLE OF CONTENTS

### NETWORKING

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to a Wi-Fi Network</td>
<td>8</td>
</tr>
<tr>
<td>Join a Network</td>
<td>8</td>
</tr>
<tr>
<td>Manage Wi-Fi Connections</td>
<td>10</td>
</tr>
<tr>
<td>Drill Down to Network Details</td>
<td>12</td>
</tr>
<tr>
<td>Turn Wi-Fi Off</td>
<td>16</td>
</tr>
<tr>
<td>Capture the Page</td>
<td>16</td>
</tr>
<tr>
<td>Knock, Knock, Apple’s There!</td>
<td>16</td>
</tr>
<tr>
<td>Auto-Join and Auto-Login the Next Time</td>
<td>18</td>
</tr>
<tr>
<td>Wi-Fi Troubleshooting</td>
<td>20</td>
</tr>
<tr>
<td>Can’t See Wi-Fi Networks or a Network You Need</td>
<td>20</td>
</tr>
<tr>
<td>No Wi-Fi Signal Strength in the Indicator</td>
<td>20</td>
</tr>
<tr>
<td>Too Many Wi-Fi Networks</td>
<td>21</td>
</tr>
<tr>
<td>Correct Password Not Accepted</td>
<td>22</td>
</tr>
<tr>
<td>No Internet Service after Connecting.</td>
<td>22</td>
</tr>
<tr>
<td>Check a Web Page with Safari</td>
<td>23</td>
</tr>
<tr>
<td>Check or Ask about the Base Station</td>
<td>23</td>
</tr>
<tr>
<td>Check IP Address Settings</td>
<td>23</td>
</tr>
<tr>
<td>Make a Mobile Hotspot</td>
<td>25</td>
</tr>
<tr>
<td>Turn On Personal Hotspot</td>
<td>25</td>
</tr>
<tr>
<td>Turn On in iOS or iPadOS</td>
<td>26</td>
</tr>
<tr>
<td>Turn On via Another Device</td>
<td>27</td>
</tr>
<tr>
<td>Let Your Family Share It</td>
<td>28</td>
</tr>
<tr>
<td>Use Cell Data while Talking</td>
<td>28</td>
</tr>
<tr>
<td>Set a Wi-Fi Password</td>
<td>29</td>
</tr>
<tr>
<td>Name Your Wi-Fi Network</td>
<td>30</td>
</tr>
<tr>
<td>Consider Turning Off Certain Radios</td>
<td>31</td>
</tr>
<tr>
<td>Connect to Personal Hotspot</td>
<td>32</td>
</tr>
<tr>
<td>Access via Wi-Fi.</td>
<td>32</td>
</tr>
<tr>
<td>Tether with USB in macOS</td>
<td>36</td>
</tr>
<tr>
<td>Choose to Use Cellular Data or Wi-Fi</td>
<td>41</td>
</tr>
<tr>
<td>Which Network Are You On?</td>
<td>41</td>
</tr>
<tr>
<td>Select Which Service to Use</td>
<td>42</td>
</tr>
<tr>
<td>Manage Cell Data Usage</td>
<td>44</td>
</tr>
<tr>
<td>Carriers Shift to Throttling</td>
<td>44</td>
</tr>
<tr>
<td>Keep Usage Restrained</td>
<td>45</td>
</tr>
<tr>
<td>Enable Low Data Mode in Cellular Settings</td>
<td>45</td>
</tr>
<tr>
<td>Tracking Cellular Usage on an iPhone</td>
<td>45</td>
</tr>
</tbody>
</table>

Click here to buy the full 185-page “Connect and Secure Your iPhone and iPad” for only $20!
### Privacy Settings
- Setup without Much Sharing ........................................... 92
- Control System Privacy ........................................... 94
- Siri ................................................... 95
  - What Siri Knows about You ................................ 96
  - Siri and On-device Searching ................................ 97
- Safari .................................................. 99
  - Apple’s Suggestions ....................................... 100
  - Sharing and Commenting .................................... 100
  - Passwords and AutoFill ..................................... 101
  - Watching the Watchmen ...................................... 101
- Location .............................................. 104
  - The How and Why of Location ................................ 104
  - Opting In and Opting Out .................................... 106
- Photos .............................................. 110
- Bluetooth in Apps .......................................... 110
- Share My Location .......................................... 110
- Privacy Settings and Allowing Access ......................... 112

### Keeping Creeps Away
- Block Numbers and Email Addresses ............................ 113
- Call–Blocking Apps .......................................... 115
- Filter iMessages and SMS ..................................... 117
  - Filter SMS with Third–Party Apps ......................... 118

### SECURITY

#### Create, Manage, and Use Strong Passwords
- What Makes for a Good Password ................................ 120
- Work with iOS and iPadOS’s Built–in Manager ................. 122
  - Passwords & Accounts ....................................... 122
  - iOS and iPadOS Help with SMS Login Codes ............... 125
- Use Passwords in Web Sites and Apps and Devices .......... 127
  - Safari .................................................. 127
  - Other Apps ............................................. 128
- Fill in on Apple TV .......................................... 129
- Use Third–Party Password Managers ............................ 129

#### Connect to a Secure Wi-Fi Network
- Connect to a Small Network .................................... 131
  - Share a Wi–Fi Password ................................... 132
  - What’s Behind Simple Wireless Security ................... 134
- Connect to a Corporate or Academic Network ................ 134

#### Use Two–Factor Authentication
- What Have You Got in Your Pocket? ............................. 136
- The Risk of SMS 2FA Factors .................................. 137
- Turn On Apple's Two–Factor Authentication ................... 139
  - Enable Two–Factor ......................................... 139
It’s true that an iPhone or iPad can be used without a live network connection, but their natural states are always hooked up. In the first part of the book, you’ll learn how to work with the three types of mobile wireless communication—Wi-Fi, cellular, and Bluetooth—for general connectivity, with personal hotspots, for audio/video streaming, and for file transfer.
Connect to a Wi-Fi Network

Wi-Fi works quite simply in iOS and iPadOS, but there’s a lot of hidden detail. In this chapter, you’ll learn how to interpret the Wi-Fi settings view, manipulate custom network settings, and troubleshoot common problems.

Join a Network

Open the Settings app and tap Wi-Fi to view nearby networks. You see a single name for all Wi-Fi routers that broadcast a network with that name. Tap a network name to attempt to join it.

You can also use a quicker method added in the latest OS:

1. Swipe to reveal the Control Center.
2. Hold down on the network area.
3. Hold down on the Wi-Fi icon.
4. Select a network from the list that appears (Figure 1).

**Tip:** Tap Wi-Fi Settings to bring up Settings > Wi-Fi, which is discussed next.

The first time you tap a network name to connect, your device joins the network immediately unless encryption is enabled on the network. In that case, you are prompted for a password; once you’ve entered the password and tapped the Join button, you join the network.

**Note:** For more on connecting with a password or other methods, see Connect to a Secure Wi-Fi Network in the Security section of the book.
Figure 1: Hold down on the Wi-Fi icon in the Control Center’s expanded network area to bring up a list of Wi-Fi networks to join.

If you don’t have a network’s password and you’re with a friend who has previously logged in, place your device near theirs and tap the network that you want to join. If you’re in that person’s contacts, their device will prompt them to approve sending your device the password (Figure 2)!

Figure 2: When my younger kid places his iPad near my iPhone and tries to join Portage Airbasestation, I see the message at left. I tap Share Password, and the password is silently shared to his iPad. Then iOS lets me know it succeeded.
Wi-Fi Troubleshooting

Although Wi-Fi generally works well, you may at times be unable to get a live network connection. Here is troubleshooting advice for common cases.

Can’t See Wi-Fi Networks or a Network You Need

If your device can’t see any Wi-Fi networks or a network you think should be available, eliminate variables by trying the following:

- With no Wi-Fi networks detected, be sure that Wi-Fi isn’t turned off. Swipe to reveal Control Center (or launch Settings). (This has happened to me more times than I’d like to admit.)
- You may be connected to the wrong network. In Control Center, press and hold the Wi-Fi button to expand the networking panel; the name of the network you’re connected to appears under the Wi-Fi button.
- It’s possible that you are out of range. Move the device closer to where you know (or think) a base station is located. Although every Apple mobile device sports an excellent Wi-Fi radio, Wi-Fi reception can be blocked by thick obstructions, such as solid stone and brick walls, or by walls made of chicken wire covered by plaster.

Note: It’s also possible that the base station, not your handheld, is in trouble. And I have seen the Wi-Fi radio in an Apple mobile device fail intermittently or completely, requiring that the device be entirely replaced.

No Wi-Fi Signal Strength in the Indicator

You’ve selected a network and, if necessary, entered a password, and tapped Join—but the signal-strength indicator in the upper left still shows gray radio waves instead of black. This means that an initial con-
nection was made, but then you quickly moved too far away from the base station, or the base station was shut down or restarted with new information. If the connection process had failed while underway, you would have seen a notification alerting you.

Try connecting again. If that fails, restart your device: Press the Sleep/Wake button until you see a red slider for powering down. Slide it, wait until the spinning indicator disappears and the screen goes entirely black, and then hold down the button again for a few seconds. An Apple icon appears and the device starts up.

**Too Many Wi-Fi Networks**

You can find yourself swimming in a sea of Wi-Fi networks in your vicinity, which often makes it hard to select the one you want to join. If you know the network’s exact name, you can type it in:

5. Launch Settings.
6. Tap Wi-Fi.
7. Slide down until you can tap the Other button (**Figure 6**).

![Figure 6](image)

**Figure 6:** The Other Network option lets you enter a network name and optional password from scratch.

8. Enter the network name exactly and, if there’s a password:
Make a Mobile Hotspot

Every iPhone and every iPad with cellular has a built-in data modem that lets the device access high-speed mobile data networks. This modem lets us use our iPhone or cellular iPad while we’re traveling instead of having to buy a separate cellular modem or router with a separate monthly service fee.

Personal Hotspot lets you connect other devices to your phone or tablet as a conduit to the mobile Internet. While the name implies a Wi-Fi hotspot connection, which is one component of it, you may also tether via Bluetooth or USB with desktop computers and other devices to extend access. All three methods may even be used simultaneously.

Personal Hotspot’s availability varies by carrier, although operators around the world offer it: Consult this list by Apple to check on yours.

Note: In this chapter, I talk about a mobile hotspot or Personal Hotspot to refer to all the features, but I use the term tethering when the discussion is specifically about Bluetooth or USB.

WARNING! Most cellular operators put limits on Personal Hotspot use. They may offer a data rate lower than that of your phone (600 Kbps instead of LTE, for instance), cut you off after a certain amount of data (like 15 GB), or throttle you to 128 Kbps (2G) or 3G speeds after a monthly cap is hit.

Turn On Personal Hotspot

There are two ways to turn on the Personal Hotspot feature: directly on your device or through another computer, iPhone, or iPad.
Whenever you use these methods, the device that turns on the Personal Hotspot then automatically connects to it.

**WARNING!** Devices that connect to a Personal Hotspot typically treat it like a regular Wi-Fi or Ethernet network, which can mean it’s easy to rack up huge amounts of usage. Pause or disable sync services, like Dropbox, and online backup systems, like Backblaze. You may also want to avoid using streaming video services or digital media downloads while connected. You can also turn on the new Low Data Mode on your Wi-Fi connection.

**Turn On in iOS or iPadOS**

Enable it in Settings > Personal Hotspot. Now you can switch the hotspot on and set a Wi-Fi password. The screen is also full of connection information (Figure 7). (It’s also found in Control Center if you hold down on the network connections area.)

![Cellular Personal Hotspot](image)

**Figure 7:** The Personal Hotspot view lets you turn access on or off as well as set a Wi-Fi password.

**Tip:** Before you use Personal Hotspot the first time, you may need to open it via Settings > Cellular (iOS) or Settings > Cellular Data (iPadOS).

Personal Hotspot has three states starting in iOS 11, although this is not obvious at first glance:

- On and Discoverable: other devices can connect
- Off: the feature is entirely off
- On but Not Discoverable: it can be used only via USB
Choose to Use Cellular Data or Wi-Fi

There are plenty of good reasons to pay attention to whether your iPhone or cellular iPad is accessing the Internet via a Wi-Fi network or mobile broadband. You may need greater bandwidth than the cellular network can provide, or be budgeting data on a low-bandwidth plan or while traveling.

Whatever the reason, you can determine which network you’re on and set the type of network to which your device connects. And you can even enable a hybrid mode that taps into cellular data when Wi-Fi is flaky.

Which Network Are You On?

iOS has an indicator in the status bar that shows which network connection is active. The range of throughput is huge (such as 30 to 300 Mbps with the fastest methods), because there are such wide ranges of generations of cellular networks and Wi-Fi base stations in use.

And each mobile device supports many rates for each standard while also offering backward-compatible support for older networks.

Here’s what the indicators mean:

- **No service**: Can’t connect to any network.
- 🌠: Connected via Wi-Fi. The number of waves, from a dot to three, indicates signal strength. Downstream rates from can be as fast as 1 Gbps with an iPhone 11 or 11 Pro and the newest Wi-Fi 6 gateways.
- **Wi-Fi**: Wi-Fi Calling is enabled.
- **5G**: Marketing letters for the fastest available LTE, rather than the 5G networking technology revision that is not available on Apple phones—or really almost any phones. Downstream rates can top 40 Mbps, but will increase as deployments get denser. Upstream can top 10 Mbps.
- **LTE**: Connected via LTE. Downstream rates can top 20 Mbps. Upstream is several Mbps.
- **4G**: Connected via 4G (on GSM networks only). About 6 Mbps downstream and below 2 Mbps upstream.
- **3G**: Connected via 3G. Maximum rates vary by network from 1.4 Mbps (CDMA) to 4 Mbps (GSM) downstream and hundreds of Kbps to over 1 Mbps upstream.
- **E**: Connected via EDGE, a 2.5G standard (GSM only). About 200 Kbps downstream and 40–50 Kbps upstream.
- **GPRS**: Old 2G networks, about 40–50 Kbps in each direction.

## Select Which Service to Use

You can force a cellular device to use either cellular or Wi-Fi service instead of letting it automatically switch depending on whether or not a suitable Wi-Fi network is available. Because iOS and iPadOS don’t offer network profiles as in macOS, which would make it easy to switch, you must use the Settings app to enable or disable a service.

To enable or disable cellular data service:

- **To use just a cellular connection and avoid Wi-Fi, perhaps to keep a continuous VPN connection or for security reasons, either:**
  - Swipe to show Control Center and tap the Wi-Fi icon to disconnect.
  - Tap Settings > Wi-Fi, and then set the Wi-Fi switch to Off.
- **To rely only on Wi-Fi, accepting that you may have times during which you have no Internet connectivity:**
  - Swipe for Control Center and tap the Cellular Data icon to disable it.
  - Tap Settings > Cellular Data (iPad) or Settings > Cellular (iPhone), and then turn Cellular Data off.
Manage Cell Data Usage

When Apple introduced the iPhone, it convinced its first carrier, Cingular (subsequently bought by AT&T), and then other carriers to offer unlimited data plans in the U.S. and a few other places. As smartphones multiplied and networks became congested, carriers pushed back and started limiting “unlimited” plans and offering fixed amounts of data, while charging overages beyond that.

In 2019, the pendulum has swung way back in many places. Carriers in many countries charge a flat rate and throttle throughput after a certain amount of data has been used. Some carriers offer something close to unlimited to most people: 20 to 50 GB of data per month before throttling. There are still many provisos, but overage fees have largely disappeared.

Carriers Shift to Throttling

All four major U.S. cellular carriers have no overage fees, and some offer what are effectively unlimited data by throttling after a set amount of data has been used in an individual or pooled family plan in a billing period.

Limited-use plans from AT&T, for instance, offer cheaper options for a single line or families that pool 3 GB or 9 GB. After you exceed that limit, your account throttles to 128 Kbps for the remainder of the billing period.

“Unlimited” plans from all four carriers rely on congestion throttling. In that scheme, you will get at least 128 Kbps or 3G after some amount of use, depending on the network. However, you can still achieve LTE rates if the area in which you’re using your device isn’t congested at the moment. (The one exception is Verizon’s lower-tier plan, where congestion throttling can happen at any time.)
Tethering for hotspot use also varies from carrier to carrier, typically limiting usage as a fraction of an “unlimited” plan. With T-Mobile, for example, you get 50 GB of unthrottled use each month on your smartphones and tablets, after which you’re given lower priority for data on congested networks. However, Personal Hotspot isn’t available on its cheapest plan, and is limited to 3 GB and 15 GB per month on its middle- and top-tier plans.

**Tip:** Some smaller carriers in the U.S., like Red Pocket and Ting, have national coverage and let you set relatively small amounts of data use—like 500 MB to 1 GB— to keep monthly costs lower, sometimes half as much as the lowest major-carrier plan.

---

**Keep Usage Restrained**

You can have full-speed mobile access when you need it without breaking your limits if you ration usage. What you need is a strategy.

**Enable Low Data Mode in Cellular Settings**

Starting in iOS 13 and iPadOS 13, you can enable Low Data Mode in Settings > Cellular (iOS)/Cellular Data (iPadOS) > Cellular Data Options. This turns off background data use by third-party apps and limits activity by the OS (Figure 20).

This means you have to check email manually and perform other updates “by hand.” It effectively limits data use to the foreground app you’re using. This can be a great tool for reducing accidental data usage.

**Tracking Cellular Usage on an iPhone**

An iPhone shows your locally tracked consumption of cellular data via Settings > Cellular > Cellular Data under Current Period. This number has two problems:

- It’s not guaranteed to be accurate. Your carrier’s records are definitive (Figure 21). In practice, it’s pretty close.
Place Calls via Wi-Fi

Cellular phone calls are just data. The stream of audio data that composes them, however, can be routed in different ways depending on the generations of cellular technology that a phone supports and on how carriers choose to configure their networks. Wi-Fi Calling effectively extends cellular calling to home and office Wi-Fi networks. It’s seamless once enabled besides displaying a tiny Wi-Fi label in the status bar.

Wi-Fi Calling is great when a good cell signal isn’t available, often inside a building or house. Carriers that offered similar features used to provide incentives for using Wi-Fi, like unlimited domestic calling. But now they just extend your voice plan to Wi-Fi, whether it’s unlimited or otherwise.

**Note:** All four major U.S. carriers support Wi-Fi Calling, but it varies with smaller carriers and with phone operators outside America. Consult Apple’s page that shows features supported by carriers worldwide.

**Note:** Wi-Fi Calling is distinct from Voice over LTE (VoLTE), a method of routing voice calls over LTE mobile networks. I discuss that in the Personal Hotspot chapter, in the section “Use Cell Data while Talking.”

Turn On Wi-Fi Calling

Apple doesn’t turn on Wi-Fi Calling by default. Instead, you have to enable it, and then walk through a variety of steps that vary by carrier.
Enable Wi-Fi Calling on Your Main Device

Start in Settings > Phone > Wi-Fi Calling (Figure 25). Once you tap the switch, you’re prompted to enable Wi-Fi Calling.

![Enable Wi-Fi Calling on This iPhone](image)

**Figure 25:** You have to tap the switch and then agree to enable Wi-Fi Calling.

**Tip:** If you know your carrier offers Wi-Fi Calling, but its switch is dimmed out, Apple suggests restarting the phone. If that doesn’t work, try resetting your iPhone’s network settings by going to Settings > General > Reset and tapping Reset Network Settings.

If all goes well, you proceed through a set of steps that warn you about emergency calls, and have you fill out the address at which you typically use the phone with Wi-Fi Calling (Figure 26).

It’s relatively easy for 911 service to pinpoint you on a cellular-connected call, because your phone has to connect to a nearby tower. For a Wi-Fi-based call, location can be provided by GPS and other factors, but it’s not as neat a process. Hence the form to fill out.

When you place an emergency call with Wi-Fi Calling active, Apple says the iPhone will first try to reach a cellular network. If a cell network can’t be used, the address you enter for Wi-Fi Calling may be the one that’s sent as a fallback to responders.
Airplane Mode

Before you’re flying so high with some guy in the sky, you need to disable radio communications on your mobile device. The Airplane Mode switch makes this simple.

The U.S. allows the use of handheld personal electronics below 10,000 feet, even though laptops and other large devices are supposed to be stowed so they don’t become projectiles. (1,000-page books are still fine, bizarrely.)

Cellular radios remain banned, and one ostensibly isn’t supposed to use Bluetooth at all, and should not turn on Wi-Fi unless in a plane equipped with Wi-Fi service.

The FAA Caught Up with Science

Until a few years ago, the FAA enforced a kind of commercial urban myth: that the cellular radios in cell phones as well as the circuitry in personal electronics like an ebook reader could cause interference with the avionics (electronic flight systems) on commercial aircraft.

This was out of an abundance of caution even years after it was clearly proven that there was no such risk—and after it was shown that cell phones are routinely left on, or even used, in flight without any adverse effects.

What’s Airplane Mode?

Airplane Mode is available to all iPhones, iPads, and Apple Watches, and is a simple way to set your device to a legally required quiet mode during flight. In the Settings app, tap the switch next to Airplane Mode. You see an airplane icon in the top status bar when the mode is active.
Saves battery life, too: If you don’t need to use any of the radios for network access, peripherals, or location, Airplane Mode is an effective way to extend battery life, too.

With a Watch, turning on Airplane Mode one enables it on its paired iPhone and vice-versa.

When you turn on Airplane Mode in the Settings app—or by swiping to show Control Center and tapping the airplane icon—the OS turns off three separate radio systems on an iPhone, cellular iPad, and cellular Watch: cellular, Wi-Fi, and Bluetooth. On a Wi-Fi-only iPad or any iPod touch or non-cellular Watch, Wi-Fi and Bluetooth are disabled.

GPS works in Airplane Mode: Once, Airplane Mode disabled the GPS radio, even though there was no reason for that, as the radio passively receives signals from satellites. For years now, you can use GPS positioning with a map that has data stored offline, to track your path with GPS coordinates, and to geotag photos and other documents.

On flights on which Wi-Fi is available for Internet access, you can separately tap and re-enable Wi-Fi in the Settings app. Some people also use Airplane Mode to reduce battery usage by disabling its radios, and turn Wi-Fi on for local network access.

When you turn off Airplane Mode, all your previous settings for access are flipped back on. With a Watch, you have to separately disable Airplane mode on both the Watch and its paired iPhone.

To Sleep, Perchance To Transmit

When you push the Sleep/Wake button on the top or side of your device to put it to sleep, you might think the entire device is suspended. But this standby mode is pretty active. Certain background operations continue, and a cellular iPad, cellular Watch, and any iPhone can receive email and other updates via push over a cellular data connection.

The OS also maintains Wi-Fi connections on a minimal continuous level. Sleep is more like lightly daydreaming. That’s a reason to use Airplane Mode: to prevent all of this from happening when you don’t intend it to.
Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, earpieces, headsets, and keyboards to an iPad or iPhone for listening to music and entering text. It’s also the glue that binds together devices for Continuity’s Handoff features and connects the Apple Watch with an iPhone by default.

While this book covers aspects of Bluetooth elsewhere, read this chapter to learn how to set up and manage Bluetooth devices.

**Tethering:** Bluetooth can provide Internet service to an iPhone or iPad from another piece of hardware, such as an iPhone with Personal Hotspot enabled, a laptop, or a cellular router with Bluetooth as an option. See the earlier chapter *Make a Mobile Hotspot* for details.

Bluetooth Basics

The Bluetooth SIG, a trade group, certifies devices as Bluetooth compliant for particular profiles, which include things like text entry, stereo audio, file transfer, and modem access. Apple’s mobile devices work with any device that meets the Bluetooth spec for several profiles, including audio, peer-to-peer transfer, and external keyboards.

When you connect with Bluetooth, the process is known as *pairing*. Some devices can be paired with several hosts (like computers or mobile devices); others can pair with only one host at a time, and must be re-paired to switch. Bluetooth devices are discoverable when they are set to allow a pairing connection.

Bluetooth is handled from the Bluetooth view (Settings > Bluetooth). This view lets you turn Bluetooth on and off and displays a list of Bluetooth...
peripherals under My Devices and Other Devices. The My Devices list shows any devices that have been previously attached to the device and the current status of such devices. The Other Devices list displays any discoverable devices within range. (It’s labeled just Devices before you connect any Bluetooth device.)

**Bluetooth and Low Energy (LE)**

Bluetooth 4 brought a low-power mode called Bluetooth LE (sometimes called Bluetooth Smart) to the mix. It lets devices with tiny batteries that are meant to be changed infrequently communicate in tiny, power-conserving bursts. You could have Smart devices in your home’s alarm system, and an app could let you tap to see if any windows are ajar, for instance.

Apple has used Bluetooth LE extensively in later releases of iOS, iPadOS, and macOS to enable signaling between devices for AirDrop (see [Pass Files with AirDrop](#)) and some of the Continuity features, like Instant Hotspot (see [Turn On via Another Device](#)).

Bluetooth LE is also used to communicate with the Apple Watch, and is a key part of HomeKit, Apple’s home-automation technology. With both the Watch and HomeKit, Wi-Fi is a fallback when Bluetooth signals don’t reach, but it consumes much more power on both ends.

Apple supports Bluetooth 5 in many of its devices, which builds on features in version 4, while increasing throughput and range.

**Pairing Any Device**

To start pairing, follow these general steps (the specifics for particular profiles are given later in this chapter):

1. Tap Settings > Bluetooth.
2. Activate Bluetooth discovery on the other device if required. This may require enabling a setting or holding down a button (sometimes a special pairing button) for several seconds.

   On your mobile device in the Bluetooth view, the other device appears, naturally enough, in the Other Devices list (Figure 30).
3. Tap the desired device. The OS attempts to connect.
4. Depending on the device, the OS will do one of the following:
Pass Files with AirDrop

AirDrop lets you pass photos, URLs, contact cards, and any arbitrary file from a Mac, iPhone, or iPad to another of any of those kinds of hardware on the same Wi-Fi network. It’s a neat way to bypass email, text messaging, or a sync service like Dropbox.

Configure AirDrop

AirDrop is one of the simplest pieces of iOS and iPadOS technology. There’s only one set of choices to make (Figure 35).

Figure 35: Control Center is where you set AirDrop access.

1. Swipe to show Control Center.
2. Hold down on the networking area, which displays the AirDrop icon and its status at bottom left (cellular devices) or upper right (Wi-Fi iPad).
3. Tap the AirDrop icon.
4. Tap one of the options (Figure 36):
   ▶ Receiving Off disables AirDrop.
   ▶ Contacts Only shows your device only to people whose email address is in your Contacts. This is the default option.
   ▶ Everyone lets anyone on the local network see that you’re available.

Click here to buy the full 185-page “Connect and Secure Your iPhone and iPad” for only $20!
Figure 36: Pick how AirDrop advertises itself on a network.

**WARNING!** Some people have reported receiving unwanted images, including obscene ones, in public places if they have AirDrop set to Everyone. My advice is to leave it set to Contacts Only.

Regardless of this setting, anyone who has your iCloud account email address in their contacts will appear for you in the latest OS as a more-privileged destination than folks who don’t have you as a contact.

Share with AirDrop

AirDrop is available in any share sheet in iOS, iPadOS, and macOS: You can send URLs, files, photos, contacts, and other items to anyone nearby.

When you tap the Share icon on an iPhone or iPad, AirDrop becomes available in two ways. First, any nearby person for whom you’re a contact appears among a list of possible recipients in a top row starting at furthest left with an AirDrop icon overlaid (Figure 37).

Second, you can tap an AirDrop icon in the second row. Tap it and you see folks who know you and all “Everyone” destinations. The list is divided into People (those in your contacts) and Devices (both your own devices logged into the same iCloud account and anyone set to Everyone). People have their contact name displayed; devices, their sharing name.
Stream via AirPlay

Apple’s AirPlay technology lets you stream audio and video from Apple equipment to a variety of other hardware, including stereo receivers, computers, the Apple TV, HomePods, and more.

What’s just as good is that Apple licenses the specification so that other companies can extend AirPlay to be more useful. In this chapter, you’ll learn how to set up AirPlay, but also how to use it more broadly than with Apple’s software and hardware.

AirPlay 2, a version that can pass audio to multiple speakers at once, appeared in 2018 across all Apple OSes and iTunes for Windows.

Select AirPlay Devices

This chapter has to start a little backwards, because before you can use AirPlay, you need a destination—or two or more with AirPlay 2! It’s easier to walk through how you can configure your iPad or iPhone to point to an AirPlay receiver, and then look at the many kinds of uses.

To select any AirPlay-compatible device on the same Wi-Fi network as your mobile device, follow these steps:

1. Swipe to reveal Control Center.
2. Tap the AirPlay icon at the upper-right corner of the music player. (If no AirPlay destinations are available, the AirPlay icon doesn’t appear.)
3. Select the device you want to use as a destination (Figure 43).
   - Your device is shown at the top with a checkmark.
   - Bluetooth audio devices appear with an audio Bluetooth icon.
- Other audio-capable devices are shown with a stereo speaker icon.
- Video-capable devices are shown with an Apple TV icon, whether or not they are actually an Apple TV.
- If destinations support AirPlay 2, they appear with a circle to their right, and you can tap to add them, instead of switching to them.

4. If the OS is currently playing media, you should see a play/pause button you can tap to return to the playback view.

![Image of AirPlay settings](image.jpg)

**Figure 43:** Available AirPlay destinations are identified by type.

---

**Connecting with a Passcode or Password**

An AirPlay device can be locked with either a four-digit passcode or a password.

- For code access, the device to which you’re connecting will display the four digits. Enter those in the mobile device to connect.

- With a password, you enter the password set on the destination device.

Some Apple and third-party apps offer direct AirPlay device selection. The same options appear. In some cases, you might see a Done button rather than play/pause. You can also tap elsewhere to exit the view.
The online world is a tough place to keep your personal and financial details private. Even companies we should be able to trust often push at the limits of reasonable and ethical use of our information—especially in tracking us and aggregating our online profile from a thousand little shards into one complete picture.

Our privacy encompasses our personal information (our name, address, phone number, height, weight, and eye color), our financial information (bank accounts, credit cards, purchases, credit score, and much more), and data about us, like our current location, our browsing habits, and our typical travel patterns.

Privacy and security are complementary concepts. In this section, you’ll learn how to use controls and filters to limit the ability of Apple and third parties to track you and to retain data to which you give them access. The next section, Security, addresses keeping information intended to be secret away from the prying eyes of others.
Privacy Leaks

What information, either owned by you or about you, should you be concerned about other people getting their hands on? In this chapter, I take a brief walk through a few different ways to slice that question so that you know in the coming chapters precisely what you want to allow, monitor, and block.

The difference here between privacy and security is that to constitute an invasion of privacy it doesn’t necessarily require that a malicious party or malware obtain the information discussed below. Where it tips into security issues, discussed in the last section of the book, is when you’re explicitly preventing unwanted intrusion that is malicious, criminal, or on behalf of government agencies.

Where Data Lives

Data is a monolithic term, but when we talk about your data being accessible to other parties, or leaking, we should define where it comes from:

**Stored data on your device.** The OS, its apps, and remote systems may be able to access, with or without permission, information you have stored on your mobile hardware. This can include contacts, photos, and emails.

**Device hardware.** The OS offers highly granular permission control for every kind of hardware element, whether a microphone or an activity sensor. This information can be extremely private. An app that can record you speaking or that can shoot video without your knowledge and stream or upload it later would be terrifying.

**Data in transit.** Information traveling between your iPhone or iPad and a legitimate destination could be intercepted or tampered with.
Information stored at a web site. Any interaction with a site can lead to it storing information about you, whether associated with an account and willingly provided or tracked and associated with a unique ID.

Cloud–stored data. Many services we use rely on data stored in the cloud, a collection of servers without a specific location, as information can be fluidly stored among whatever servers are available for primary storage and redundancy. Clouds may diffuse storage within a data center, among servers across a country, and even at locations around the globe.

What Kinds of Data

Beyond where data is located, you should also consider the kinds of information that you store on your iPhone and iPad and how it might be used. Just the way in which you use the Internet could provide fodder for legitimate and illegitimate purposes.

Behavior

Whatever you do can be tracked, although Apple makes it hard for some of this information to leak or be requested by anyone other than itself. Almost all of the following requires permission from a user (discussed in the next chapter) unless a malicious app was installed, which is unlikely.

Differential Privacy

Starting in iOS 10 and macOS Sierra, Apple added differential privacy, a technique of acquiring data that, if implemented and operated well, strongly resists tracking back a particular behavior or response to any individual user. It accomplishes this by adding random noise to all data before it’s sent from your hardware.

The technique dates back decades to randomized response, which was developed to get honest answers to questions risky to answer. If an American survey subject were asked in the 1950s whether or not they were a member of the Communist Party, the safe answer was always “no,” even if the interviewers assured them of privacy.
Apple Blocks Tracking

Advertising-technology companies have built elaborate ways to track us across web sites, apps, and even real-world purchases that we make. The goal is to assemble a valuable profile of us, full of demographics (our age, race, income, and so on) and our purchase habits. This allows ad-tech companies to collect the greatest fees from advertisers, who believe super-targeted ads produce better outcomes.

Consumers increasingly have had enough, and hundreds of millions of people use ad blockers, anti-tracking software, private browsing, and other tools to disrupt unwanted online tracking. This includes Content-Blocking Safari Extensions in iOS and iPadOS, a feature that lets users install apps to block the loading of trackers and other kinds of web-based content.

Apple has taken a strong stance in this area, and over the last few years has rolled out a variety of features designed to deter tracking without blocking advertising or preventing advertisers from measuring the results of ads. In this chapter, I discuss Apple’s approach, including a new addition in 2019 in the latest Safari across all its platforms.

Safari Blocks Cookies

Browser cookies can feed a browser a unique identifier that’s stored locally. Every time a browser makes a web-based request for a page or other item that matches the same domain, it also packages and includes the cookie as part of the set of headers sent to that web server. Cookies are often used to plop a long-term or per-session identifier into a browser after a login or during an otherwise anonymous visit.
Starting in iOS 11 and macOS 10.13 High Sierra, Apple revamped how it approaches cookie storage and user choice. Previously, you had to select one of four options that had a lot of nuance behind them, and it wasn’t always obvious which one was correct.

Now, there are just two switches: Prevent Cross-Site Tracking (on by default) and Block All Cookies (off by default).

**Note:** Several years ago, a few privacy researchers mooted the idea of a Do Not Track browser signal that would let a user tell web sites they didn’t want to be tracked. While the idea gained traction—Apple and others included it—for a lot of reasons I discuss in [this Fast Company article](#), the idea ultimately fell apart.

Cross-site tracking lets ad networks and others feed cookies to your browser that can identify you across the Internet, essentially connecting your visits behind the scenes. This is why when you search for, say, “small superglue containers,” suddenly superglue ads appear to you everywhere you browse.

Starting with Safari in 2017, Apple added a sequence of timeouts for cookies based on the source from which they’re served to you. It calls this Intelligent Tracking Protection (ITP).

It’s a little complicated, but ITP differentiates between first-party cookies, those fed to your browser by the site you’re visiting, and third-party cookies, those fed from other domains. But it also uses built-in clues and relies on machine learning (using data kept entirely on your device) to identify third-party cookies designed entirely to track you across sites.

Tracking cookies get generated without user interaction, typically by resources loading instead of someone entering a user ID and password and logging in or engaging with some kind of feature on a site.

First-party data remains in place indefinitely, because it can only be used if you return to that site. If you don’t, there’s no harm in retaining it.

But for third-party data, Safari works this way:

- For the first 24 hours after you have an interaction with a site, third-party cookies and data remain active and available from other sites. This is much like how it works today.
Privacy Settings

Apple states repeatedly that it’s committed to keeping its customers’ data private, and it does seem to do a better job than other companies because it’s primarily interested in selling us stuff—hardware, software, and services—rather than pushing advertising at us.

However, there are both centralized and scattered settings that let you control on a large scale and in small ways all sorts of data that leaks from your iPhone or iPad to Apple and beyond.

**Note:** Apple’s full privacy policy spells out in great detail how it promises to handle your personal data and information about you.

Setup without Much Sharing

It’s a privacy conundrum: Apple encourages you to enter personal or private details and connect your mobile device to its services before it lets you choose how you want to share data. You can work around this a bit with a new device or when you erase one to start from scratch.

**Note:** You can also set up one device by having another one nearby and entering your existing device’s passcode. This may bypass some privacy options, however.

Start setup. On the Choose a Wi-Fi Network screen, Apple won’t let you proceed until you either select a Wi-Fi network or, on a device with an active mobile data plan, tap Use Cellular Connection (Figure 47). The moment you do this, some information about your activities starts transmitting immediately—although it’s not much at this point!
Figure 47: You have to pick a network.

On the Location Services, choosing Disable Location Services ensures nothing related to your position is sent. (If cellular service is available, even if you chose Wi-Fi in the previous step, your device’s pings to cell towers are recorded, however—that’s unavoidable.)

On the Apps & Data screen, don’t enter an iCloud account’s information, but instead choose Set Up as New iPhone (Figure 48). On the Apple ID screen, click Don’t Have Apple ID or Forgot It?, then confirm you want to skip. You can connect your Apple ID and iCloud account later.

Figure 48: Don’t restore a backup, but start from scratch.
Keeping Creeps Away

Every technological breakthrough has a downside. iMessage was a big step up over text messaging: Encrypted to just the members of a conversation, allowing long messages, including rich media. It was kind of perfect. Except Apple never thought about it being used for harassment.

There was no way to block unwanted incoming iMessages, even though carriers offered various tools to block incoming calls and, in some cases, text messages from numbers you specified. The same was true for FaceTime audio and video.

It took until iOS 7, several years ago, for Apple to add the first blocking tools, which it’s gradually broadened since then. In this chapter, I look at built-in, automated, and third-party options for blocking unwanted contact.

Block Numbers and Email Addresses

Apple lets you block incoming voice calls, text messages, iMessages, FaceTime calls, and email messages.

Because email addresses can be used with iMessage, FaceTime, and email, and phone numbers can be used with SMS, calling, iMessage, and FaceTime, it makes sense to have a single block list across all these services.

You can block phone numbers and email addresses one at a time:

- In Phone, you can select any number and tap the info button (or select any contact) and then tap Block This Caller.
- In Messages, tap a conversation, tap the avatar, tap the info button, tap the right-pointing arrow at the far right (not the icons next to it), and tap Block This Caller.

- In FaceTime, tap the info button next to any Video or Audio entry, and tap Block This Caller.

- In Mail, tap a sending address and then tap Block This Contact.

Once you tap and confirm with Block Contact, all associated information is added to the Blocked list (Figure 59).

The list of blocked phone numbers and addresses appears the same whether accessed from Settings > Phone, FaceTime, Messages, or Mail. You can tap an entry to view all associated details, or swipe left and tap Unblock to allow them access to you again.

![Blocked List Example]

**Figure 59:** The Blocked list shows all banned email addresses and phone numbers.

**Note:** Caller ID is used to block phone calls, but unfortunately it’s not a secure method of identification. A harasser can turn off Caller ID or, with third-party services, change the number that appears.
Security encompasses many forms: What ways can you manage password use and create unique, secure logins? How do you deal with a device being stolen? How do you protect its contents when it’s out of your control? How do you prevent people from snooping on your network sessions? Can you recover your device if it’s lost? In this part of the book, you’ll get answers that will make you feel better when using a device in all situations.
Create, Manage, and Use Strong Passwords

Apple’s built-in password-management system creates, manages, and fills in strong, unique passwords for every web site you visit and every app you use that has opted to work with the system.

While Apple has tightly integrated its own approach, it also offers full-fledged integration of third-party password managers.

Tip: For a lot more about the ins and outs of good password management, read Joe Kissell’s Take Control of Your Passwords.

What Makes for a Good Password

Most of the advice you read about choosing a good password is bad, including the “strength” bars on web sites that purport to reveal the quality of password you picked.

Fortunately, password generators, including from Apple and third parties, have gotten with the ticket. Here are the accurate facts:

- Pick a long password made of words you can easily remember and type or tap when you need to enter it regularly, like with a password vault or your iPhone or iPad passphrase.
- When forced to use a complex password (letters, numbers, and symbols), it needs to be longer than 9 characters—preferably 12 to 14.
- Use a unique password every time you create an account anywhere, and change old passwords that you’ve reused to new, unique ones.
- Rely on a password manager, such as the Apple provided one.
- Sign up for Have I Been Pwned? to get notifications of breaches that include your email address.

Now, on to the particulars.

A long password made of randomly chosen words is as strong as a short one that’s a random collection of letters, numbers, and punctuation. For any password you have to enter, pick one that’s 20 or more characters long and that you can remember. Make up a story to help you remember, even. For instance, for rabbit-airplane-canada picture a rabbit flying an airplane to Canada.

**Note:** If you’d like to read more about using words in passphrases instead of incomprehensible nonsense, read my 2015 Fast Company article, “Everything You Know About Passwords Is Wrong,” in which I talk to an expert researcher on password selection and cracking.

In many cases, a web site or app forces you to pick a password that contains uppercase and lowercase letters, numbers, and punctuation. You also rarely need to enter those by hand, and so a complicated password is fine—but make sure it’s long. A web site password checker might tell you Apple10! is very strong and acceptable, but it’s only 8 characters and includes a word found in a dictionary. It could take seconds to minutes for a cracker using common brute-force software to crack it. Pick 12 to 14 characters for complex passwords.

Apple’s suggested passwords combine complexity and simplicity by being relatively long but (unless a web site doesn’t allow it) comprising only letters and dashes.

Every password you use should be unique at every site and service. That sounds horrible, which is why you can use Apple or third-party software to generate them for you. In both the OS and third-party software, you can see a list of all stored passwords that you have reused.

Finally, Have I Been Pwned? is a great resource run by an Australian security researcher and trainer, who carefully vets and collects information from database breaches. If he adds a breach to his site and you’ve
Most home networks are secured, and business networks almost universally employ some way of keeping outsiders out. Connecting to these secured networks is often as easy as entering a password, but not always. This chapter helps you handle any difficult security situations you encounter.

If you’re setting up Wi-Fi security for a network, this chapter also discusses what sort of security to use and how users with mobile devices will connect.

Wi-Fi security divides into three main types: methods used for small networks, methods for large ones, and outdated methods you should avoid.

**Note:** Cellular networks have their own security methods that users can’t affect.

**WARNING!** Public hotspots, whether free or fee, typically have no encryption protecting data; if they have security enabled, it’s via a shared password that provides no effective protection from other people on the network. When you connect, I recommend using only secured services or a virtual private network (VPN) connection. Read *Connect with a VPN* for details.

### Connect to a Small Network

Nearly all home and small-office networks that have wireless security enabled require the entry of a short password or passphrase. Enter the password when prompted, tap Join, and, if entered correctly, you’re done.
The password is stored for the next time you’re near the same network, and it’s automatically supplied by the OS. If you don’t want to join the network automatically the next time you’re nearby, or don’t want to store the password on your device, launch Settings, tap Wi-Fi, tap the info (i) button next to the network, and tap Forget This Network. (This only works while you’re connected to the network, however.)

If you have iCloud Keychain enabled, entering a Wi-Fi network password into any synchronized device means that you won’t have to enter it again. Thus, you might connect to a network via the OS that you’ve already connected to in macOS and not be prompted, and vice versa.

**WARNING!** Readers have told me that they can wind up in an iCloud Keychain loop: they delete a network on one device, but iCloud Keychain resyncs it from another before the deletion takes place and syncs outward! There’s no real solution: persist at removing the network until it “sticks.”

---

**Share a Wi-Fi Password**

iOS and iPadOS have two easy ways to share a Wi-Fi password with someone in the vicinity: One relies on Bluetooth, the other on a QR Code.

**Share a Wi-Fi password via Bluetooth**

You have a simple way to share a Wi-Fi password with someone nearby that requires just a single tap. Both the person already connected and the person connecting must have Bluetooth enabled, and the sharing person needs the iCloud account email in their contacts of the other person.

Let’s say you have the password and your friend Jo does not. When Jo tries to connect to the Wi-Fi network, they see the usual password entry field. However, if you’re near enough, your device shows a sheet with a large Wi-Fi logo that prompts you to share. Tap Share Password and Jo’s password field automatically fills in and they join the network.

**Share Network Access with a QR Code**

Back in iOS 11, Apple added a nifty visual way to share network details with a minimum of fuss: You can use a QR Code and the Camera app!
Apple’s two-factor authentication (2FA) for Apple ID lets you secure access to your accounts with a password plus something extra that you have under your control. In this chapter, you learn how to set up 2FA, how to secure your extra pieces against discovery or loss, and how to reset an account.

What Have You Got in Your Pocket?

Apple lets you tie in an Apple ID for several purposes in iOS and iPadOS: for iCloud sync, iCloud Drive, App Store purchases, iMessage, and more. However, without making an extra effort, an Apple ID is protected only by the password you set. It can be reset and potentially hijacked in a number of ways should someone gain access to your email or know your security questions for resetting a password.

The way around this is two-factor authentication (2FA). A factor is a bit of proof that you are who you say you are. Requiring two factors of different sorts makes it more likely that you are the legitimate owner of an account or have authorized access for a service.

A two-factor system generally employs something you know, such as a memorized password, coupled with something you have or possess—such as a phone, a smartcard, or other hardware—or something you are, like a fingerprint. Usually there’s an emergency backup, too: a one-time code that can be used in a pinch, or a process to prove your identity.

In Apple’s implementation, when you enable two-factor authentication, you keep your existing password on your Apple ID, and add at least one phone number that can receive SMS (text) messages or voice calls, and one or more trusted mobile devices or Macs.
**WARNING!** Once you turn on 2FA, if you can’t recall your password or lose access to your phone number and all your trusted devices, you have to go through a recovery process with Apple to regain access to your account, which can take up to a week. If you can’t prove to Apple you’re the legitimate owner, you have to create a new Apple ID, which makes you lose access to any associated purchases, unsynced items, backups, and the like.

**Tip:** Apple added automatic second-factor filling via SMS in iOS 12 for other companies’ sites, as I discussed in *iOS and iPadOS Help with SMS Login Codes*.

**Note:** Apple initially offered a harder-to-use *two-step verification* for improved account security. It dropped this older method a few years ago, but allows accounts that have it active to keep using it until any device connected with the account logs in from macOS 10.13 or later or iOS 11 or later. The account is then automatically upgraded to 2FA. Two-step is managed via Apple’s Apple ID site.

---

**The Risk of SMS 2FA Factors**

Even though a number of 2FA systems don’t primarily rely on SMS, and let you use a code-based system like Authy or Google Authenticator, most of them fall back to SMS if you simply click a link—no other validation is required. This is true of Apple’s system.

This is unfortunately increasingly risky, especially to protect email, financial, and other accounts that can be used in a cascade of cracking to steal your identity.

You may have heard about SIM (Subscribe Identity Module) hijacking, but if you haven’t, you need to know. A SIM is used with the majority of cell phones worldwide (and AT&T and T-Mobile in the U.S.) as a unique identifier for billing and to which the carrier assigns a phone number. You’ll note that if you move the SIM from one iPhone to another, the phone number follows it? That association lives in the carrier’s database.

With SIM hacking, someone uses social engineering—they call up a cell phone company or go into a store and fool someone—to get your phone number.
Connect with a VPN

The data that travels to and from your iPhone or iPad isn’t secure even when you’re connected to a Wi-Fi network with a strong password. Any data you send that’s not encrypted could be sniffed by anyone else on that network.

The same is true for any point between you and your data’s destination or wherever you’re running an active session, whether you’re using a protected Wi-Fi network, an open one, or a cellular data connection: any party in between, for unencrypted services, can see exactly what you’re doing.

Fortunately, nearly all the apps we use and most web sites now employ secure connections, checking that item off the list. But if you want to put a cherry on top, add a virtual private network (VPN). It makes sure that all your communications are wrapped inside encryption.

Umbrella Protection

A virtual private network connection is a nifty way to prevent any sniffing of your local network hookup. A VPN creates what’s called an encrypted tunnel that extends between a device—an iPhone, iPad, or laptop, or desktop—and a VPN server somewhere else on the Internet. This lets your information traverse any local network with protection as well as every node on the Internet between you and the VPN server.

For corporations, VPNs can extend the aegis of corporate security to remote devices. For individuals, that’s less the case. With a company, the VPN server is within the corporate network and any data leaving that server is protected by company firewalls and intrusion prevention.

But if you’re using a VPN just to protect your local link (the connection between your device and the hotspot), data remains encrypted only...
until it hits the VPN server, usually located in a data center. From that data center to its destination, data is unprotected (unless wrapped in an encrypted method, like TLS on the web, described earlier), but that’s typically just fine. The main locus of risk is the local link.

What about Other Data? When I began writing this book years ago, I had to include instructions for securing email, web connections, and other services. In 2019, however, the web has largely moved to https for everything, email connections are encrypted by default nearly everywhere, and encrypted messaging apps are readily available. VPN adds to security, ensuring that anything that remains sent in the clear gets wrapped up, while also making your activities—to what you’re connecting—invisible to peepers.

And because major Internet sites—like Google, Apple, and the rest—have distributed sets of computers and even private links to big data centers, the hop from the VPN server to the destination network may be within the same building or close by.

Before you can set up a device, however, you need to find a VPN service.

Get VPN Service via an App

Many, many apps offer VPN services from a few hours or a fixed amount of data to unlimited monthly plans. With a VPN for hire, the connection you make—as noted above—runs from your device using the local Wi-Fi or cellular network, then goes through any intervening local area network routers and higher-level backbone routers. It winds up at one of the company’s VPN servers located in a data center, where it’s then sent over the open Internet.

Note: You can also install a VPN app for the Apple Watch and Apple TV.

Pick a VPN app

Because it’s exceedingly inexpensive for an app developer to set up VPN service, many thousands of offerings proliferate, and it’s difficult to figure out which ones to trust.
Protect Your Device

Now that you know how to keep your data from being intercepted in transit, how can you prevent your stored data from being rifled if your iPhone or iPad is outside your control?

Apple has three robust ways to secure a device: with a passcode, Touch ID fingerprint-recognition system, and Face ID. All iPhones and iPads that support the latest operating system include either Touch ID or Face ID and associated robust hardware encryption.

When a device is on and locked, its data is inaccessible until a passcode is entered or Touch ID/Face ID accepted, which unlocks the encryption keys needed to read stored information.

**WARNING:** If you forget the passcode and Touch ID or Face ID isn’t available (such as after a reboot), your data stored only on the device is lost forever. iCloud and other cloud-stored data remains available as long as you have that account information.

Use a Passcode

Your best single protection against anyone unauthorized having access to data is enabling the passcode lock. This allows you to set a six-digit code required to wake and gain access to the device.

When Touch ID or Face ID are enabled, you must also have a passcode set, and Apple will ask you for that passcode on a regular basis.

Let’s start with setting up a strong passcode, and then move on to when you’ll be prompted for one.
Set up a Passcode

To set the passcode lock, follow these steps:

1. In Settings, tap Passcode. On Touch ID–equipped devices, the option reads Touch ID & Passcode; with Face ID, Face ID & Passcode.

2. Tap Turn Passcode On.

3. If you want to use the default, a six-digit passcode, tap it in and re-enter it when prompted.

   You can also opt to tap Passcode Options and pick an alphanumeric password of letters, punctuation, and numbers; a custom numeric code; or a four-digit numeric code (Figure 84).

![Passcode Options](image)

Figure 84: You can opt for a more complicated or shorter passcode.

WARNING: Many mobile security gurus say not only is four digits too few to resist cracking, but six isn’t enough, either. They recommend picking a memorable short phrase that’s easy to enter but impossible to guess. See Create, Manage, and Use Strong Passwords for advice.

You can also enable the passcode lock remotely if you have an active iCloud account and Find My iPhone enabled on the device. See When Your Device Goes Missing, ahead.

The Require Passcode option offers a few choices if you don’t enable Touch ID or Face ID, depending on your device:
When Your Device Goes Missing

Your mobile device is a desirable item for thieves. It’s compact, it has a high retained value, and there’s a huge market for used models.

Without freaking you out about theft, I want to tell you how you can protect your data when your device has disappeared, make it impossible for a thief to use your device, and find your device if it’s stolen or lost.

How Find My Works

You can find the last reported position of any iPhone, iPad, or Mac via Find My, which is linked to your iCloud account. You can see the device’s location, play a sound on it, lock it or mark it lost, or erase it!

Note: U.S. phone carriers also offer phone-tracking services, which can work across a family account and different smartphones and dumb phones. Each comes with a separate fee and various enhancements and limitations. If everyone in your family is using an iPhone, there may be no advantage.

With Family Sharing turned on, anyone in the group can see where an iOS device is, unless the owner has disabled letting that person or anyone see his or her current location. With that user’s password, all Find My features are available through other Family Sharing members’ accounts.

Note: Apple combined Find My Friends and Find My iPhone into the single Find My app in iOS 13, iPadOS 13, and macOS 10.15.
How Find My Sends Its Location over Wi-Fi or Cellular

The feature relies on a device sending Apple’s servers a regular update of location information derived from Wi-Fi, cellular, and GPS signals and data. All devices that can use Find My (back several years) provide details using Wi-Fi; iPhones and cellular iPads add cellular radios and GPS.

With Find My active, a device with GPS and cellular regularly sends updates over Wi-Fi or cellular networks derived from its GPS receiver and from ranging information it has about nearby cell phone towers that allow it to trilaterate.

**Note:** You may be more familiar with the term *triangulation*, which relies on using known fixed positions and measuring angles. *Trilateration* uses the intersection of geometric areas, such as the radius of signal strength from cell towers.

However, all iOS and iPadOS (and macOS) devices also scan for nearby Wi-Fi networks and send a snapshot of that information to an online system run by Apple whenever the device has an Internet connection.

Apple integrates that with information fed to it by iPhones and iPads with GPS built in and examines signal strength of Wi-Fi gateways, allowing it to figure out fairly precisely where each is located. (Gateways broadcast a unique hardware network identifier along with a network name, which can be scanned without connecting to a network.)

**Note:** Apple *caches some information* about location on the phone for up to seven days to avoid frequent network access to look up information, or to use Wi-Fi positioning in an area you’ve been recently even if you don’t have current Internet access.

This is a two-way connection: Through Find My on one of your other devices or via iCloud.com, you can push a sound and message, as well as lock or erase the hardware.

Using Find My also tells your remote devices you’re looking for them, and when they receive that message, they update their position more regularly, typically even if they’re in a standby mode.

There’s a flaw with this finding process, of course: A lookup requires an active connection.
Update History

version 1.0 (September 19, 2019)
Initial release.

version 1.0.1 (September 20, 2019)
Bug fixes. Added details about Sign In with Apple and controlling sharing location when sharing photos.

version 1.0.2 (September 24, 2019)
Expanded information about joining a Wi-Fi network via the Control Center's networking area and by sharing a password with someone in your contacts who is nearby. Expanded details about photo and Bluetooth/iBeacon sharing.
I dedicate this book as always to my wife, Lynn, and kids, Ben and Rex. On this journey through life, we are trying our best every day. They ground me and remind me to leave the house at times.

Thanks to Jeff Carlson for technical editing and proofreading on this edition, and Charles Fleishman, Scout Festa, and Jeff for their varied editing assistance across several editions!

Thanks to Joe Kissell, publisher of the Take Control books series, for his interest and support in distributing this independently produced book.
About the Author

Glenn Fleishman was trained as a type setter, received a degree in art, and works as a journalist, type historian, and programmer. Glenn appears regularly in Macworld, Increment, TidBITS, Fast Company, and other publications where he writes about security, copyright, punctuation conventions, printing history, and much more.

He spent 2017 as the Designer in Residence at the School of Visual Concepts in Seattle, printing his book Not To Put Too Fine a Point on It. In 2018, he released the book London Kerning, about typographic museums and memory in that city. In 2019, he launched the Tiny Type Museum & Time Capsule, a project to build 100 tiny museums full of printing artifacts. In October 2012, he appeared on the Jeopardy! quiz show and managed to win—twice!

His blog is glog.glennf.com, and he overshares on Twitter at @glennf.
Copyright and Fine Print

Connect and Secure Your iPhone and iPad
Covers iOS 13 and iPadOS 13
Copyright ©2019, Glenn Fleishman. All rights reserved.

ISBN 978-0-9994897-9-6 (ebook) / 978-1-7334954-0-0 (print)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112–2629 USA

http://glennf.com/guides

Ebook edition: This electronic book doesn’t use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. You have our permission to make a single print copy of this ebook for personal use. Please reference this page if a print service refuses to print the ebook for copyright reasons.

All editions: Although the author and Aperiodical LLC have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed “As Is,” without warranty of any kind. Neither Aperiodical LLC nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are the trademarks or that are the registered trademarks of Apple Inc.; to view a complete list of the trademarks and of the registered trademarks of Apple Inc., you can visit


Click here to buy the full 185-page “Connect and Secure Your iPhone and iPad” for only $20!