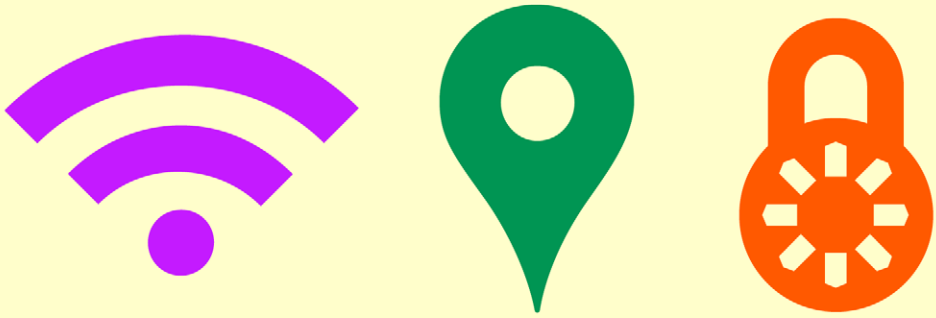
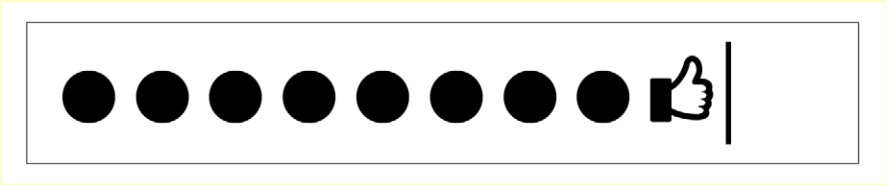
A Practical Guide to

NETWORKING, PRIVACY & SECURITY IN iOS 11





BY GLENN FLEISHMAN

Welcome

Welcome to *A Practical Guide to Networking, Privacy, & Security in iOS 11*, version 1.1, written by Glenn Fleishman, originally published in October 2017 by Aperiodical LLC, and updated in December 2017. See **page 179** for updates to this edition.

This book describes how to use your iPhone, iPod touch, or iPad with iOS 11 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 iOS device, the Apple Watch, Safari's cookie protections, Personal Hotspot and Instant Hotspot, two-factor authentication with an Apple ID, using AirDrop and AirPlay, and solving connection problems.

Visit **our updates page** to check for new versions and re-download any of the ebook files. Use the password `wickedgood`. **Sign up for our 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 we release future editions covering newer versions of Apple's operating system. We will not sell, rent, or share your information.

Find us on the web at **http://glennf.com/guides**.

Introduction

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 iOS device, requiring little thought as to how it connects to a cellular or Wi-Fi network, it becomes quite complex as soon as you drill down to any details. This is especially true when connectivity fails, and you try to troubleshoot.

Privacy is a subject that deserves much more attention than it's gotten in the past—and people are starting to pay attention. 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 provides tools that enhance your ability to control that.

Security is an even denser area. Apple makes the default choices in iOS reasonably secure, but to ensure real protection for your data—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.

TABLE OF CONTENTS

NETWORKING

PRIVACY

SECURITY

NETWORKING

It's true that an iOS device can be used without a live network connection, but its natural state is always hooked up. In the first part of the book, you'll learn how to work with the three types of iOS 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, 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. Networks that use the same network name for both bands or on multiple base stations appear as a single entry. Tap a network name to attempt to join it.

> ***Not seeing an expected network?*** *See* ***Wi-Fi Troubleshooting****.*

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.

Once your iOS device joins a network, the network name and any associated login information is added to an internal network list. Unlike in macOS and Windows, you can't examine this list and remove entries. The device uses this list to re-join a network when it is in range.

Tip: Are you tired of your device popping up a list of nearby Wi-Fi networks while you're trying to do something else? Turn off Ask to Join Networks, described a couple of pages ahead.

Tip: You can remove a stored network's entry only when you're connected to it. See **Forget This Network**.

Apple Watch Wi-Fi and Cellular

In addition to communicating with a paired iPhone via Bluetooth, every Apple Watch can connect to its iPhone using Wi-Fi if they're both on the same network. However, for an iPhone and Watch to be on the same Wi-Fi network, the network has to meet some very particular criteria:

- The network must use the 2.4 gigahertz (GHz) band. (See **Wi-Fi Troubleshooting**.)
- For an open or hotspot network, it must not have a portal or login page.
- For password-protected networks, the iPhone associated with the Watch must have previously connected to the network.

With watchOS 4, you should be able to connect to a new Wi-Fi network without the iPhone nearby as long as it has no password and no portal to use iPhone-free features, like maps.

Apple Watch Series 3 has an option for cellular networking—allowing access to notifications, email, texts, and more—even when the iPhone isn't available . But owners aren't required to activate it and pay for cell data access. When a Watch Series 3 has an active data plan, it only works on the carrier's footprint—there's no roaming available.

Managing Wi-Fi Connections

iOS centralizes Wi-Fi management in the compact space of the Wi-Fi settings view (**Figure 1**). To reach it, open the Settings app and tap Wi-Fi.

The Wi-Fi view always shows three elements, but optional fourth and fifth items may also appear:

- **Wi-Fi switch:** Tap this switch to disable and enable the Wi-Fi radio. The currently connected network, if any, appears beneath the switch.
- **Personal Hotspots:** If an iPhone or iPad is nearby running iOS 8.1 or later, it appears as a Personal Hotspot, whether or not that feature is active. (This is the Instant Hotspot feature described—and shown in figures—in **Turn On via Another Device**.)

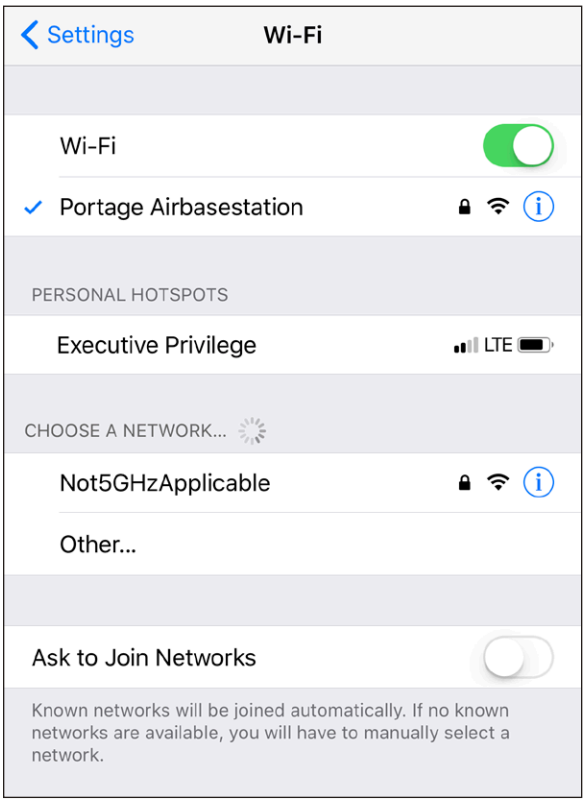


Figure 1: *The Wi-Fi view has a list of available networks.*

- **Choose a Network:** In this area, you may see a list of networks. Each entry in the list has three or four elements:
  - **Network name:** A network uses this name to *advertise* itself to Wi-Fi adapters that are looking to make a connection. The network name is also called the SSID (Service Set Identifier) in some of the geekier base station configuration tools.
  - **Security recommendation:** If you connect to a network that isn't encrypted, this message is displayed.

- **Lock icon:** A lock may appear, indicating that there's some form of protection on the network.
- **Signal-strength indicator:** One, two, or all three radio waves in the indicator are black (starting at the bottom) to show the strength of the signal being received by the device.
- **Information:** Tapping the info ⓘ button—or, starting in iOS 11, anywhere in the network name's line—reveals technical details about the network, as well as an option to forget the network. For more about these details, see **Drill Down to Network Details**, a few pages ahead.

- **Set Up an AirPort Base Station:** This option appears only if your device detects a nearby unconfigured Apple-branded base station. (I talk more about that in ***Take Control of Your Apple Wi-Fi Network***, a guide to wireless networking with Apple base stations and hardware, published by Take Control Books.)
- **Ask to Join Networks:** With this switch, choose whether to be alerted about nearby networks to which the device hasn't previously connected.

> **Tip:** If Ask to Join Networks is off, you won't be alerted about new networks nearby when a known network isn't available. However, the Choose a Network list always shows all named networks around you.

Drill Down to Network Details

For most network connections, you don't need to go beneath the surface. However, for an unusual connection, such as one requiring a fixed, or static, network address or a different domain name server than the network's default, go to Settings > Wi-Fi and then tap the info ⓘ button or anywhere in the line for the current network (a checkmark is by the listing) to set up the connection details.

The resulting view has the network name at top and three or four configuration areas, depending on the network (**Figure 2**). Let's look at each.

Unsecured network

Apple added a fairly severe warning about using an unencrypted network connection in iOS 10. It displays "Security Recommendation" in the main

Wi-Fi view, and then explains further in this details screen. And it has a link to follow to get even more information.

What makes the message seem a little silly is that it appears for all public hotspots—including the ones in Apple Stores. It should rather suggest you use a VPN, which I discuss in **Transfer Data Securely**.

Forget This Network

Tap the Forget This Network button to remove the network from the list of previously joined Wi-Fi networks. This also disconnects the device from the network immediately and prevents it from connecting to that network automatically in the future. Forgetting a network can solve network problems, too, by letting iOS dump any corrupted or cached information before the next time you connect.

Auto-Join

Auto-Join lets you opt whether to connect the next time the network is nearby. This lets you keep a stored profile that you can tap to use without having it connect automatically. (A separate option, Auto-Login, only appears for hotspot networks where iOS has recognized that there's a portal in place. See **Auto-Join and Auto-Login the Next Time**.)

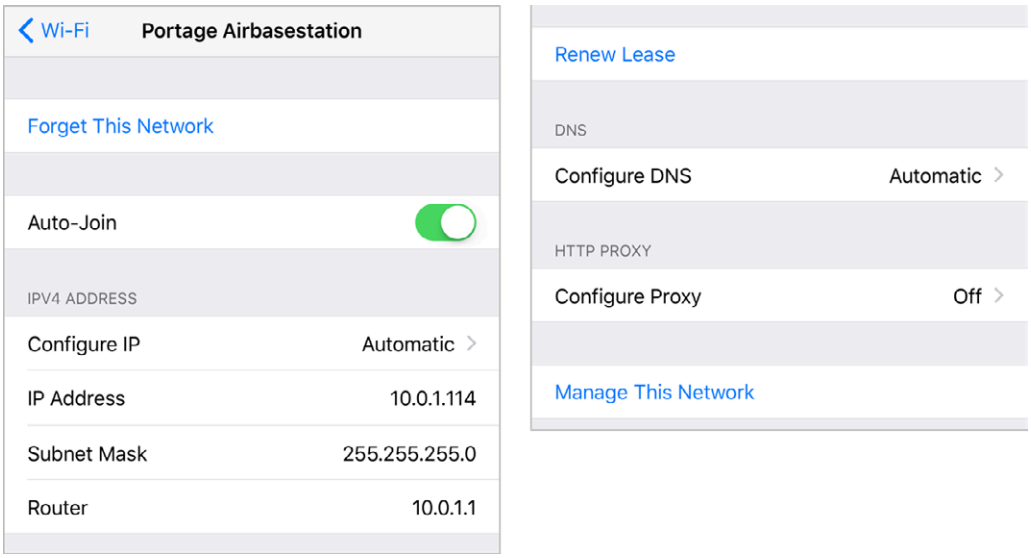


Figure 2: *You can view or set network connection values. (View split for legibility.)*

Renew Lease

The Renew Lease button is specific to DHCP. A lease is the assignment of an address by DHCP to your device. A lease can have a duration (like 15 minutes or 15 days). Occasionally, when you seem to have a network address but can't connect, tapping Renew Lease will obtain a new address and resume connectivity.

IP Address

The IPv4 Address section covers TCP/IP values used for addressing and routing. You start with a Configure IP menu that lets you pick among Automatic (DHCP), Manual (to tap in a fixed address), and BootP.

> **Note:** Apple shows IPv4 Address or IPv6 Address (or both) depending on the version of addressing used by your network. IPv4 is the original Internet flavor. IPv6 is over 15 years old, and adds a bazillion more unique adddresses to cope with the Internet's growth, but it's only now coming into wider use.

You should almost never need to change this from Automatic, as DHCP (Dynamic Host Configuration Protocol) is the most common method of obtaining an address. DHCP lets your mobile gear request a network address from a router on the network, and then use it to interact on the local network and beyond.

Back on the main Wi-Fi setup screen, when your device uses DHCP to get an address on the local network, you can't change the IP Address, Subnet Mask, or Router fields, as those values are provided by the DHCP server on the router.

Use the Client ID Field for a Fixed Network Address

On a home or work network, you may want to assign a fixed address to your devices. Apple offers this option as DHCP Reservation in the AirPort Extreme, Time Capsule, and AirPort Express base stations.

In your device's Configure IP settings, if you enter a unique value in the Client ID field, like `Glenn's iPad Pro`, you can set your base station to assign the same local network address to your device every time it connects over Wi-Fi to the network.

This is useful if you want to use a consistent IP address to connect to certain apps that provide network services, like Air Sharing HD and GoodReader, for remote access to file storage. For details on configuring DHCP Reservation, read my book ***Take Control of Your Apple Wi-Fi Network***, published by Take Control Books.

DNS

DNS (Domain Name System) is used to convert human-readable domain names, like `www.glennf.com`, into machine-readable IP addresses, like `173.255.209.35`.

Tap Configure DNS and then tap Manual to make changes from the defaults set by DHCP. This can be useful if the network to which you're connected has poorly run or slow default DNS servers. Tap the + to add additional DNS servers and the – to remove them.

The Search Domains option is something that only a network administrator should need to tell you to set.

Tip: Unfortunately, you can't set DNS for every connection in iOS—you can set it only for individual networks. It's only worth the effort to set it for connections you use frequently, such as your home Wi-Fi connection.

HTTP Proxy

This option, located at the bottom of the detail view, is typically used only in companies and schools. It redirects web requests that you make to the Internet at large to a local server that handles them indirectly. It also allows the use of a caching proxy, in which recent pages retrieved by anyone in an organization are fed to you from this server instead of from the remote web site. This reduces bandwidth consumption.

Manage This Network

On a network that uses Apple's Wi-Fi hardware, this button will appear. Tap it, and it launches the AirPort Utility app if it's installed, or prompts you to download it if not. The app lets you view the network's configuration, make changes, and examine some details of operation.

Turn Wi-Fi Off

Whenever the Wi-Fi radio is active, even if you aren't connected to a network, it's scanning for networks, which can slowly drain the battery. If you're nowhere near a network you can access or if you want to conserve battery life, turn off Wi-Fi by tapping Settings > Wi-Fi and then setting the Wi-Fi switch to Off. (See **Airplane Mode** for more details.)

> ***WARNING!*** *Control Center also has a Wi-Fi switch, but tapping it only* ***disconnects*** *from the current Wi-Fi network. It doesn't turn Wi-Fi off, but temporarily disables networking connections. This is because Apple now uses Wi-Fi (and Bluetooth) for a lot of purposes beyond local area networking. For the full details, see* ***Airplane Mode****.*

Capture the Page

iOS has a clever feature that lets it display a hotspot network login screen and, in some cases, remember the login and other details. However, you can get stuck reconnecting to the same network.

You'll find these types of networks in public places such as cafés, libraries, and airports. After you connect to the network, which appears as open and unprotected, you're required to launch a browser and view a hotspot connection page (also called a captive portal) before you can use the Internet.

Normally, to reach the captive portal, you must try to visit any web site in a browser, and have your browser be redirected by the network to the login page. Instead, iOS (and on a Mac since 10.7 Lion) does a test that detects such redirections whenever you connect to a Wi-Fi network.

Immediately after your iOS device joins a Wi-Fi network, it tries to connect to Apple's web site. If it doesn't get through, it assumes that it has reached a captive portal. Then, the next time anything happens on the device that requires Internet access (like retrieving email), iOS displays a special screen showing the portal's web page as if it were in Safari.

The hotspot network's captive-portal page will typically ask that you do one of the following (rarely more than one):

- Read a set of terms and conditions for use and tap an Agree button; enter an email address and tap an Agree button; or check a box that says "I agree" and tap a Submit button.
- Require that you register an account to use the network at no cost. With an account, you can log in and use the network.
- Require that you either pay for a connection to the network using a credit card, or enter login information for an active account on the network or an active account of a roaming partner.

After you carry out any of those actions, iOS should close the special screen and Wi-Fi service should be available. These pages are still often absurdly not customized for mobile devices, and the type and buttons are tiny. You'll need to pinch to zoom in almost all of the time.

Connect to a Captive Portal If It's Not Detected

If the special screen doesn't appear, you can reach the captive portal by launching the Safari app. Most of the time, the previously visited page in Safari will try to load; if you have a blank page, enter any site address, like `example.com` or `apple.com`, and tap Go.

After you enter any required data, the login system should redirect you to the web page you tried to visit in the first place.

Mobile Device Hotspot Access via Boingo

If you travel frequently or work in many different areas, an alternate way to connect to hotspots is by paying for a Boingo Wireless plan. The Boingo for Consumers plan has a flat monthly rate to connect to more than 1 million hotspots worldwide. Boingo's iOS and other apps automatically join free networks, too, bypassing the special screen and login procedure you often have to go through. You launch its app to connect.

The mobile plan lets you connect to any of its hotspots worldwide using up to four phones, tablets, cameras, or the like at a time. A North and South America plan allows two devices, including laptops, at a time. An unlimited laptop plan covers 200,000 hotspots and also allows up to four of anything. Boingo also has regional and global plans, as well as hourly and pay-as-you-go services.

Auto-Join and Auto-Login the Next Time

The next time you visit a hotspot network that you've previously accessed, iOS will automatically join the network and attempt to use the same credentials or button clicks that you used the previous time to gain access. This can lead to problems if that information is no longer valid or if the device doesn't present it correctly.

In my testing, iOS often shows the same screen for login again without automatically filling it, especially if there's an Agree button to tap in order to avoid you agreeing to terms that might have changed.

You can disable joining and logging in to the network again in this fashion by turning off Auto-Join or Auto-Login for the connection, the second option available only when you are connected to the Wi-Fi network, even if you haven't logged in or proceeded past the connection web page (**Figure 3**).

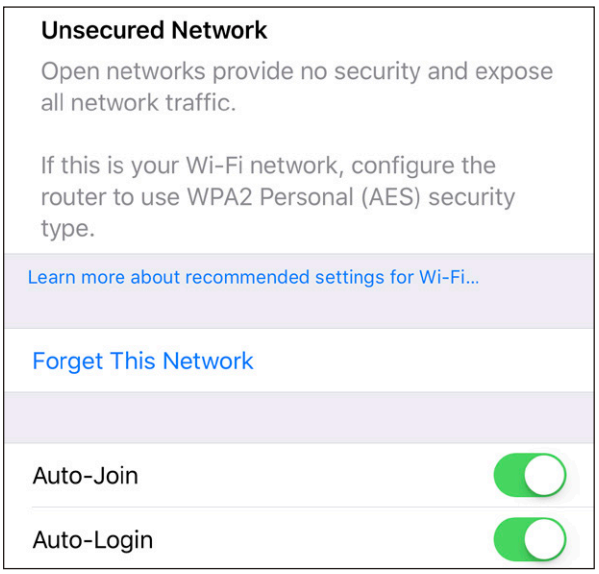


Figure 3: *iOS shows Auto-Login when you connect via a portal.*

To turn off Auto-Join or Auto-Login, follow these steps:

1. In the Settings app, tap Wi-Fi.

2. In the Choose a Network list, tap the info ⓘ button to the right of the network name.
3. In the configuration view, switch off Auto-Join, Auto-Login, or both.

Time-Limited Hotspot Access

Some hotspots limit your use to a specific period of time. This might be implicit, using your unique network adaptor's ID—its MAC (Media Access Control) address—or another bit of tracking information based on when you first accepted a network's terms of services.

Some locations with hotspots give you a network code to enter at a portal page, which grants you access for a fixed amount of time. In those cases, you should turn Auto-Login off; otherwise, the next time you connect, it may attempt to enter a one-time use code that's expired, and it may be difficult to connect properly with a new code.

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 from the screen's bottom 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 iOS 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.
- Wi-Fi networks can operate over two frequency bands: 2.4 gigahertz (GHz) for the 802.11b, g, and n standards, and 5 GHz for the 802.11a, n, and ac standards. However, not all iPhones and iPod touches have 5 GHz radios. iPhones before the iPhone 5 and iPod touches before the 5th generation can't access 5 GHz networks, and neither can the Apple Watch. (All devices support 2.4 GHz, however.) It's rare but possible a network you need only operates in the 5 GHz band.

> **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 iOS 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 connection 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:

1. Launch Settings.
2. Tap Wi-Fi.
3. Slide down until you can tap the Other button (**Figure 4**).
4. Enter the network name exactly and, if there's a password:
   a. Tap Security.
   b. Select the method (almost certainly WPA2).
   c. Tap Other Network to return to the previous screen.
   d. Enter the password in the Password field.
5. Tap Join.

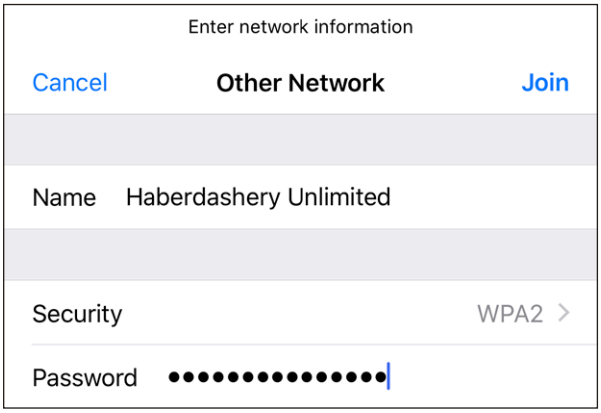


Figure 4: *The Other Network option lets you enter a network name and optional password from scratch.*

Tip: If you don't know the kind of network security on the network you're trying to join and you have a Mac nearby, hold down the Option key and select the Wi-Fi menu, then hover over the network name. A small popup displays the security type.

Tip: Starting in iOS 11, you can also tap a key icon above the keyboard to search through your stored passwords. This lets you pick an existing password, rather than re-entering it, if you have the correct password stored.

Correct Password Not Accepted

As described in the chapter, **Connect to a Secure Wi-Fi Network**, a network that requires either a password or a username and password will reject your device if you enter it improperly.

But what if you're positive you're entering the password or username and password absolutely correctly?

- Check whether you were given the password with correct capitalization, which counts in Wi-Fi passwords as in others.
- Spaces can be part of WPA2 passphrases, but spaces are hard to indicate when written down. Confirm you're not missing a space.

No Internet Service after Connecting

You connected to a Wi-Fi network but cannot access the Internet from any programs you try. Here's how you can figure out what's wrong.

Check a Web Page with Safari

The most common cause of this problem is that you've connected to a network—likely a hotspot network, but possibly a guest network—that requires a password, button tap, or other action.

Launch Safari and try to reach any page, such as google.com:

- If you are redirected to a login page, follow the instructions. You may need to pay for access, or you may have connected to a network that requires a password; consult **Capture the Page** for more information.

  Remember to forget: *Because you've connected successfully to the Wi-Fi network, even though you haven't been granted access to the Internet, you need to remove the network from the list of those you've previously joined or you'll have this problem every time you're in range. Tap Settings > Wi-Fi, tap the info ⓘ button beside the network name, and then tap Forget This Network. Tap Confirm.*

- If Safari throws up a connection error, try the next fix.

Check or Ask about the Base Station

If you're on a network where you can control the base station or ask someone who has access (a friend, barista, network administrator, or the like), you might ask them to confirm that there's no problem.

In some cases, a base station can continue to provide service to users who are already connected, but not properly allow new users to connect. Some have limits, as low as five or 10 connected devices, and that limit may only rarely be hit.

Check IP Address Settings

This may sound obscure, but it's an easy way to see if your device has obtained a network address from the router to which you've connected. To check on your assigned IP address, follow these steps:

1. In Settings, tap Wi-Fi.
2. Tap the network name.

   The IPv4 Address section should be set to Automatic for almost all networks; another value should be chosen only if you've been told otherwise. (See **Drill Down to Network Details**, earlier in this chapter.)

   If the IP address starts with `169`, then iOS wasn't able to obtain an address from the network. The `169` address range is self-assigned, meaning the device gave itself an address that can't be used on the network, and stopped checking.

   Here are several ideas for fixing the IP address:

- Tap Renew Lease; this causes iOS to ask again for a network address. If successful, the IP address will change from a number starting with `169` to an address starting with another range, typically `192.168` or `10`.
- In the main Wi-Fi view, tap the Wi-Fi switch to Off, wait a moment, and tap it back to On. Tap the network's name to see if the address is now assigned.
- If you're at an event or a hotspot venue, ask the network's operator, the front desk, or whomever. The router may have crashed. (You can look around and see if other people look frustrated, too.)
- Restart the device. Press the Sleep/Wake button until a red slider appears. Slide to power off. Wait until the spinning indicator disappears and the screen turns black. Hold the button down again for a few seconds. An Apple icon appears, and the device starts up.

Make a Mobile Hotspot

Every iPhone and every iPad with cellular has, in addition to a Wi-Fi radio, 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.

iOS's 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.

Which models? *Every iPhone model and iPad with cellular that can use iOS 9 or later can make use of every option.*

WARNING! *Most cellular operators, including the four big U.S. carriers, 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, or throttle you to 128 Kbps 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 iOS device or through another computer or iOS device.

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 don't treat it any differently than a regular Wi-Fi or Ethernet network—which can mean it's easy to rack up huge amounts of usage. You will want to pause or disable sync services, like Dropbox, and online backup systems, like Backblaze. You may also want to avoid using any streaming video services or digital media downloads while connected via a Personal Hotspot.*

Turn On in iOS 9 or Later

Enable it in Settings > Cellular Data (iPad) or Settings > Cellular (iPhone).

Tap Personal Hotspot to open the Personal Hotspot screen. Now you can switch the hotspot on and set a Wi-Fi password. The screen is also full of connection information (**Figure 5**).

After the first time you tap On, Personal Hotspot appears as an option on the Settings app's left pane (iPad) or main screen (iPhone) so you can access it quickly. (It's also found in Control Center if you hold down on the network connections area.)

Figure 5: *The Personal Hotspot view lets you turn access on or off as well as set a Wi-Fi password.*

Personal Hotspot has three states 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's on standby

You can turn Personal Hotspot off only from Settings. You can use Control Center to turn it on when it's off, and after that you can only toggle between Discoverable and Not Discoverable. That lets you leave the hotspot on, but temporarily disable it without going to the Settings app.

Philosophically, I'm not sure there's much difference between Off and On but Not Discoverable.

Turn On via Another Device

If you have multiple iOS devices running iOS 8 or later, or the right vintage of Mac running Yosemite or later, you can take advantage of Instant Hotspot, a feature that lets you turn on Personal Hotspot from another device.

Instant Hotspot is part of Continuity, a set of connections between your iOS devices and between iOS and macOS. However, the devices must meet a list of conditions for Continuity to work:

- You have iOS 8.1 or later or starting with OS X 10.10 Yosemite or later installed on the computer or device you're using to activate the hotspot, and at least iOS 8.1 on the device you're using as a hotspot.
- Your Mac is a model released in mid-2012 (MacBook Air and MacBook Pro) or later (Mac Pro, Mac mini, and iMac).
- Your iOS device was released in the last few years. (See **complete list**.)
- Your iPhone and the other iOS device or Mac are signed in to the same iCloud account.
- Both devices have Bluetooth enabled and are on the same Wi-Fi network.

On a Mac, select the Wi-Fi menu, and choose the device in the menu under Personal Hotspot (**Figure 6**).

On another iOS device, launch Settings, tap Wi-Fi, and choose the device in the Personal Hotspots list (**Figure 7**).

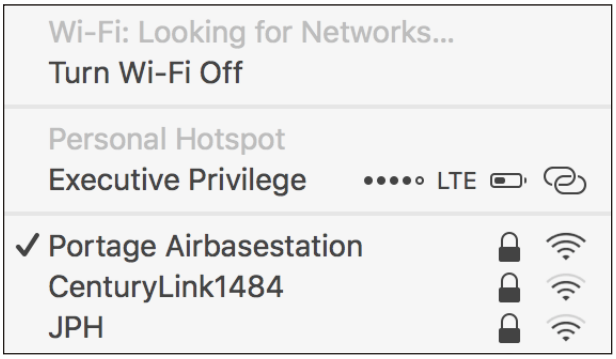


Figure 6: *Instant Hotspot puts an iOS device into your Wi-Fi menu in macOS.*

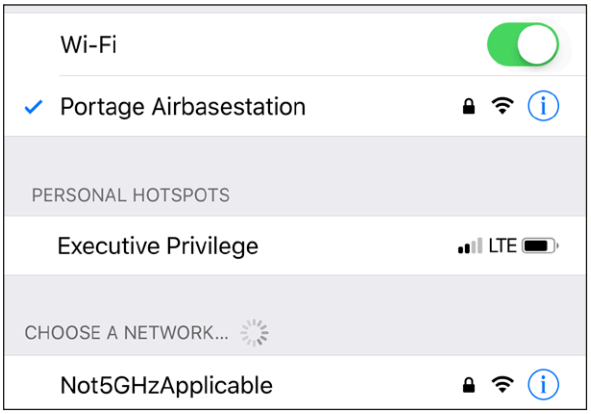


Figure 7: *In iOS, pick a device from the Personal Hotspots list.*

Even if you're not planning to connect, you can see the battery life, signal strength, and connection strength of your iOS device as a compact set of graphics in the menu or list.

You Can't Always Use Cell Data while Talking

It can be a little confusing to tell whether an iPhone can continue to have an active cellular data connection while a voice call is underway. On some carrier networks, data is suspended; on others, it slows. Wi-Fi data always works during a voice call, but when you're using Personal Hotspot, you're always relying on the cellular network for data backhaul.

Whether you can talk and use data at the same time depends on several factors, including carrier network. AT&T, T-Mobile, and most other networks around the world use one cellular technology for voice (called GSM), and Sprint and Verizon use another (known as CDMA). But all four—and nearly all carriers worldwide—have converged on LTE for their fastest, latest networks. (Apple switched from CDMA-only and GSM-only phones years ago to models that can activated on either type of network and later used on the other type with some provisos.)

Digital cell technology is divided up into second-, third-, and fourth-generation (2G, 3G, and 4G) standards, plus some interim ones 2G was the first to carry digital voice, and all forms of 2G allow either data (at dial-up modem speeds) or voice, but not both at once.

The 3G standard that GSM network operators picked could carry voice and pure data at once, but Sprint and Verizon opted for a flavor of network that would carry data only over 3G.

LTE is a 4G standard that was designed to allow voice and data to intermingle for all phones and carriers. However, phones and networks were upgraded before the voice part, known as Voice over LTE (VoLTE), was ready to go. (VoLTE and a higher-quality voice compression algorithm mostly rolled out together, so a VoLTE call also *sounds* better.)

Data networking without VoLTE

When there is an incoming voice call or you place a call:

- **Verizon, Sprint, and most CDMA networks:** Data use, including Personal Hotspot, is immediately suspended.
- **AT&T, T-Mobile, and GSM networks:** Data use continues, but is shunted to a 3G, 3G+, or pre-LTE 4G network.

  If you don't answer a call or when you hang up, data use returns to the highest-speed available network.

Data networking with VoLTE

The list of requirements to make or receive a VoLTE call has reduced over the few years that I've revised this book, making it easier to both have high-quality voice calls and keep using data:

- **Requires an iPhone released in 2014 (iPhone 6/6 Plus) or later.** Even though earlier iPhone models seemingly had the circuitry, these models are the only ones supported in the U.S. and most other countries
- **May have to be on the same network.** VoLTE works between carrier networks—sometimes! There's no way to be sure, but AT&T, T-Mobile, and Verizon are all working together as of mid-2017.
- **Carrier must have deployed.** Only Sprint has remained behind on VoLTE.

If you meet these requirements, receiving a call or placing one will happen relying on VoLTE, and your Personal Hotspot or other data use will continue at full LTE speeds.

Set a Wi-Fi Password

When you first turn on Personal Hotspot, iOS creates a strong WPA2 password. To connect a device over Wi-Fi to the hotspot, you must enter this password on that device.

The default password created by your phone was once a sequence of recognizable words and numbers with certain carriers. Now, in all my testing, it's always a random set of letters and numbers

You *must* use a password—Apple doesn't let you have an open hotspot. But you may choose to compose your own. You have to enter one that's eight characters or more, although you can make that `12345678` if you must. Tap to enter your own password.

For this kind of connection, where it's not a base station in a fixed location that someone might try to access, I suggest thinking of an eight- or nine-letter word and adding two punctuation marks to the end, like `memorable?%`.

Extra Security with Personal Hotspot

Using USB, Bluetooth, or Wi-Fi to connect to a hotspot device provides a strong layer of security around your connection, which is reassuring if you're at a location like a coffee shop, where the network may not be well secured. USB is a physical connection and can't be monitored. Bluetooth has its own strong automatic security. Apple's required use of WPA2 Personal for Wi-Fi ensures protection there, too. (See **Connect to a Small Network**.)

Although the backhaul to the mobile broadband network isn't impregnable, it does require either a dedicated effort to crack your particular communication or a wiretap at the carrier to intercept data. Personal Hotspot lets you secure the local link at a location where you would otherwise use Wi-Fi but where I would recommend using a VPN (virtual private network) to prevent interception by those around you.

Name Your Wi-Fi Network

The Wi-Fi network has the same name as your iOS device. This is typically your name, or that of whichever account you used to set up the iOS device (**Figure 8**). If you don't feel like broadcasting your account name whenever you turn on Personal Hotspot, you can change it.

To change the name, visit Settings > General > About > Name and enter a new name. Or, with the device connected to iTunes via either USB or Wi-Fi, click the device's icon in the top bar in iTunes, then click its name to select it, which highlights the name. Type a new name, and click again or press Return. Turn Personal Hotspot off and back on for the new name to be broadcast.

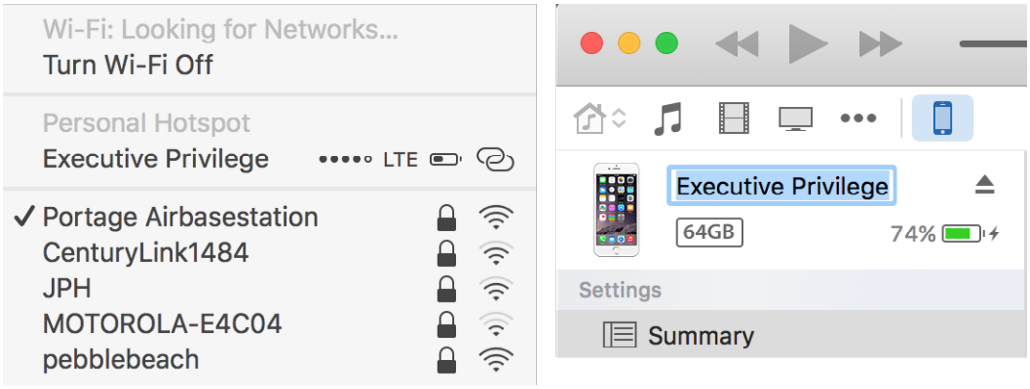


Figure 8: *The Wi-Fi network name (left) is identical to the name of your device, which you can see in iTunes (right) or in Settings.*

Consider Turning Off Certain Radios

Now that you've turned on Personal Hotspot, you might not want it to be available through Bluetooth or Wi-Fi, because nearby devices of yours

might accidentally connect to it. The only way to prevent a connection from a device with the right credentials is to turn off those radios.

If you use Settings > Wi-Fi or Settings > Bluetooth to disable either or both of those radios, this can also disable a number of other iOS features, like Continuity and Apple Watch connectivity.

For that reason, iOS 11 added a kind of standby mode via Control Center. Swipe up from the bottom (or down from the upper right with an iPhone X) to show Control Center and tap Wi-Fi or Bluetooth and they switch to Not Connected. This leaves the radios on, but doesn't allow connections for Personal Hotspot. (This is explained further in **Airplane Mode**.)

Control Center is now a great way to see what's going on with Personal Hotspot at a glance. Open Control Center and hold down on the networking area to reveal an expanded network view that includes AirDrop and Personal Hotspot in addition to Airplane Mode, Cellular Data, Wi-Fi, and Bluetooth (**Figure 9**). Every mode has text beneath that shows that method or feature's status.

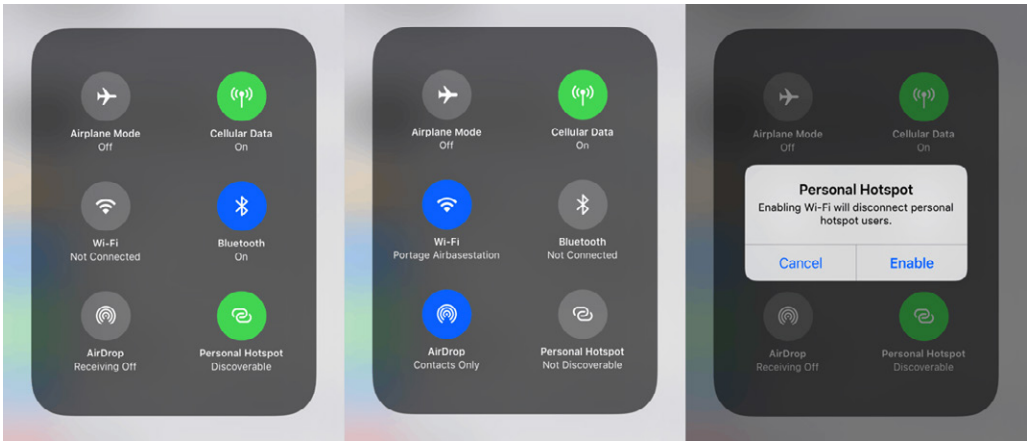


Figure 9: *From left to right: hotspot on and Wi-Fi unavailable; Bluetooth and hotspot on standby; and trying to re-enable Wi-Fi with the hotspot running.*

When you enable Personal Hotspot, it sets Wi-Fi to its Not Connected mode, because the hotspot has taken over all Wi-Fi connections: this helps you visualize that you're no longer getting an Internet connection via Wi-Fi. Disabling Cellular Data turns off Personal Hotspot, which shows Off beneath its icon. You'll note also that AirDrop changes to

Receiving Off whenever you're using Personal Hotspot—iOS can't handle incoming AirDrop files while managing connected devices.

> **Note:** In iOS 10 and earlier releases, Apple would warn you about the combination of radio choices you made when Personal Hotspot was either enabled or you turned it on. Apple initially removed those in iOS 11.0, relying on the expanded network view labels. However, in 11.2, it added popup explanations back into the mix.

Connect to Personal Hotspot

With Personal Hotspot on, you have three choices for how to connect:

- **Wi-Fi:** Any Wi-Fi–equipped device can connect just as if the iOS device were a wireless router. The limit of devices varies by carriers from three to five and isn't published anywhere.
- **USB:** Plugging your computer into your iPhone or iPad gives you a high-speed data connection that you know works as long as the cable isn't bad. The downside? Being literally tethered.
- **Bluetooth:** This method requires more steps to make a connection initially, but it gives you cable-free flexibility. Most Bluetooth-equipped devices can connect through this method, including iPhones, iPod touches, and iPads. No more than three devices may connect via Bluetooth at the same time.

> ***Pick Wi-Fi or Bluetooth?*** *Wi-Fi can consume more battery power than Bluetooth, so you might opt for Bluetooth tethering, but Bluetooth tops out—even in the latest 5.0 spec—at 3 Mbps of raw throughput or about 2.1 Mbps of actual throughput. That's as little as 1/10th of LTE speeds.*

Regardless of your carrier, you can't connect more than five devices across all these methods. Additional connections will be refused.

Once you make a connection, a blue pulsing banner appears across the top of the iPhone or iPad's screen (**Figure 10**). (The iPhone X minimizes this display to the upper-left notch.) The banner shows the number of devices connected, too. If the device is on standby, a smaller status banner appears on the Lock screen when you wake it (**Figure 11**).

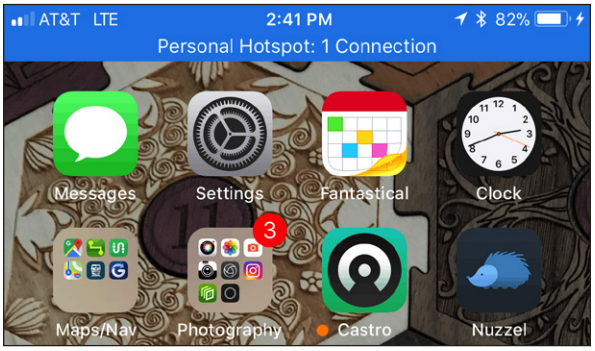


Figure 10: *A banner lets you know whenever your device is acting as a cellular modem for a computer via USB, Wi-Fi, or Bluetooth.*

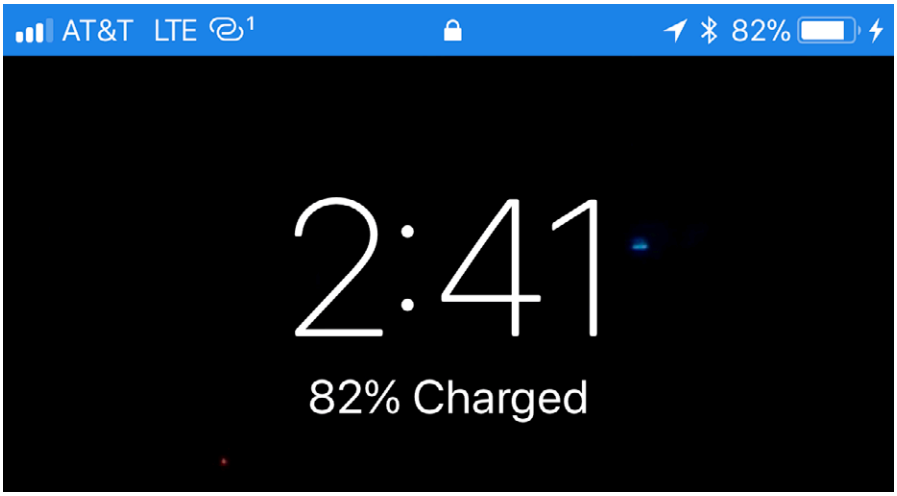


Figure 11: *The Lock screen shows whether the hotspot is active and connected devices.*

> **Note:** Windows computers, Android phones, and other devices can also connect via Wi-Fi; many devices can also connect via Bluetooth; and Windows at least can also tether via USB. The process is identical on those platforms to hooking into a Wi-Fi, Bluetooth, or USB shared network.

Access via Wi-Fi

Using Wi-Fi to connect to a Personal Hotspot is the easiest case because no special setup is required. You use whatever method you normally

employ to connect to a Wi-Fi network from the device, and I provide directions for several common operating systems just ahead. The name of your iOS device is the name of the Personal Hotspot network.

Connect via Wi-Fi in macOS

In macOS, you can use the Wi-Fi menu on the menu bar to select the Personal Hotspot network by name:

1. Click the Wi-Fi menu to see a list of available networks.
2. Choose the network's name.
   - For an iOS 8.1 or later Personal Hotspot and Yosemite, it appears as it does in Instant Hotspot: an item with the cellular connection type, battery level, and signal strength (**Figure 12**). (If Personal Hotspot is not active on the device, selecting the hotspot in the macOS menu turns it on.)

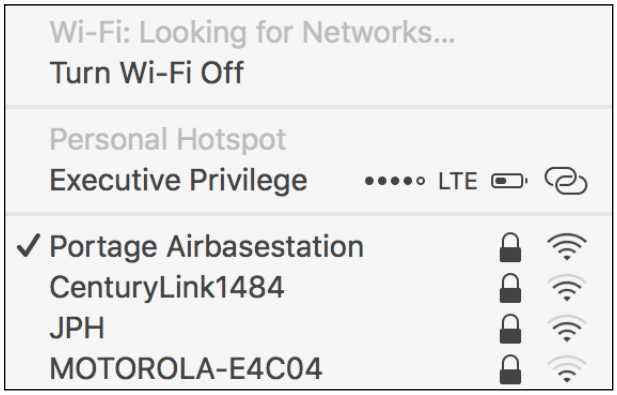


Figure 12: *Select the hotspot under Personal Hotspot.*

   - For an iOS 8.0 or earlier, or with earlier versions of OS X than Yosemite, Personal Hotspot shows up in the main list of networks with a linked-chain icon just to the left of the signal strength icon (**Figure 13**).
3. Enter the password, and click Join (**Figure 14**).

> ***Future connections:*** *If you leave Remember This Network checked, you won't be prompted in the future for the password. The flip side of that benefit is that it's difficult to prevent future automatic connections when the personal hotspot's Wi-Fi connection is active.*

Figure 13: *In iOS 8.0 and earlier, the Personal Hotspot's network name appears in the Wi-Fi menu's networks list.*

Figure 14: *Enter the network's password to connect.*

You're now connected. Your Mac will stay connected as long as the Personal Hotspot feature is active. The next time you turn on the Personal Hotspot, your Mac will reconnect if you stored the password and if your Mac isn't already associated with a Wi-Fi network.

Disconnect from Personal Hotspot Wi-Fi

To stop using the Personal Hotspot, hold down the Option key and then select the Wi-Fi menu. Now select Disconnect From Network Name and your link is severed.

Don't auto-join in the future

If you want to prevent the Mac from connecting automatically in the future, follow these steps:

1. Launch System Preferences and select the Network pane.
2. Select Wi-Fi in the list at left.
3. Click the Advanced button.
4. From the Wi-Fi pane, select the Personal Hotspot network, then click the minus button to delete it.
5. Click OK and then click Apply.

Connect via iOS

In iOS, use the Settings app to connect to the Personal Hotspot network.

From and to an iOS 8.1 or later device

1. Select Settings > Wi-Fi.
2. Choose the network from the Personal Hotspots list (**Figure 15**).
3. Enter the password when prompted.

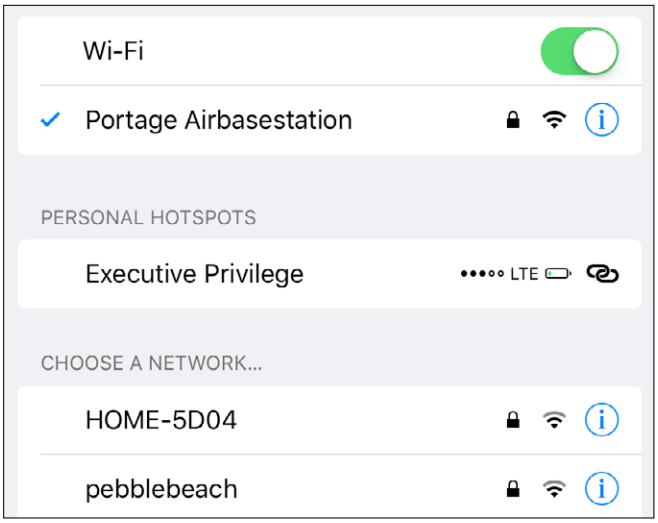


Figure 15: *Look in the Personal Hotspots section (above) or for the chain icon.*

You are now connected. The chain icon appears at the left of the iOS status bar instead of the normal Wi-Fi icon.

Disconnect by opening Control Center and then simply tapping the blue Wi-Fi icon. (Tapping it again will reconnect unless you use Settings > Wi-Fi to pick a different network.)

To or from an iOS 8.0 or earlier device

1. Select Settings > Wi-Fi.
2. Choose the network from the list. Personal Hotspot networks are shown with a special chain icon in iOS 4.3 and later.
3. Enter the password when prompted.

You are now connected. The chain icon appears at the left of the iOS status bar instead of the normal Wi-Fi icon.

Automatic reconnection

As long as the password is stored for the iOS network and isn't changed, your iOS device will reconnect automatically whenever it's in range and the Personal Hotspot Wi-Fi connection is active. To stop using the mobile hotspot right away, choose another network from the list or turn off the Wi-Fi adapter.

If you want to prevent connecting automatically in the future, while the hotspot connection is active, tap the blue info ⓘ button next to the network name and then tap Forget This Network. This removes the network's stored setting and disconnects the device from the Personal Hotspot immediately.

Disable Wi-Fi sharing in iOS

To turn off the hotspot on the device that is sharing its connection, just tap Settings > Personal Hotspot and then turn off the Personal Hotspot switch; or, open Control Center and hold down on the networking area, and then tap the Personal Hotspot icon. Or, you can tap Settings > Wi-Fi and turn off Wi-Fi entirely.

You can also block all existing connections from client devices that aren't using iCloud Keychain by changing the Wi-Fi password on the Personal Hotspot screen. This will also prevent devices with a stored password from reconnecting automatically or manually until you provide the changed password. (With iCloud Keychain, the correct password is syn-

chronized among all connected devices, so the moment you reconnect successfully, so will all other devices once they sync.)

Tether with USB in macOS

Connect your iOS device to your computer using a USB cable. The first time you enable Personal Hotspot and plug the device into a Mac via USB, macOS alerts you that the interface is added and the Mac's Network system preference pane adds an adapter entry (**Figure 16**).

Figure 16: *An entry appears in the adapters list.*

MacOS automatically activates tethering and turns that red dot green.

> ***Not active?*** *If you're not seeing this, you may need to launch iTunes the first time you tether. iTunes doesn't seem to have anything to do with USB tethering except initial activation.*

To halt the active USB tethering connection, disconnect the USB cable. Alternatively, you can disable the iOS adapter profile. In the Network system preference pane in macOS, select the iPhone USB or iPad USB adapter, and then from the gear ⚙ pop-up menu, choose Make Service Inactive. Click Apply in the lower-right corner.

Connect with Bluetooth

On your hotspot device, make sure Bluetooth is turned on: swipe to show Control Center and check that the Bluetooth icon is active. If it's not, tap it. (You can also manage Bluetooth from the Settings app.)

Once you're sure it's enabled, you can make a Bluetooth connection from macOS or iOS, as I describe next.

Bluetooth uses less power than Wi-Fi, almost nothing in standby mode, so a Bluetooth connection could allow both an iOS device and a paired piece of hardware to work longer without AC power.

Note: I cover Bluetooth in more detail in **Set Up Bluetooth** if you'd like to learn more.

Bluetooth tethering with macOS

Follow these steps to set up a Bluetooth connection between your hotspot device and a Mac running Yosemite or later (instructions are substantially different in earlier versions of macOS):

1. Launch System Preferences, and select the Bluetooth pane.
2. Your iPhone or iPad should appear in the list of devices (**Figure 17**). Click Pair. (If it doesn't appear, check that Bluetooth is enabled on the iOS device and that it's within a few dozen feet of your computer.)

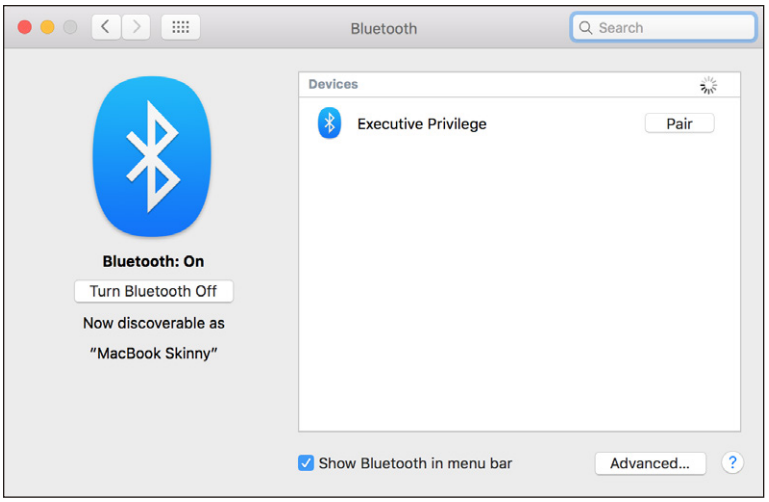


Figure 17: *Initiate pairing from macOS.*

3. A pop-up dialog appears with a 6-digit code. On the iOS device, a similar confirmation dialog pops up (**Figure 18**).
4. Confirm that the code is identical, which prevents a so-called man-in-the-middle attack with someone nearby trying to intercept the connection. (That's very unlikely, but it could happen.) The additional cue is the name of the device. Click Pair on the hotspot device. On the Mac, your iOS device should now appear in the list (**Figure 19**).
5. Now, in System Preferences, click Show All, then select Network.

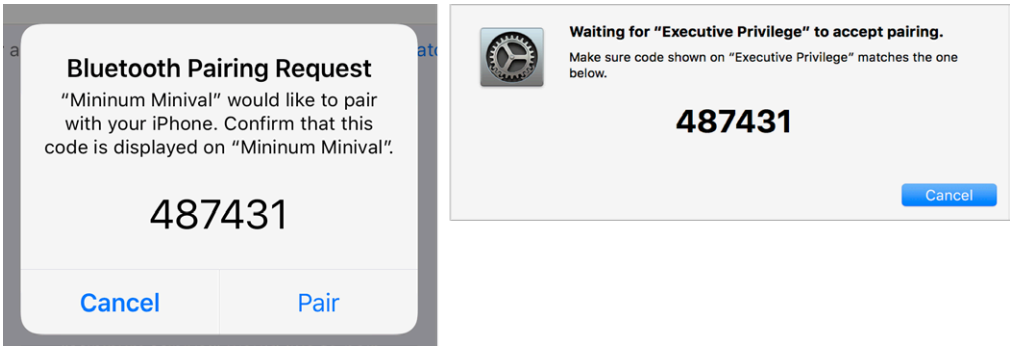


Figure 18: *The Mac and iOS device both display the same code.*

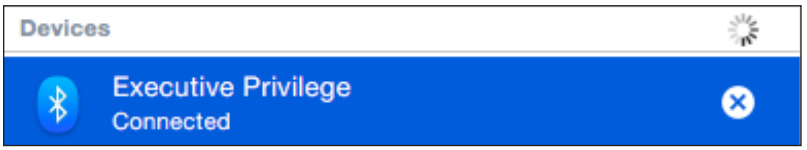


Figure 19: *The device is paired in macOS and connected.*

6. In the adapters list at left, you'll notice a new Bluetooth PAN entry; *PAN* stands for Personal Area Network, and it's the kind of network that Bluetooth creates. Your device should be selected in the Device pop-up menu (**Figure 20**). Click Connect.

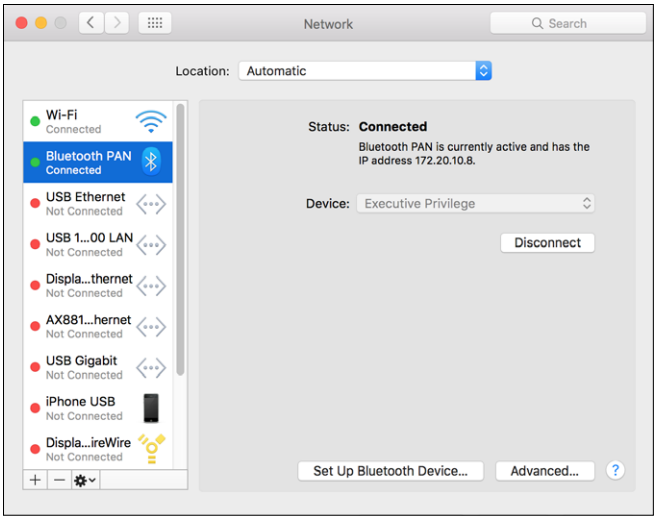


Figure 20: *The Network preference pane lets you manage the connection over USB.*

7. On the Mac, you'll see the Status label set to Connected (Figure 20), and if the Bluetooth system menu icon is showing, it will have dots bisecting it. On your hotspot device, the Internet tethering banner will appear.

   To disconnect Bluetooth tethering, you can do any of the following:

- In the Network preference pane, with Bluetooth PAN selected in the adapters list, click the Disconnect button.
- On your iOS hotspot, in Settings > Personal Hotspot, tap the Personal Hotspot switch to Off.
- In iOS, open Control Center, hold down on the network area, and then tap the Personal Hotspot icon.
- Turn off Bluetooth networking. In iOS, tap Settings > Bluetooth; on the Mac, look in the Bluetooth system preference pane or the Bluetooth menu on the menu bar.

Bluetooth tethering with iOS

Although all iOS devices have Wi-Fi built in, Bluetooth consumes less battery power and may be a more appropriate choice. You can set up a Bluetooth connection between any iOS device running iOS 4.3 or later and a hotspot device quite simply:

1. View Settings > Bluetooth.
2. If Bluetooth is off, tap the switch to turn it on.
3. Tap the Personal Hotspot in the list of Devices (**Figure 21**).

   Both devices show confirmation dialogs (**Figure 22**).

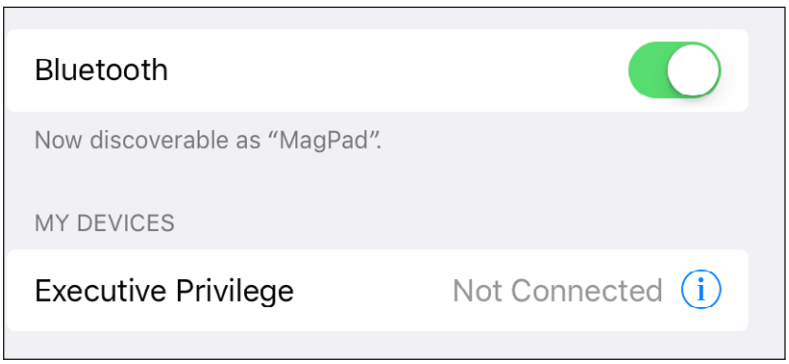


Figure 21: *The hotspot appears in the My Devices list; here, it's "Executive Privilege."*

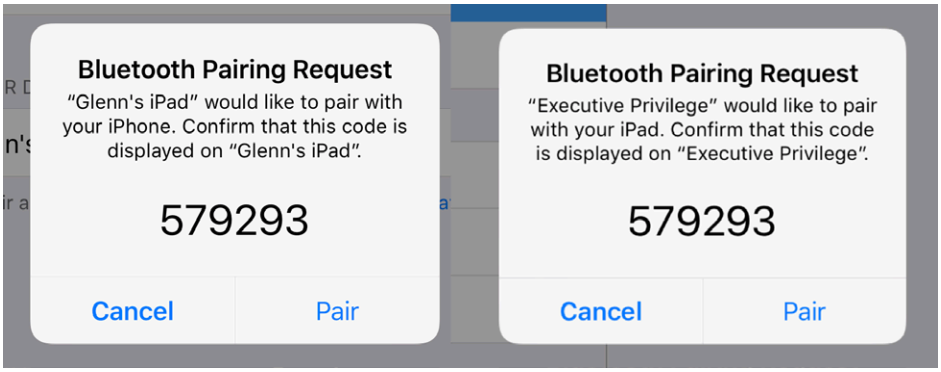


Figure 22: *Tap Pair on both devices to proceed.*

4. If the codes match, tap Pair on both devices.

   The iOS device is now connected over Bluetooth, and a chain icon appears at the left of the status bar instead of the normal Wi-Fi icon.

   To disconnect from the Personal Hotspot, do either of the following:

- **On the connected device:** Slide Bluetooth's switch to Off.
- **On the iOS hotspot:** Turn off or disconnect Personal Hotspot or Bluetooth.

  To reconnect, open Settings > Bluetooth and then tap the name of the Personal Hotspot in the Devices list.

  You might want to discard a stored Bluetooth pairing from the Devices list if, for instance, you're using a friend's device or you don't want someone else using your iOS device with the paired connection. To remove the pairing, tap the info ⓘ button next to the device name and then tap Forget This Device.

Use Bluetooth Tethering from iOS to a Laptop

A side benefit of the capability to tether over Bluetooth is that you can also use your iOS devices to grab Internet access from a laptop. For instance, if you're in a hotel or other location in which you have to pay for each device you connect to a Wi-Fi network, you were previously out of luck in relaying an Internet connection from a laptop to an iPhone, iPod touch, or iPad. Now you can.

Under macOS, use the Sharing system preference pane's Internet Sharing option to share the Wi-Fi connection via Bluetooth PAN. Choose Wi-Fi from the Share Your Connection From pop-up menu, and check the Bluetooth PAN box in the To Computers Using list (**Figure 23**). Then check the box next to Internet Sharing in the Service list at left.

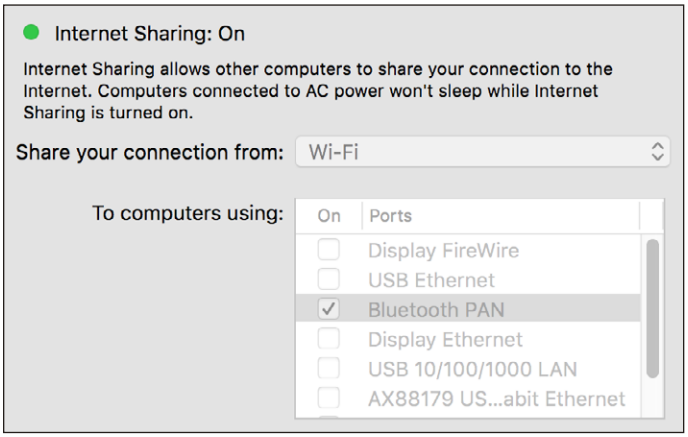


Figure 23: *Via the Bluetooth PAN connection, you can share your Wi-Fi connection with iOS devices.*

If you don't see Bluetooth PAN in the To Computers Using list, open the Network preference pane. Click the plus button at the bottom of the adapters list, and choose Bluetooth PAN from the Interface pop-up menu. Click Create, then click Apply. When you return to the Internet Sharing option in the Sharing preference pane, the Bluetooth PAN will be there.

Choose to Use Cellular Data or Wi-Fi

There are plenty of good reasons to pay attention to whether a cellular iOS device 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. With iOS 10 and later, you can 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 (**Table 1**). The range of bandwidth is huge (such as 30 to 300 Mbps as the top rate), because iOS 11 supports generations of cellular networks and Wi-Fi base stations. And each iOS device supports many rates for each standard while also offering backward-compatible support for older networks.

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 doesn'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.

Table 1: *Deciphering Indicator Icons*

Indicator	Explanation	Bandwidth
No service	Can't connect to any network. You may also see five underscores.	None.
	Connected to a Wi-Fi network. The number of white waves, from one (shown as a dot) to three, indicates signal strength from weakest to strongest.	Rates as high as 30–300 Mbps, but limited by the broadband service to which a Wi-Fi router connects.
Wi-Fi	Wi-Fi Calling is enabled, but this doesn't affect cellular data usage.	N/A
LTE	Connected via LTE.	From 5–100 Mbps downstream, 2–25 Mbps upstream.
4G	Connected via 4G (GSM only).	Downstream up to 6 Mbps and upstream up to 1.9 Mbps.
3G	Connected via 3G.	GSM: Down 1.7–4 Mbps; up 384 Kbps–1.9 Mbps. CDMA: Down, 600 Kbps–1.4 Mbps; up, 500–800 Kbps.
E	Connected via EDGE, a 2.5G standard (GSM only).	Roughly 200 Kbps downstream (all GSM iOS devices); 40–50 Kbps upstream
GPRS	Connected via 2G using either GPRS (GSM) or 1xRTT (CDMA).	Roughly 40–50 Kbps.
	Connected via tethering; see **Make a Mobile Hotspot**.	

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 set Cellular Data to Off.

> **Note:** In the case of an iPad, turning off cellular data disables all mobile network access; for an iPhone, voice calling, voicemail, and messaging remain available.

> **Note:** In previous versions of iOS, Apple made it seem as though you were connected via Wi-Fi to a regular hotspot network even though Personal Hotspot was in use. In iOS 11, Wi-Fi appears to be off when the hotspot features has taken over its use, reducing confusion.

If a Wi-Fi network is acting flaky, you can avoid the problem in one of three ways:

- Use Wi-Fi Assist, introduced in iOS 9 (**Figure 24**). This option, set in Settings > Cellular (iPhone) or Cellular Data (iPad)—swipe way way way down to the bottom—taps into mobile broadband when Wi-Fi connectivity is too poor to use. Apple says it won't download attachments, use background downloading, or let third-party apps stream audio or video so as not to burn through all of your cellular data plan.

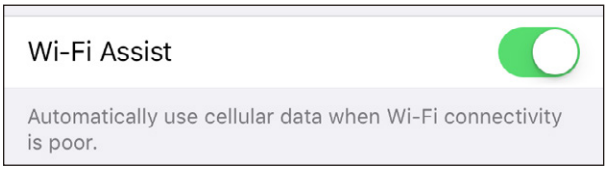


Figure 24: *Wi-Fi Assist swaps to cellular as needed.*

> ***WARNING!*** *Some people have had problems with Wi-Fi Assist, where they believe (based on their bills) that it consumes cellular data for kinds of activities Apple says the feature shouldn't, and even when the user believes their iPhone is continuously connected to Wi-Fi. This makes me suggest that you disable it—it's turned on by default!—unless you have a particular situation in which you feel it's worthwhile. The Wi-Fi Assist switch shows total bytes used by it since the last time it was activated or stats were reset.*

- Switch off Wi-Fi, and force the use of cellular data.
- Use the method noted in **Forget This Network** to disconnect the Wi-Fi network. Wi-Fi is still enabled, but not used when it has no network connection.

Manage Cell Data Usage

When Apple introduced the iPhone, it also managed to first get AT&T and then other carriers to offer unlimited data plans in the United States and in a few other countries. That didn't last, as networks became congested with heavy data use and carriers started to offer limited plans and charge overage fees for usage above a monthly limit.

But the pendulum swings both ways. Starting in mid-2016, U.S. carriers ununder heavy competition started to offer phone and tablet plans with unlimited data usage—with provisos that made unlimited have some limits.

Carriers Shift to Throttling

By mid-2016, all four major U.S. cellular carriers shifted phone, tablet, smartwatch, and other plans to remove overage fees and offer unlimited data by allowing LTE speeds up to either a firm set amount for some plans or squishier ones for others. After that point, data throttling kicks in, reducing data rates.

Limited-use plans from AT&T, for instance, pool 1 GB, 3 GB, and so forth each month. 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.

Here are the details of major plans in October 2017, *certain* to change. (These plans also bundle a lot of other features depending on tier and carrier, including things like LTE data use in Mexico and Canada, worldwide unlimited calling, and free Gogo service on airplanes.)

- **AT&T:** Mobile Share Advantage plans have several tiers for pooled monthly data use, and throttle to 128 Kbps when the pool empties. Unused data rolls over to the next month. The plans include tethering. AT&T also has unlimited plans with 22 GB a month before congestion throttling may kick in. Unlimited plans come in two varieties: one has no hotspot use and the other allows 10 GB before 128 Kbps throttling.
- **Sprint:** Unlimited Freedom includes 23 GB of usage before congestion throttling plus 10 GB of tethering before dropping to 128 Kbps.
- **T-Mobile:** T-Mobile has a single plan with add-ons. The basic plan allows up to 32 GB of LTE data before congestion throttling comes into play. Tethering is limited to 3G. The lower-tier add-on includes 10 GB of tethering at LTE before dropping to 3G. The higher-tier add-on features unlimited LTE subject to the same monthly 32 GB total.
- **Verizon:** In a lower-tier plan, Verizon offers unlimited LTE data, but could throttle for congestion at any time, and tethering can't go faster than 600 Kbps. On a higher-tier plan, throttling only comes into play after 22 GB of use for each line, and tethering is at LTE rates for 15 GB of data, after which it drops to 600 Kbps.

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.

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 25**). In practice, it's pretty close.

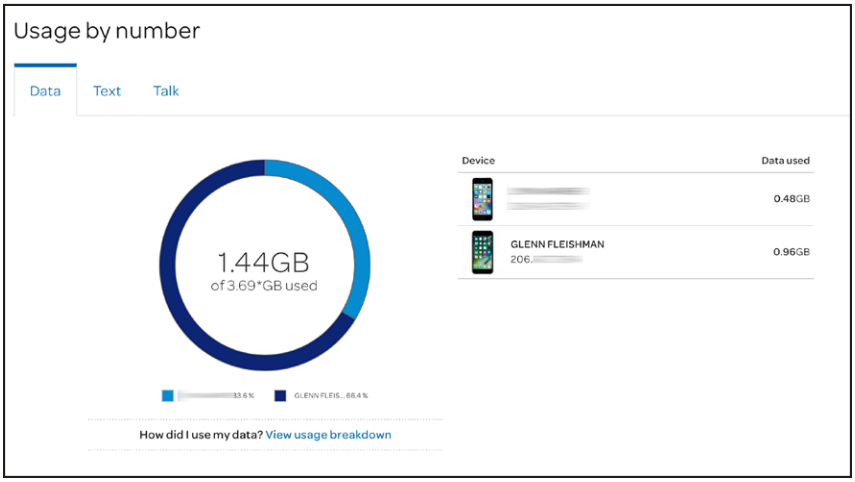


Figure 25: *AT&T's online data statement is the only one you can rely on for billing.*

- It isn't aligned with your billing period. Rather, it's a total of all data consumed since the last time you tapped Reset Statistics at the very bottom of the Cellular or Cellular Data view.

You can, of course, visit your carrier's web site and get usage information that's typically accurate to within 24 hours, sometimes much less.

If you'd like this number to be more useful, set yourself a reminder in your calendar for the first of each month (or the start of your billing period if it's another increment) to visit Settings > Cellular and tap Reset Statistics (**Figure 26**).

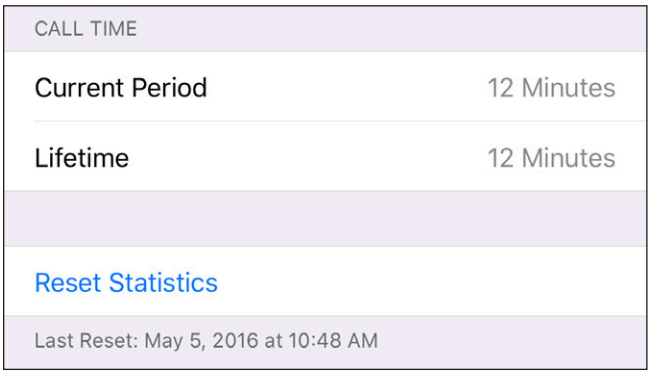


Figure 26: *Tap Reset Statistics to zero out your current cellular data numbers.*

You can find out how much data you've used just via Personal Hotspot in the Cellular/Cellular Data view. Tap System Services at the bottom, and all iOS uses, including Personal Hotspot, are displayed (**Figure 27**).

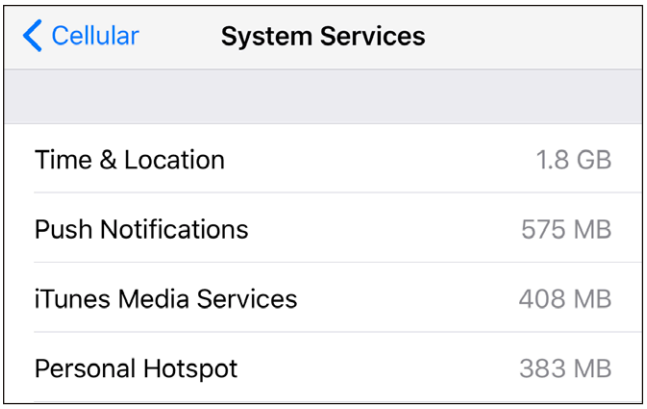


Figure 27: *You can discover Personal Hotspot's portion of overall cellular data.*

Check Cellular Usage on an iPad

A Wi-Fi + Cellular iPad has an additional way to track usage via the Settings > Cellular Data > View Account screen, which shows details from the carrier, including the billing period, how much data is included, and the data consumed so far in that period.

Turn Cellular Data On Only When You Need It

There are times when you'd prefer not to have an active cellular connection or cellular data link on an iPhone or cellular iPad, notably when you're close to the throttle limit of your service plan or traveling outside an area included in your data plan. You can change how the cellular radio interacts with a network in two ways:

- To turn off data only, in Settings > Cellular Data (iPad) or Settings > Cellular (iPhone), set the Cellular Data switch to Off (**Figure 28**). You can also tap the Cellular Data icon in Control Center. This disables the data link only. With an iPhone, you can still place and receive voice calls and send and receive SMS/MMS text messages.

Figure 28: *The Cellular Data switch lets you turn all mobile broadband access on or off.*

- To shut off the entire cellular connection, set Airplane Mode to On in the upper left of the main Settings screen, or tap the Airplane Mode button in Control Center. Airplane Mode turns off Bluetooth, Wi-Fi, and cellular radios, although you can re-enable Bluetooth and Wi-Fi separately. See **Airplane Mode** for details. It also dramatically extends your battery life in most cases.

  You can also control other cellular data parameters:

- Setting Cellular Data Options > Enable LTE to Off will eliminate use of LTE networks and rely on slower 2G, 3G, and non-LTE 4G networks (**Figure 29**). This is useful when LTE networks near you are spotty and you're having trouble staying connected as your device swaps back and forth between 2G/3G and 4G LTE. This may also reduce battery use.
- In some markets, the Enable LTE option may read Voice & Data, and let you pick 2G, 3G, or LTE as network options.

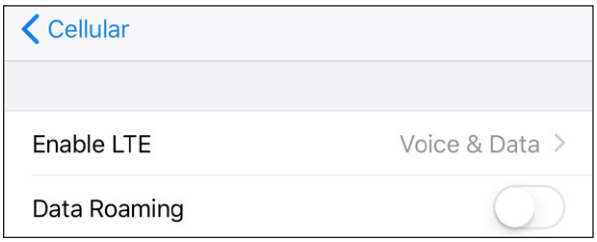


Figure 29: *Disabling LTE helps if nearby LTE networks are erratic. Data Roaming affects use outside your home service area.*

- Data Roaming can ensure that you don't consume expensive mobile bytes while you're outside the home area for your carrier. In some cases, you might have limits; in others, you might be charged.

Limit Your Activities on the Cell Network

Unless you are connected with Wi-Fi, limit your Internet-related activities to those that don't use much data, such as checking email or viewing web pages.

Various items in Settings let you limit whether cellular data can be used for an app or activity, including:

- Use the options in Cellular Data (iPad) or Cellular (iPhone) to prevent excessive use of certain services from consuming a lot of your data allocation. You can turn on and off specific apps, and see their data consumption (see **Figure 30**).

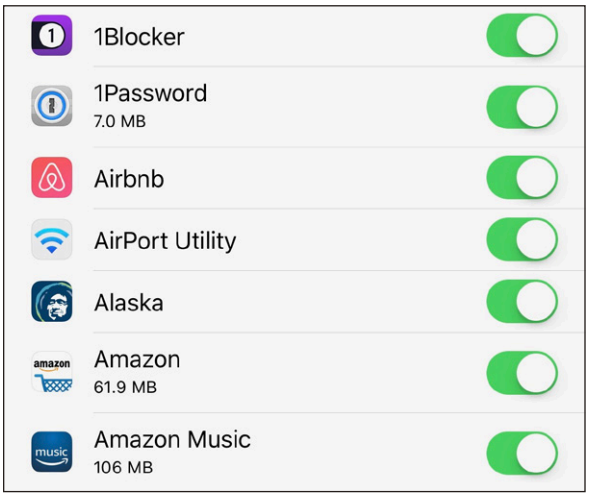


Figure 30: *Opt out of using cellular data for certain iPhone apps.*

- In the Safari settings, you can disable syncing the reading list, which is relatively low bandwidth depending on how you use it.
- In iCloud > iCloud Drive, swipe to the bottom and you can disable syncing all items in the list over cellular.
- In the iTunes & App Stores, you can choose whether or not to use cellular data for automatic downloads (four different options for things you've purchased and updates).
- In Music, turn off the Use Cellular Data option for playback and downloads of the Apple Music or iTunes Match service, if you subscribe to either one.

- Cache data you need. Plan ahead and download for offline use from cloud or other services. For instance:
  - Use Google Maps offline. While it doesn't burn up lots of data while online, its offline mode lets you consult interactive maps when there's no network connection or when you're roaming on an international network. Enter a place name, tap the name at the bottom, then tap the three stacked dots at upper right. Next, tap Save Offline Map.
  - Use the Music or Videos apps, find items you want, and tap the cloud icon to download them locally. (This is a good time to consider iTunes USB or Wi-Fi syncing for larger files.)
  - Amazon Prime users can download certain movies and TV shows via the Amazon Instant Video app for offline playback.
- You can also enable or disable kinds of cellular use via settings within certain apps even when you've allowed the app to use cellular bandwidth. For instance, the podcast app Castro has a cellular data switch in its Downloads area to let you opt to download episodes over either Wi-Fi and cellular or Wi-Fi only (**Figure 31**). But even with that switch set, you can still stream episodes over a mobile network (and Castro warns you that you're streaming).

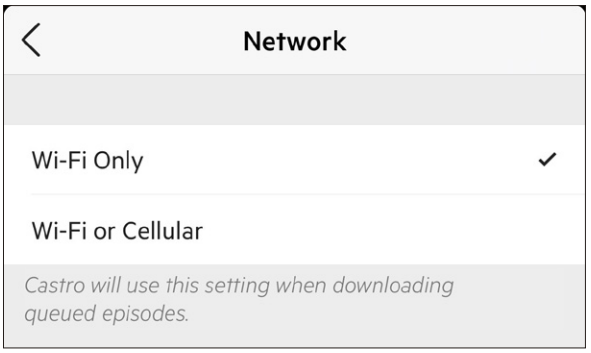


Figure 31: *Castro lets you choose to limit downloads to Wi-Fi.*

Note: The Maps app used to consume lots of data because Apple loaded image data from Google to power its software. Now both Apple's Maps and Google Maps rely on vector-oriented data—when you're not looking at satellite views—and, in my tracking, download vastly less information.

More generally, you should avoid using or disable the cellular use in Settings for:

- Audio-streaming apps, such as those used by radio stations and networks. Usage is generally small, but it can add up.
- Video-streaming apps like Hulu Plus, YouTube, Netflix, and Vimeo. It's easy to run through a gigabyte or more in an hour, depending on your device and connection.
- Photo-browsing apps like Flickr. Depending on the app, even swiping past a photo might download a megabyte or more.

Note: Depending on your carrier and other parameters, you should receive push notifications, text messages, or both as you approach or exceed whatever the included monthly cellular usage total is before throttling.

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 "**You Can't Always 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.

Note: Wi-Fi Calling may not work in iOS 11 with every carrier on an iPhone 5s, the oldest phone that can handle this latest operating system update.

Enable Wi-Fi Calling on Your Main Device

You start in Settings > Phone > Wi-Fi Calling (**Figure 32**). Once you tap the switch, you're prompted to enable Wi-Fi Calling.

Figure 32: *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 have to proceed through a set of steps to opt in that warn you about emergency calls placed when Wi-Fi Calling is enabled, and have you fill out the address at which you typically use the phone with Wi-Fi Calling (**Figure 33**).

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 fill-out form.

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.

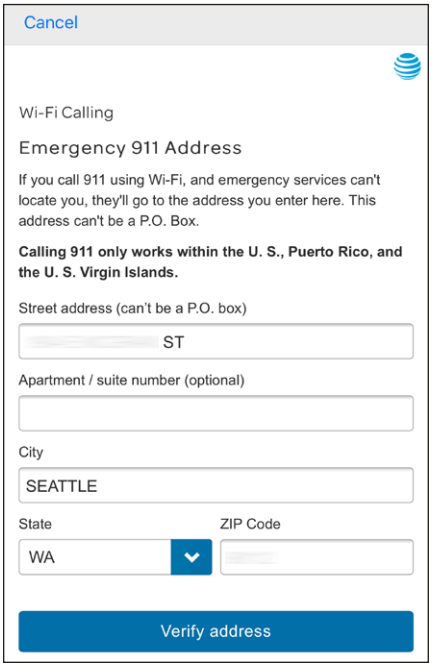


Figure 33: *Your address entered for Wi-Fi Calling becomes the default used if no better location can be derived from your phone.*

When you've entered your address and tapped Verify Address, the carrier checks to make sure the information you entered matches a legitimate address. If not, you're prompted to correct it; otherwise accept it. You're told that Wi-Fi Calling will be available in a few minutes; tap OK. Whenever it's active, the word "Wi-Fi" appears following the carrier's name in the status bar.

Once Wi-Fi Calling is active, you can enable and disable it at will by tapping its switch (**Figure 34**). This may be necessary if you wind up on a Wi-Fi network with inconsistent quality.

Enable Wi-Fi Calling on Other Devices

Apple's Continuity feature, introduced a few OS releases ago, allows you to make cellular calls from iPads, iPod touches, and macOS devices on the same Wi-Fi network as your iPhone. Wi-Fi Calling extends that, letting you call even when your iPhone isn't nearby! (However, you can't use other iPhones!)

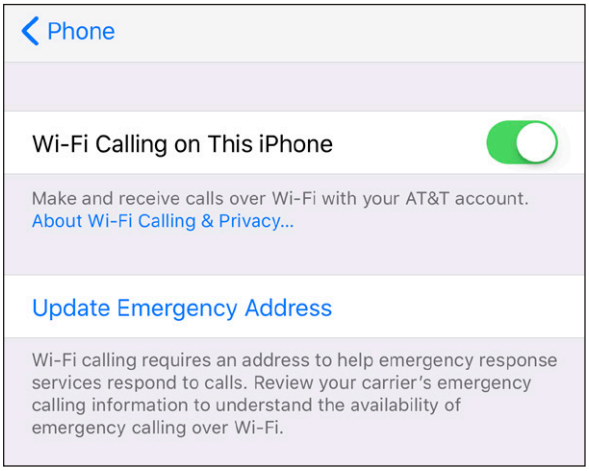


Figure 34: *Once Wi-Fi Calling is enabled, you can disable it with a tap or update the stored emergency address.*

Which devices work with Wi-Fi Calling. *An iPad or iPod touch has to be running iOS 9 or later; an Apple Watch needs watchOS 2 or later; and a Mac has to have El Capitan or later installed, and be a model released in 2012 or later, except the 2012 Mac Pro.*

In Settings > Phone > Calls on Other Devices, tap Allow Calls on Other Devices (**Figure 35**). You may already have this enabled if you were previously using Continuity for cell calls.

Figure 35: *You can share Wi-Fi Calling among all your iCloud-linked devices.*

Note: Not all carriers offer what Apple clunkily describers as "Wi-Fi Calling on supported iCloud-connected devices." It's offered by the big four U.S. carriers, however.

Now tap Add Wi-Fi Calling for Other Devices. It may take a moment for this to become active. On each iOS device and macOS computer logged into the same, you can now use Wi-Fi Calling. You may get alerted on every device with a warning asking if you want to upgrade to Wi-Fi calls on the device you're on. You can click Turn On or Not Now.

If you don't see that dialog, or you click Not Now, you can upgrade at will. In iOS, go to Settings > Phone > Calls from iPhone, and tap Upgrade to Wi-Fi Calling. In macOS, launch FaceTime, and then select FaceTime > Preferences > Settings, check Calls From iPhone, and click Upgrade to Wi-Fi Calling. You'll be asked to confirm on both platforms.

On devices on which you've never previously used Wi-Fi Calling, you should see a six-digit code appear, which you then enter in a dialog that likewise shows up on your iPhone (**Figure 36**). Tap Allow, and Wi-Fi Calling will now be available. You can update your emergency address on any linked device, or disable cellular-linked calls, too.

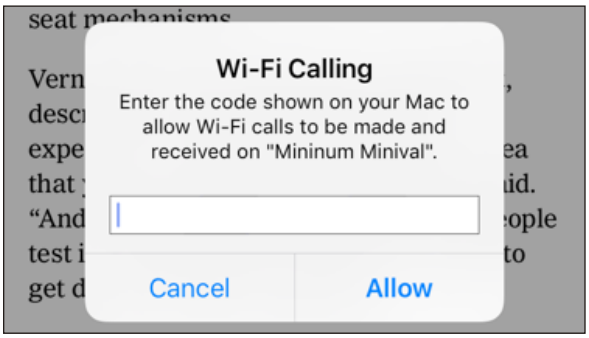


Figure 36: *The first time you use another device with Wi-Fi Calling, it shows a six-digit code that you have to enter on your iPhone to authorize it.*

You get one final warning, however: "Your location will now be used to make emergency calls." Click or tap OK.

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 in iOS, available to all iOS devices, 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.*

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

GPS works in Airplane Mode: *Starting in iOS 8.3, Airplane Mode stopped disabling the GPS radio, even though there was no reason to disable it before. The radio passively receives signals from satellites. You can use GPS positioning even with all other radios off with an offline mapping tool.*

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 Airplane Mode back to Off, all your previous settings for access are flipped back on.

Tip: Airplane Mode can also help avoid international charges, because when an iPhone has its radios off, it cannot receive calls. Also, you can neither inadvertently place a call nor use data.

To Sleep, Perchance To Transmit

When you push the Sleep/Wake button on the top or side of your iOS 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 and any iPhone can receive email and other updates via push over a cellular data connection.

iOS also maintains Wi-Fi connections on a minimal continuous level. Sleep is more like lightly daydreaming for an iOS device. That's a reason to use Airplane Mode: to prevent all of this from happening when you don't intend it to.

When Radios Turn Off and When They Don't

You can choose to separately turn off some radios in iOS:

- Wi-Fi: In Settings, tap Wi-Fi, and set Wi-Fi to Off.
- Bluetooth: In Settings, tap Bluetooth, and set Bluetooth to Off.
- GPS: Tap Settings > Privacy > Location Services, and set Location Services to Off.

> ***Is GPS really off?*** *GPS is a receive-only system; with Location Services off, ostensibly, the GPS receiver isn't powered up and attempting to find data.*

> ***WARNING!*** *Disabling Location Services prevents iOS from using GPS, Wi-Fi, and cell-tower based information to provide location data to iOS.*

There is no way to entirely disable the cellular radio separate from Airplane Mode. You can opt to disable various cellular modes, as discussed in **Manage Cell Data Usage**.

Starting in iOS 11, the buttons in Control Center for Wi-Fi and Bluetooth no longer act like the switch in Settings for each radio. Tapping those buttons puts the radios in a kind of standby mode. When you hold down on the networking area, it expands to show six networking features or radios with text labels beneath. Tapping Wi-Fi or Bluetooth toggles them between a blue active state and a white Not Connected state.

Apple made this change so iOS could continue to work with a number of Apple-specific features like AirDrop, Handoff, and Location Services, and keep connected to hardware like the Apple Watch and the Apple Pencil.

Wi-Fi re-enables if you tap its button, connect to a network via Settings, or walk or drive to a new location. Bluetooth re-enables if you tap its button or connect to a peripheral. Both leave standby mode when you restart your device and at 5 a.m. local time.

Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, earpieces, headsets, and keyboards to an iOS device 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 iOS device 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 iOS 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.

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 iOS 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 and macOS to enable signaling between devices for AirDrop (see **Exchange 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 iOS device in the Bluetooth view, the other device appears, naturally enough, in the Other Devices list (**Figure 37**).
3. Tap the desired device. iOS attempts to connect.
4. Depending on the device, iOS will do one of the following:

- Simply proceed: iOS pairs without requiring a code or confirmation. You'll see this with simple devices.

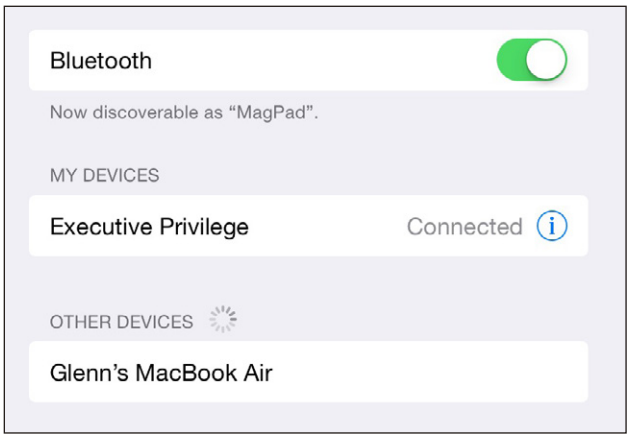


Figure 37: *An unpaired device (my MacBook Air) is discovered.*

- Show a Pair button: In some cases, you don't need to type a pairing code, but you get a dialog like the one in **Figure 38** on each device. Compare the code, and tap Pair on each to confirm.

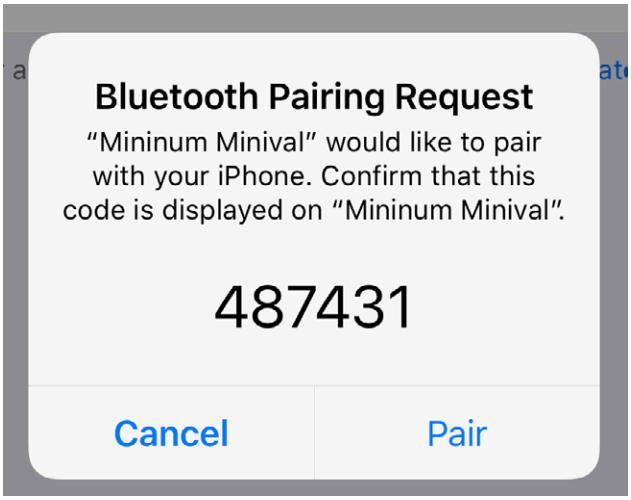


Figure 38: *iOS devices and Macs just ask you to confirm.*

- Show a field in which you enter a code: The code will either be provided by the other device or—in the case of a peripheral without a way to choose or display characters—noted in its manual. It's typically `0000`.

- Display a code that you enter on the other device: Your iOS device generates a PIN (called a "passkey" here) to be entered in the pairing device.

The paired device is now shown as Connected in the list.

> ***Prevent accidental pairing and attacks:*** *You're asked to confirm a code to ensure that it's the right device and that nobody else is trying to control the two devices trying to pair. The cryptography behind this would prevent both devices from seeing the same code if someone had managed to interpose themselves into the pairing. Sometimes you'll see a different code if someone else nearby happened to be trying to pair a Bluetooth device at the same time, however!*

iOS shows a Connected label for paired devices that are turned on and available, and Not Connected for those that aren't in range or are turned off (**Figure 39**).

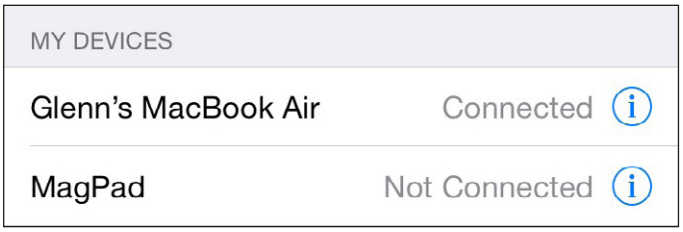


Figure 39: *The MacBook Air is paired and connected; the iPad is paired but not connected.*

Disconnect hardware from Bluetooth by tapping the info ⓘ button and tapping Disconnect.

> **Tip:** To remove a pairing, select the peripheral in the Devices list, tap the info ⓘ button, and then tap Forget This Device.

> ***WARNING!*** *If you walk away from a Bluetooth keyboard while it's still on, it can maintain a connection over a long distance. I was mystified as to why I couldn't get an on-screen keyboard to appear on my iPad when two rooms away from an Apple Wireless Keyboard until I recalled I hadn't turned it off.*

Hands-Free Profile

The Hands-Free Profile in Bluetooth lets you have audio conversations using the mic and headphones (or speakers) on a variety of devices, such as over-the-ear or in-ear headsets. You pair a device just as described in **Pairing Any Device**, earlier.

On an iPhone, you can answer incoming calls by tapping the answer button on the headset. When you place a call, the last chosen mic/headphone is used, but you can pick from the available options, even as the call is underway, by tapping the Audio button. In the example in **Figure 40**, I could choose among the headphones/headset combo I have from Sony, the iPhone's earpiece/mic, or the speakerphone option on the iPhone.

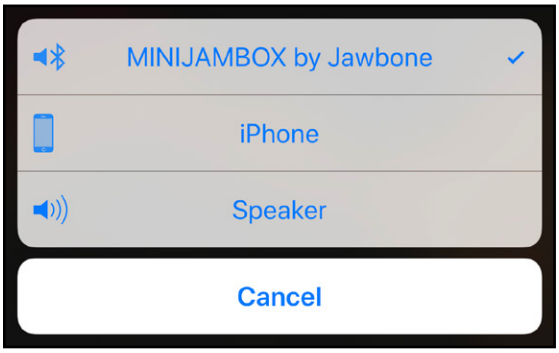


Figure 40: *When placing a call, you can choose a Bluetooth device.*

Picking an audio source also works to let you use a headset for other programs, such as Skype or FaceTime, that don't require a cellular network or an iPhone.

Audio Devices

Once you've paired stereo headphones, you can use them just as you would headphones plugged into any iOS device. You can tap the start, stop, and other controls in an app playing back audio, or, if your Bluetooth headphones or headset has these controls, you can handle those options remotely.

Apps that allow audio playback should show a special AirPlay icon when multiple audio output options are available. You can also swipe to reveal Control Center and change all iOS audio output to another audio device. (See **Stream Music and Video with AirPlay** for more about that technology.)

Tap the icon to pick an audio destination, which includes the device's built-in speakers), active Bluetooth headphones, and any Apple TVs or AirPlay speakers connected to your network (**Figure 41**).

Figure 41: *Tap the AirPlay button in the audio playback controls to choose among available audio output destinations.*

Only one output source may be selected from the list at a time. Tap a device to choose it. Audio continues to play throughout and seamlessly switches whenever you tap.

You can stop using Bluetooth headphones with one of three methods:

- Turn off the Bluetooth headphones using the power button.
- In Settings > Bluetooth, in the entry for the headphones, tap the info button, tap Forget This Device, and then tap OK.

- Move the iOS device and the Bluetooth headphones out of range of each other. I like this option least, because Bluetooth can work over a long range. If you leave your headphones at home and take your mobile device with you, then this option makes sense.

  In all cases, audio output reverts to the speakers automatically.

Exchange Files with AirDrop

AirDrop lets you trade files, URLs, contact cards, and a few other kinds of things among Macs and iOS devices 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 technology. There's only one set of choices to make (**Figure 42**).

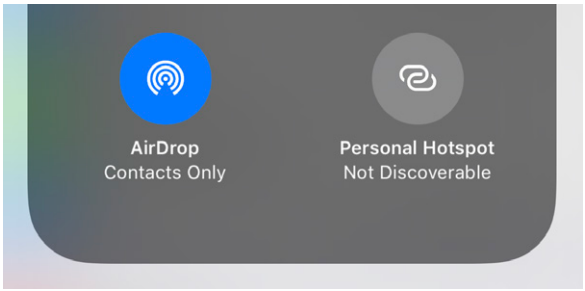


Figure 42: *Control Center is where you set AirDrop access.*

1. Swipe to show Control Center.
2. Hold down on the networking area, which displays the AirDrop icon and its status at bottom left.
3. Tap the AirDrop icon.
4. Tap one of the options (**Figure 43**):
   - 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 to receive files.

Figure 43: *You can pick how AirDrop advertises itself on a network.*

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

Share with AirDrop

AirDrop is available in any Share sheet in iOS and macOS: you can send URLs, files, photos, contacts, and other items. When you tap the Share icon in iOS, AirDrop will appear at the top, whether or not you've turned off discovery in Control Center; in macOS, it's an option you can select. You'll see a list of all users on the local network who make themselves discoverable to everyone, or who have you in their Contacts (**Figure 44**).

Share via iOS

To share over AirDrop, tap the Share icon and then select the user. The recipient will either automatically receive or tap or click to accept or reject the file, as described below.

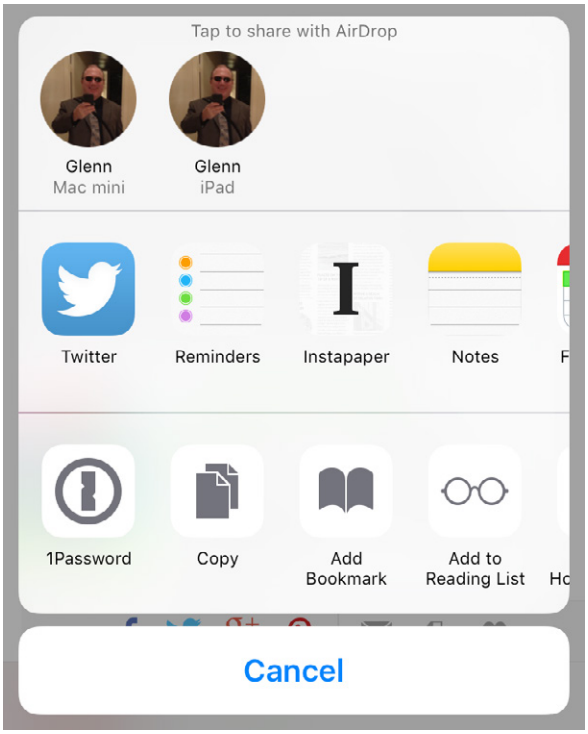


Figure 44: *The Share sheet shows all available AirDrop users.*

When a file or other item is accepted or received, the label Sent appears on the icon for the person to whom you transmitted the item (**Figure 45**).

Figure 45: *The Sent label appears to confirm delivery.*

Receive an Item in iOS

iOS prompts you to accept an AirDrop transfer from someone else or from yourself if the sending and receiving devices don't use the same iCloud account (**Figure 46**). If you click Accept, the items are received.

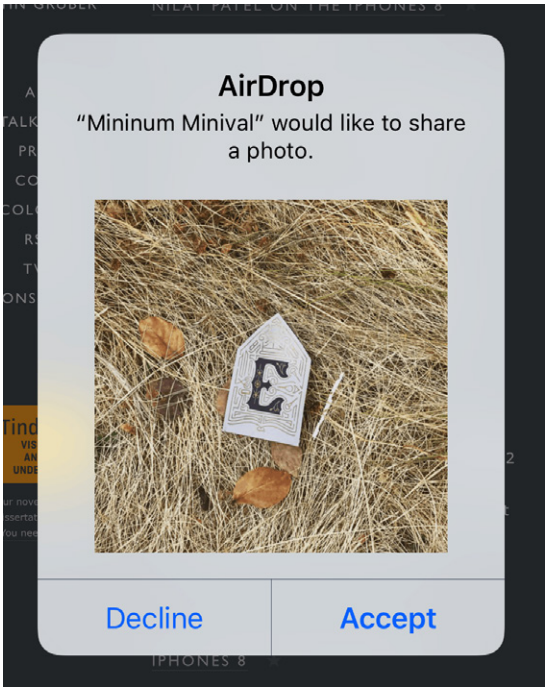


Figure 46: *You're prompted to accept incoming files from a device that isn't logged in to the same iCloud account.*

When logged in with the same iCloud account in iOS 11, there's no prompt. Instead, you see an unusual overlay notification, and then the appropriate app is opened for the item received (**Figure 47**).

Figure 47: *iOS 11 accepts items without a prompt when the same iCloud account is used on both the sending and receiving sides.*

Incoming items are handled differently by type:

- Image files are added to your Photos collection, the Photos app is launched, and the image is opened.
- URLs are opened in Safari.
- Other files are opened by the appropriate app, if it's installed. For instance, a Soulver file from macOS opens in Soulver for iOS on my devices.
- If no appropriate app is found, an Open With menu appears from which you can select a program that can handle the generic data or that manages generic files, like GoodReader and Transmit (**Figure 48**). You can also choose Save to iCloud Drive.

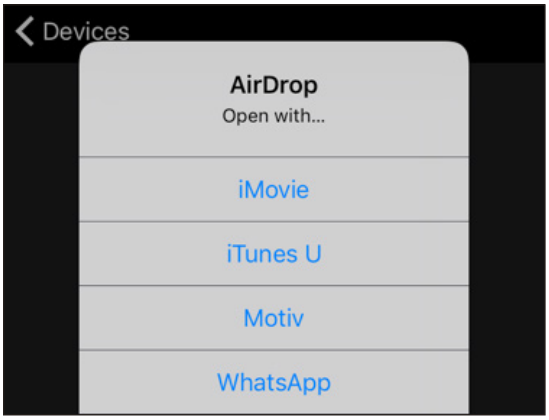


Figure 48: *With no matching app, iOS prompts you for possibilities.*

AirDrop and macOS

macOS can share any Finder item via AirDrop:

1. In the Finder, choose Go > AirDrop (Command-Shift-R) or click the AirDrop item in a Finder sidebar window. The AirDrop window shows available recipients (**Figure 49**). (On Macs with Handoff support, it also has the same pop-up menu for configuring how your system is discoverable.)
2. Drag a file, folder, or set of items onto a recipient's icon.

3. With the same logged-in iCloud account and a recipient using iOS 9 or later or macOS, the item is received. In all other cases, the recipient is prompted to agree to Save, Decline, or Save and Open.

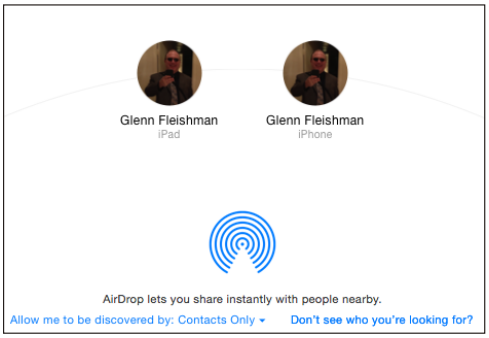


Figure 49: *A collection of recipients is shown in the AirDrop window.*

In apps with a Share button, click it and choose AirDrop, and you can pick a recipient for a URL, an image, or another item (**Figure 50**). The same conditions apply as in step 3 as to whether a recipient is prompted.

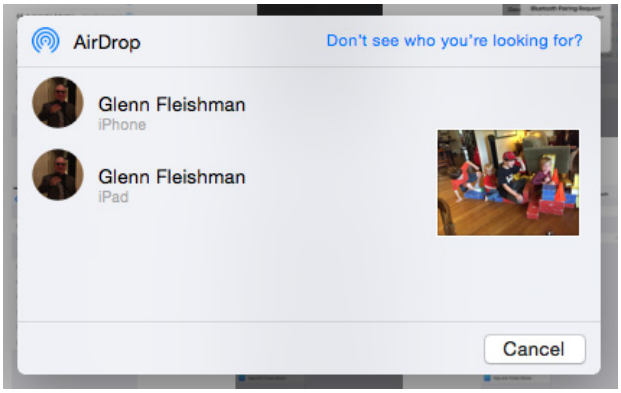


Figure 50: *You can AirDrop an item within a macOS app, too. Here, I'm sending an image from Photos for macOS.*

Stream Music and Video 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, the AirPort Express base station, 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.

Select AirPlay Devices

This chapter has to start a little backwards, because before you can use AirPlay, you need a destination. But it's easier to walk through how you can configure your iOS device 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 iOS device, follow these steps:

1. Swipe to reveal Control Center.
2. Tap the AirPlay  icon at upper right. (If no AirPlay destinations are available—or powered on—the AirPlay icon doesn't appear.)
3. Select the device you want to use as a destination (**Figure 51**).
   - 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.

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

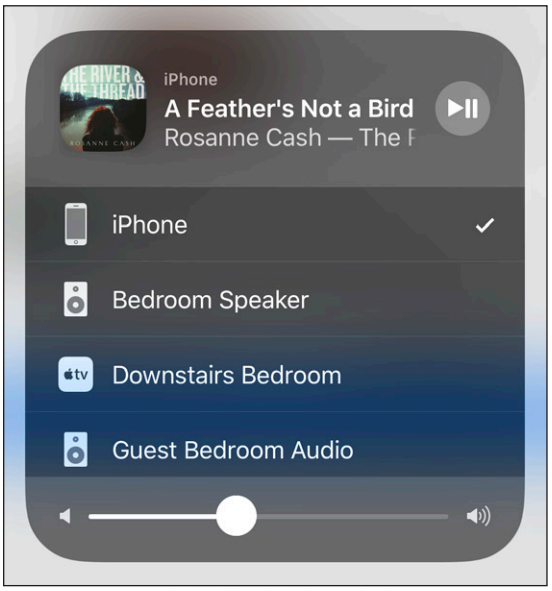


Figure 51: *Available AirPlay destinations are identified by type.*

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, and those must be entered in the iOS device to connect.
- With a password, the destination device has a password set through whatever means (such as AirPort Utility with an AirPort Express), and then you enter that password in iOS.

Some Apple and third-party apps offer direct AirPlay device selection. The same options appear, only in the form of a popover with an option to select an item (**Figure 52**). In some cases, you might see a Done button rather than play/pause. You can also tap elsewhere to exit the view.

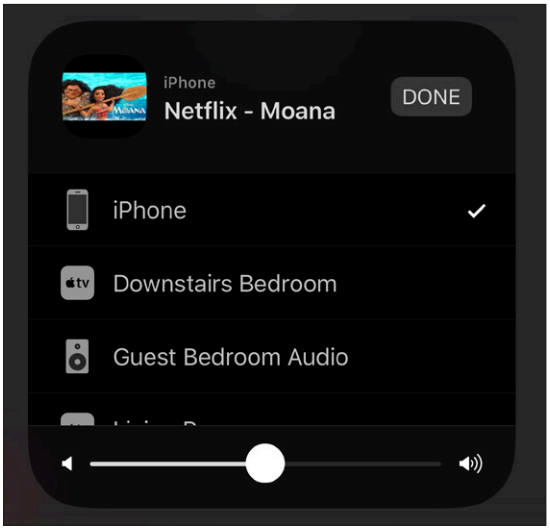


Figure 52: *The popover menu in an app offers identical controls as Control Center.*

Your iOS device retains media control, so you can use volume up/down buttons and on-screen controls such as pause and rewind.

With that out of the way, let's look into uses of AirPlay.

AirPlay 2 and Multiple Speakers

Apple announced AirPlay 2, an upgrade to its streaming multimedia protocol, in June 2017. The new version, supported in iOS 11.2 and tvOS 11.2, lets those devices stream to multiple AirPlay 2 destinations at once, including Apple's HomePod.

Third-party speaker makers have signed on in huge numbers, but even at the end of 2017, it's not clear which will offer firmware upgrade for existing equipment and which will require purchases of new hardware.

Ways to Use AirPlay

The point of AirPlay is to shunt audio or video around your local network, and there are a number of ways this is useful. I walk through the most common or useful scenarios next:

- Send audio to an AirPort Express.
- Send audio or video to an Apple TV.
- Send audio to another computer or mobile using Airfoil, or receive it using Airfoil Touch.
- Mirror the display to a Mac using Reflector, a third-party app.

> **Tip:** You can send AirPlay audio and video to any device that shows up in the list. For example, I have a Yamaha receiver with AirPlay. On my local network, I select the Yamaha, which automatically turns on and selects its AirPlay mode for input. You can't turn it off via AirPlay, but Yamaha offers a terrible iOS app that has a power button.

Configure AirPlay for an AirPort Express

Apple's own hardware lets you stream AirPlay. In fact, in its original form as AirTunes, it worked only with the AirPort Express. The AirPort Express oddly remains the only Wi-Fi base station with streaming audio support; the Apple TV offers both audio and video output.

> **Note:** Apple has apparently stopped upgrading its Wi-Fi base stations, but you can still purchase an Express, and it continues to serve this purpose.

An AirPort Express has a combined analog/digital audio port. You can use any standard 1/8-inch stereo plug, or a special digital fiber optic connection that has Toslink (an audio standard) on one end and a special compatible 1/8-inch plug on the other.

Setting up AirPlay is quite simple via AirPort Utility:

1. Launch AirPort Utility, either via iOS or in Applications/Utilities in macOS.
2. Select the AirPort Express base station. Enter the password if prompted.
3. Click the Edit button.
4. Navigate to AirPlay settings:
   - In macOS, click the AirPlay tab.
   - In iOS, tap the AirPlay item.
5. Turn on the Enable AirPlay checkbox (macOS) or switch (iOS).

6. Enter a name for the AirPort Express that will appear in AirPlay lists (**Figure 53**). You can optionally set a password, which must be entered twice identically. Click Done.
7. Click or tap Update in the Update Settings dialog that appears. The AirPort Express restarts with the new settings applied.

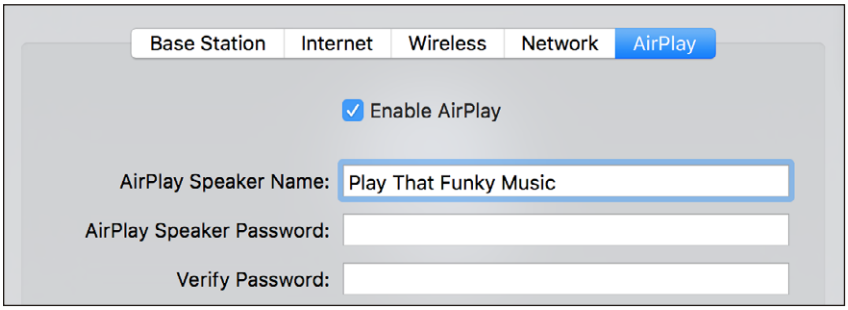


Figure 53: *AirPort Utility in macOS allows AirPlay configuration for an AirPort Express.*

Configure an Apple TV for Audio and Video

Turn on your Apple TV, navigate to its Settings menu, and then select AirPlay (**Figure 54**). You can now:

- Select AirPlay to toggle it on or off.
- Select Apple TV Name to set the device's identifier in the AirPlay list used by other hardware and software on the network.
- Tap Security and set a password.

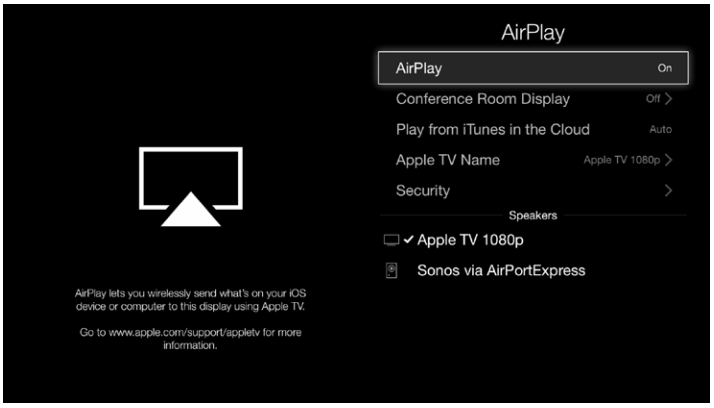


Figure 54: *Apple TV lets you set AirPlay's name and whether security is active.*

Send Audio with Airfoil

Rogue Amoeba makes **Airfoil**, a straightforward software package for streaming audio from macOS and Windows to other devices. Airfoil lets you pick a piece of software as its input and one or more destinations for audio while setting individual volume levels (**Figure 55**).

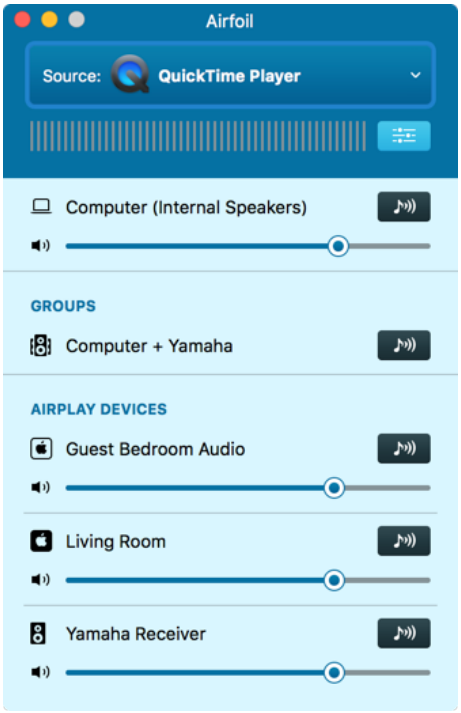


Figure 55: *Airfoil lets you stream audio from any app or the system to one or more AirPlay or proprietary Airfoil destinations.*

But Rogue Amoeba also offers complementary and complimentary (free) software that lets you use iOS more effectively.

First is **Airfoil Satellite**, available for macOS and Windows. It turns a computer into an AirPlay destination, so you can stream audio from an iOS device or a Mac. Systems running Airfoil Satellite appear in the AirPlay list in iOS.

Second is **Airfoil Satellite for iOS** (free), which acts as a remote control for Airfoil for Mac or Windows, and lets you stream audio using a proprietary protocol from Airfoil to your iOS device.

Note: Airfoil can stream to any AirPlay device, including Airfoil Satellite for macOS and Windows. It can also stream to Airfoil Satellite for iOS, Android, and Linux, which use its proprietary standard and don't appear as AirPlay devices.

Mirror an iOS Screen

AirPlay is often used for audio or to push video playback to another device. But it can also stream your active iOS display to an Apple TV. In Control Center, tap the Screen Mirroring button and choose an Apple TV destination.

However, if you want to stream the display to a Mac, you've got a third-party option. **Reflector** from AirSquirrels ($14.99) acts as an AirPlay video target. Select it as a destination in your iOS AirPlay menu, and the iOS display—minus any indication of taps—appears in a window on your Mac. You can set passcode or password access.

Being able to stream your full iOS experience is useful for demonstrations and for recording movies of what you're doing to show other people later.

Tip: Starting in iOS 11, you can record your device's screen directy. In Settings > Control Center, tap Customize Controls, and then tap Screen Recording. Now a Screen Recording button appears in Control Center. Tap it and it starts recording the screen, and puts a red bar behind the status bar to remind you that you're still recording. Tap the button in Control Center again to stop recording.

PRIVACY

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. iOS, 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. iOS 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 iOS device 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 Designed To Improve Anonymity

Starting in iOS 10 and macOS Sierra, Apple has 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 something called *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.

But there's a way around this. Give the subject a coin, and have them flip it. Heads, they always say "yes." Tails, they always give an honest answer. With a small number of people, the

results remain poor. With a large enough number, however, the statistical noise of the coin flip can be reversed out without knowing which subjects answered honestly.

Differential privacy uses the equivalent of hundreds of random coin flips, and destroys information as it creates an answer to send to Apple, so there are no intermediate steps that can be recovered and analyzed, either. (Google has used this approach for years to collect usage statistics within Chrome.)

Apple started using this method for a few kinds of information in iOS 10: QuickType and emoji suggestions, Spotlight deep link suggestions, and Lookup Hints in Notes. In iOS 11, it added the types of data people use with HealthKit (but not values collected), and web site loading speed and battery usage. Apple strongly suggests third-party developers use this approach via built-in libraries.

At this writing, **privacy researchers have raised concerns** with Apple's implementation. It's also unclear how to opt out of collected data, a big missing piece on Apple's part.

Apps

The OS can track which apps you install and which of them you launch. A developer in 2011 created a framework for other developers that relied on listing all app-registered schemas—the app-specific part of a URL—to get a partial sense of all apps installed. (For example, `fb://friends` comprises `fb`, the schema for Facebook's app, and `friends`, a destination the app interprets and then opens as the Friends list.) That framework, as well as a proof-of-concept app, has since been effectively banned.

Apps themselves can also track precisely what you do inside them. While this seems obvious, what the app does with that information is always a question. Is it sent anonymously in some form to troubleshoot and improve the program? Is it aggregated anonymously to change how the app behaves? Does it use differential privacy to randomize data so that there's no chance your individual actions can be figured out later? Is all your information sent to servers to be processed—and is it retained or deleted, and if so, how does the app maker ensure this?

Where iOS is concerned, Apple offers extensive privacy policies that explain how your data is tracked, transferred, stored, retained, and deleted. I go into this in depth in iOS Privacy Settings.

***WARNING**: It's also possible for someone to use AirPlay or on-device recording (starting in iOS 11)to capture everything appearing on your screen. However, AirPlay have to be set up through a few taps on the device, while recording displays a red banner in the status bar.*

The web and web searching

It's of interest to others how you surf: what you are looking for, which search results you click on, where you wind up, which web sites you have bookmarked, and what pages you view on them—even how long you spend on any page or how you move a cursor on that page. And, of course, when you purchase things.

Because you're using search engines and web sites, the destination where you wind up and what you do there is captured by wherever you visit. What those sites do with your information is a matter of the privacy policy on each site.

Tip: Content-blocking Safari extensions can help to block unwanted tracking and targeting; there's a whole chapter on them coming up.

However, iOS also sends various information to Google, Bing, and other search engines in different places—sometimes in Safari, sometimes in Spotlight, sometimes elsewhere. I cover how to control what information is sent in iOS Privacy Settings. The Duck Duck Go search engine is specifically designed not to retain information about you between searches, and it can be set as your default Safari search engine.

In the past, some clever hacks have let web sites trigger a browser into sending some or all of its browsing history. While the last of those was fixed a few years ago and mobile Safari doesn't have any known weaknesses, it's worth considering how often you want to wipe your browser history to prevent tracking.

Metadata

In the era after Edward Snowden's revelation, most people know what metadata is: it's information that describes other information, like the

destination of an email message rather than the contents of the message. iOS lets you send instant messages through iMessage and SMS/MMS as well as via third-party apps; use cellular and Wi-Fi calling via Phone; and use Skype and other VoIP programs for audio/video calls, chatting, and file transfer.

All of those activities involve recipients, locations of where you and they are at a given time, and the frequency and duration of contacts without revealing any of what you send back and forth.

Sensors and receivers

I noted hardware as a category above, but the more specific elements that can be tracked include:

- What you're saying (via the microphone) or doing (via the front-facing or back-facing camera). Apple displays a red bar below the status bar (which it also changes to red) and lists the program currently accessing the mic (**Figure 56**). When recording has paused but the app has still reserved the mic for its use, it shows that, too. (With Apple's Voice Memos app, it just shows the time elapsed.)

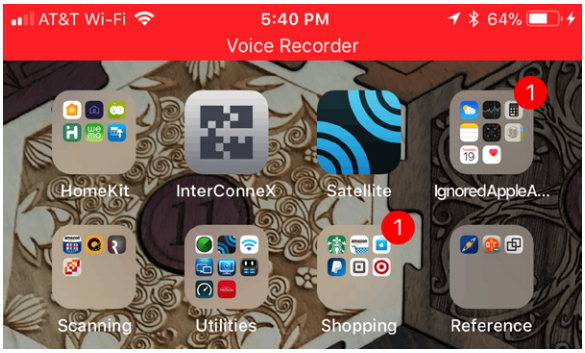


Figure 56: *While iOS is recording, it puts a red banner at top to let you know.*

- Where you are using GPS, cellular, and Bluetooth. If your location is currently being accessed, Apple puts a location icon in the status bar, unless you've disabled it. (See **Location**.)
- Your speed, heading, and altitude, via a GPS, barometer, magnetometer, and accelerometer.

Data

Finally, we should review the kind of information that could be extracted so you can consider what you opt to store:

Your fingerprints and your face. Although Apple locks all this away in a one-way Secure Enclave portion of a chip—for Touch ID and Face ID—the fact that one or more fingertips or your face unlocks a device can be a giveaway: it proves you own or have access to it, which can be evidence in a trial or otherwise used against you.

Contacts. All the emails, phone numbers, and personal data you've stored.

Email. Not just the email on your device, but if you've configured it typically, all the email also stored on your email provider's servers.

Messages. iOS stores your messages locally and indefinitely.

Historical sensor data. HealthKit, iOS, and various apps can retain a trove of data about you gathered from hardware sensors.

Photos. With iCloud Photo Library, Google Photos, or other cloud-based photo services, you're storing not just pictures and video taken by the device, but also any available from the cloud.

Faces. If you use the facial-identification feature in Photos, you're storing information about the people with whom you interact.

Where you've been and where you're going. Your current location and related position information can be obtained, and some apps retain where you've been, including things as disparate as which cellular towers your phone has recently checked in with. With travel apps and mapping apps, itineraries and destinations may also be available.

iOS 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. (It did have a small ad business, iAds, that it shut down.) 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 iOS device to Apple and beyond.

Setup without Much Sharing

It's a privacy conundrum: Apple encourages you to enter personal or private details and connect your iOS 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: Starting in iOS 11, you can set up one iOS device by having another one nearby and entering your existing device's passcode. This may bypass some privacy settings you want to adjust by hand.

Start setup. On the third setup screen, Choose a Wi-Fi Network, 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 57, left**). The moment you do this, some information about your activities starts transmitting immediately — although not much.

On the fourth screen, Location Services, choosing Disable Location Services ensures nothing related to your position is sent (**Figure 57, right**). (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.)

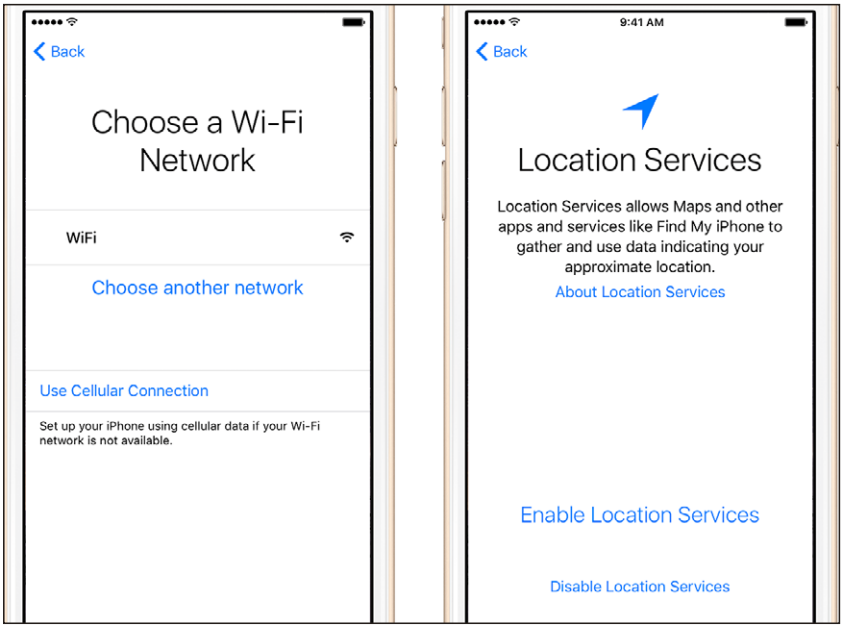


Figure 57: *You have to pick some network (left), but you can disable Location Services.*

On the seventh screen, Apps & Data, don't enter an iCloud account's information, but instead pick Set Up as New iPhone (**Figure 58**). 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.

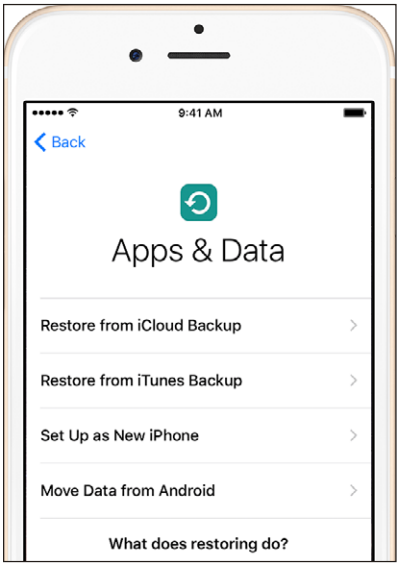


Figure 58: *Don't restore a backup, but start from scratch.*

Continue to the Siri screen, where you should select Don't Use Siri (**Figure 59**). On the Diagnostics screen, choose Don't Send. The device should now be set up.

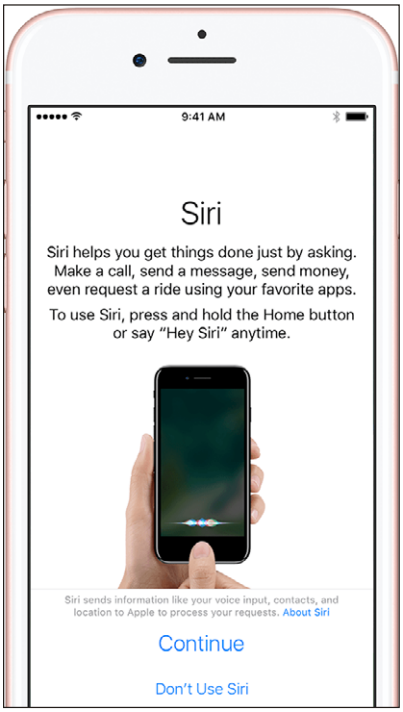


Figure 59: *Siri can leak certain data; don't use it till you can choose which associated options to allow.*

Now you can read through this chapter and decide which features to enable, whether related to privacy or to the way in which your information is synchronized to the iOS device.

Controlling System Privacy

Much of the information iOS captures about you and sends to Apple's servers is used to improve your "experience." For example, Siri can't work without sending your voice off to central processing, and it learns more about you over time as you correct its dictation and travel. But you can also reset Siri at any point, and it forgets forever the connection between any interaction and your device.

Apple typically tries to capture the least amount of information it needs, and when it needs to make a connection between you and that data, it associates your information with a tag that isn't connected permanently to your identity. You can disassociate from that tag and forget most or all of that information with a click.

In this chapter, I examine the many places in iOS where you control what you allow Apple to know about you, and how you either prevent sharing details (such as your location) or cause Apple to delete your data.

Note: The Settings > General > Restrictions options let you lock all privacy settings in whatever state you like in a separate privacy section.

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

Disabling Information for Ads

Apple scatters its settings related to how it gathers information from you to better target ads by interest and location. There are two settings you can disable:

- Privacy > Advertising: set Limit Ad Tracking to On
- Privacy > Location Services > System Services (found at the very bottom): set Location-Based iAds to Off

You can also reset an identifier that's tied to your Apple ID account and used to associated targeting information in Privacy > Advertising. Tap Reset Advertising Identifier, and the link between you and the data gathered is severed.

Siri

iOS's voice-processing technology mostly lives in Apple's cloud, and thus you need a live network connection to use Siri and Dictation. When you speak to Siri, it passes what you say to Apple's servers for a response—and other information to help provide better cues as to what you mean, some of which is never stored and some that is stored anonymously.

Siri in iOS 11 comprises several kinds of tasks:

- Actions in response to requests, like opening an app or setting a timer.
- Contextual responses that relate to information about where you are or who you are, like weather or calling your spouse.
- Dictation.
- On-device searching, formerly called Spotlight, which integrates results from Apple and third-party apps that provide indexed results to Siri.
- Search engine results via Safari.

Let's look here at the first four bullet points, and discuss Safari-related Siri behavior in the next section on Safari.

What Siri knows about you

Apple's privacy document for Siri and Dictation explains that it collects the following details:

- Your name and nickname
- Names, nicknames, and people's relationships to you that are stored in your Contacts
- Song names in your collection
- HomeKit-enabled devices
- Names of photo albums
- Your current location (if available)
- Some portions of data from third-party apps that use Ask Siri to understand what you're saying or for dictation

Apple connects this information to you using an identifier that doesn't contain information about you. You can sever this link whenever you want, by disabling both Siri and Dictation.

In iOS 11, you can't simply turn off Siri. Instead, you need to flip a couple of switches. In Settings > Siri & Search, turn off Listen for "Hey Siri" and Press Home for Siri (**Figure 60**). When you tap the second switch, you're prompted with a warning that Siri will be turned off altogether. (If you had just one enabled, turning it off also triggers the warning.)

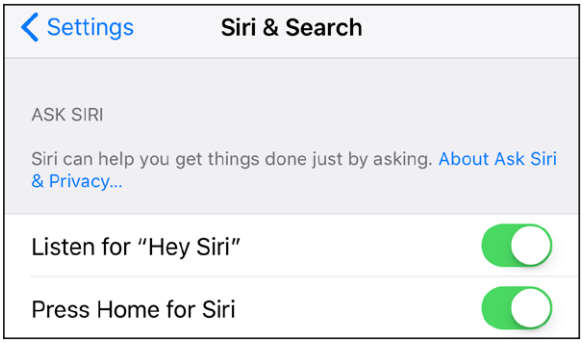


Figure 60*: Disable Siri and the link to your device is tossed, but not all data collected.*

To turn off Dictation, go to Settings > General > Keyboard, and turn off Enable Dictation. This severs the link between your device and Apple, although on its servers, Apple may retain a fair amount of:

> *"...audio files and transcripts of what you said, related diagnostic data, such as hardware and operating system specifications and performance statistics, and the approximate location of your device at the time the request was made."*

If you're uncomfortable with any of that ever being sent or retained even in that disassociated form, disable Siri and Dictation and never use them.

You can also selectively disable location hints for Siri and Dictation, so that neither service uses contextual clues, by configuring Settings > Privacy > Location Services > Siri & Dictation to Never.

Siri and on-device searching

iOS 11 relies on Siri for on-device search results in a conceptually complicated fashion. In Settings > Siri & Search, you'll see two items under Siri Suggestions: Suggestions in Search and Suggestions in Look Up. These switches, which default to on, allow Siri to make suggestions within apps or when using Search, the Look Up feature, its News app, Photos' Memories section, or Apple's keyboard (**Figure 61**). (Some of this was formerly connected to Microsoft's Bing.)

Apple uses this information to personalize results in a number of places, and it syncs this personalization through end-to-end encryption among all your devices associated with the same iCloud account.

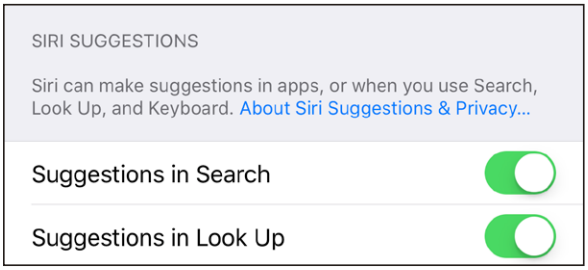


Figure 61*: Spotlight suggestions for search and look up pass information through Bing.*

To create these matches, it uploads what it describes as "generalized topics of interest," like whether you like "cooking or basketball." It also sends search queries and related information to its servers to fulfill your request, but it says the information isn't associated with you, and it doesn't include any data related to stuff stored on your device.

Further, Apple gathers location information, and details about music and video subscriptions you may have and sends that. Apple says it doesn't include any personally identifying information or account details and uses this data to improve results and not for other purposes.

However, this amount and variety of information collection may seem like too much to you. If so, you can flip either or both switches off. This will make searches less precise and adaptive, but it may be worth the tradeoff to you.

You can also disable individual apps from contributing information towards searches, such as finding files stored in Dropbox or matching text in messages in Mail. Apps are listed below the Siri Suggestions switches. Tap an app, and then you can see what kind of information it contributes towards search results—which might be used by Apple to improve Siri overall as well—and can disable that switch.

Note: A few of Apple's apps—Calendar, Contacts, Maps, and News—in that list also include a setting for Find in Apps. This enables detection of events, contact information (like phone numbers), locations, and news stories in other apps. For instance, while using Mail, someone mentioning that you should come over tomorrow at 5 p.m. turns into a link that you can tap to add to your calendar.

Safari

When you use a web browser, you're always leaking information about yourself. Use a search engine, and it knows what terms you typed in, what kind of device you're using, and your IP address. When you visit a web site, it knows what pages you request, of course, but may also track mouse movements and use tracking IDs to identify you from previous visits and across multiple unrelated sites.

Note: Apple has severely restricted the use of tracking IDs in iOS 11, as I describe later in this chapter.

Duck Duck No? Yes! *Duck Duck Go is a search engine that promises not to retain or resell personal information. Many people who dislike the tendrils of Google opt to use Duck Duck Go instead. You can set it as your preferred search engine in Settings > Safari > Search Engine.*

iOS has several options to reduce the amount of information leaking about you. iOS 9 and OS X El Capitan introduced content-blocking extensions for Safari as a sophisticated way to block tracking, ads, and creeping privacy leaks. See **Content-Blocking Safari Extensions** for a full rundown on how to use them.

Even innocuous features such as autofilling forms and storing passwords increase your risk if someone gains access to your phone or you visit a malicious site. Fortunately, Apple also has tools that help protect you.

Apple's Suggestions

Apple tries to give you the best answer for whatever you're looking for in Safari, but to do so it sends information about you to a search engine or its own servers. When enabled, the Search Engine Suggestions option at Settings > Safari transmits your query to the search engine you chose and then displays the results it offers. (Preload Top Hit downloads the first match in the background.)

Safari Suggestions displays all sorts of things—search results, apps, movie showtimes, and more—based on the terms you enter, your location, and the music and video subscriptions on your iOS device.

You can disable either or both Suggestions options entirely, or turn off location awareness, via Settings > Privacy > Location Services; swipe down to the bottom (past all the apps that use location data) and tap System Services, where you can disable Location-Based Suggestions.

Because Apple tries to be explicit about how it uses your information, you'll note a new Siri & Search item at the top of Safari settings in iOS 11. Tap this, and you can see that your behavior in Safari could influence Siri results elsewhere. If you don't want this cross-pollination, tap the switch to turn it off.

Passwords and AutoFill

Although automatically providing or filling in information would seem like a plus—as long as those details remain under your control—you may prefer not to have any such information stored permanently on your iOS device. And with iCloud, some information is synced across all devices with the same Apple ID and settings.

For example, you may not want your information filled in on a form automatically. Some web pages use AJAX, a kind of portmanteau scripting technology for live server interaction. Even if you never click or tap a submit button, that form information is sent. You also may not want someone else with access to your iOS devices—even perfectly legitimate access—to log in or fill in information on sites.

With Settings > Safari > AutoFill > Names and Passwords enabled, whenever you visit a web site and enter account information and passwords for login, Safari will offer to capture and store them (**Figure 62**). A pop-up dialog will present three options: Save Password, Never for This Website (never asked again), or Not Now (asked on next visit).

Tip: iOS 11 finally adds the ability to view and edit your stored account information and passwords via Settings > Accounts & Passwords > App & Website Passwords.

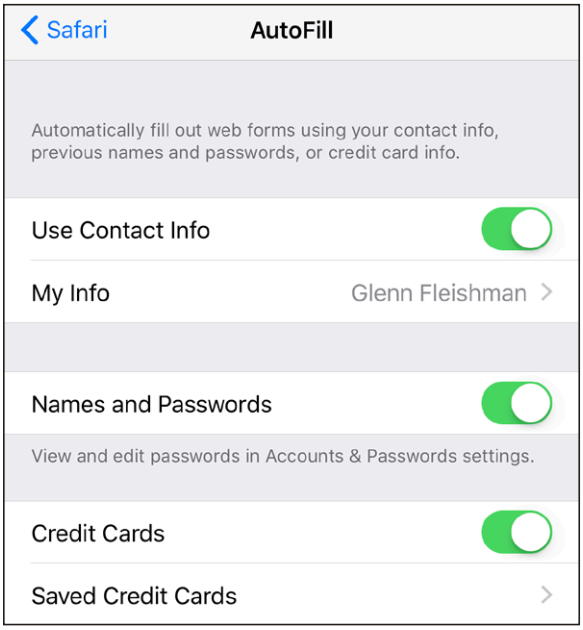


Figure 62*: AutoFill handles a lot of stored information.*

Tap the Passwords item and then enter your passcode or use Touch ID or Face ID to view and manage passwords. With iCloud Keychain turned on (Settings > iCloud > Keychain), iOS brings up all related passwords from every Safari interaction on all linked devices.

All entries matching the URL or domain appear, and iOS labels them as "from this website" or "from" plus the full domain name if it's not an exact match. You can tap one of those, or tap Other Passwords to find other entries, which brings up the searchable and scrollable list.

If you tap Forget Saved Password to remove an automatically filled-in match, iOS deletes it—but it also deletes it on all other devices logged into the same iCloud account with iCloud Keychain enabled. Be wary!

Starting in iOS 11, these passwords can also be used in third-party apps that have enabled the feature (**Figure 63**). The option to use a stored password appears above the Apple keyboard, which shows the URL and the account name. Tap the key icon to proceed. iOS shows matching passwords, but also automatically provides the search field and scrolling list to make it easier if no match appears or the match that doesn't isn't correct (**Figure 64**).

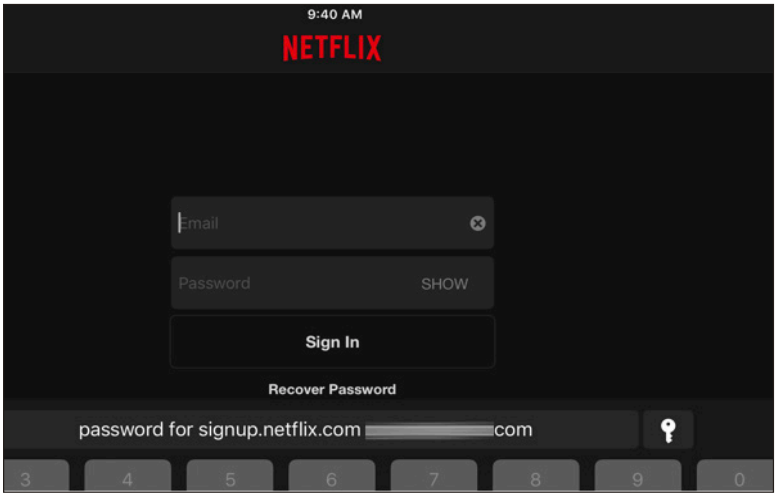


Figure 63: *Third-party apps can now tap into stored iOS passwords.*

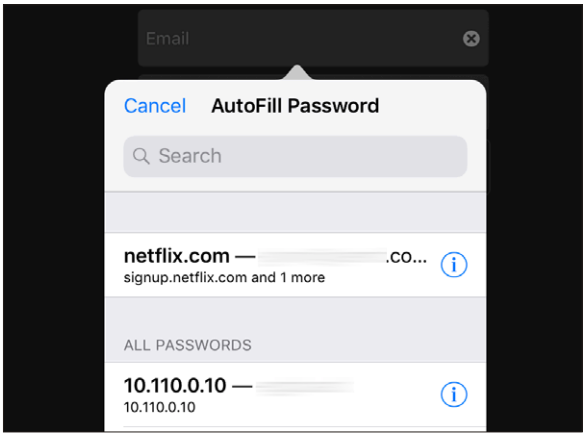


Figure 64: *App-based logins offer a somewhat different autofill approach.*

You can disable Names and Passwords in the Autofill settings at any point, and all password entries remain intact in iOS (and in iCloud Keychain) but no longer appear in Safari or other apps.

Tip: If you want to delete a bunch of entries at once, visit Settings > Accounts & Passwords > App & Website Passwords, authenticate, and then you can tap Edit to select multiple entries to remove at once. It's easier to manage deleting a lot of passwords or all of them via Safari in macOS, however. (Safari > Preferences, click Passwords, and select ranges or Edit > Select All, then click Remove.)

Safari's preferences for AutoFill also let you enable and disable pre-filling your contact information (tap Credit Cards on or off) and credit card details in Saved Credit Cards. Safari credit cards are managed separately from Apple Pay.

Watching the Watchmen

Beyond content-blocking extensions, which affect what loads in a web page, you can also control several elements of how web sites interact with you.

> ***Nuke all data:*** *While these blocking options control specific kinds of browser/server communication, you can also get rid of all data associated with web site visits by tapping Settings > Safari > Clear History and Website data. If you're signed in to iCloud, it also nukes this information from Safari on every associated computer and iOS device.*

Ask Websites Not To Track Me

A well-intentioned effort began a few years ago to let browser users indicate in an affirmative manner their preference about being tracked across one or more web sites. The so-called "do not track" setting would be a simple preference sent from a browser if the user had checked a box or enabled a switch for Do Not Track. It was that simple.

Unfortunately, advertisers and other parties who track user behavior opposed recognizing that flag. Browser makers also mucked up the clarity of Do Not Track by enabling it by default or proposing that new releases would enable it by default. This takes the user intentionality away if a browser automatically picks the option. Really, there should be three states: not yet decided (send no Do Not Track preference), no (don't track me), and yes (do track me).

Apple opted for a simple switch in Safari preferences labeled Ask Websites Not To Track Me. By default, it's set to Off, which corresponds to "no choice"; when it's switched on, you send a feeble signal to sites, who typically ignore it, but you are nonetheless sending a message!

Block Cookies

Browser cookies, discussed at greater length in Safari Content Blocking Extensions, let a server deposit a small bit of text in your browser to keep track of a session, preferences, or other account-related details—as well as for the more irritating purpose of tracking you around the web for marketing.

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).

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 on, say, "small superglue containers," suddenly superglue ads appear to you everywhere you browse.

Apple has taken a strong privacy stance in the version of Safari in iOS 11 and High Sierra by creating a sequence of timeouts for cookies based on the source form 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 devices) 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.
- After 24 hours through 30 days, that third-party web data can only be retrieved through a connection with that original first-party site. That blocks cross-site tracking, but makes it possible to retain other, legitimate data. A new interaction resets the 24-hour clock.
- After 30 days, Apple deletes the third-party cookie and other web data permanently.

ITP isn't perfect, because an increasing amount of ad and tracking technology integrates directly with a site's servers or uses a domain controlled by the first-party site, making the cookie appear first party. But I don't think this first pass at ITP is the end: Apple's analysis and monitoring would let it tag "first-party" cookies as tracking cookies as well.

If you don't like any of this nonsense, switch Block All Cookies to On, but it will likely break many sites you visit. A better option is Private Browsing, described just below.

Fraudulent Website Warning

This little switch in Safari preferences apparently protects you against phishing sites: sites that appear to be legitimate but are fraudulent and counterfeit, to which you're often directed by links in email or subverted advertising. Apple hasn't provided details for years about how it assembles the list, and I've never been warned in years of using it.

If you encounter a site that's in its blacklist, you'll be warned and asked if you want to proceed. This prevents the page from loading and attempting to fool you or even install malware. (Malware is a slight risk for iOS users, but a risk nonetheless.)

Check for Apple Pay

Starting in iOS 10 and macOS Sierra, you can pay for transactions within a Safari web browser using Apple Pay on an iPhone or other devices. This scheme uses Continuity, Apple's catchall term for linking Macs and iOS devices together for proximity-based activities, including Handoff, where you can start reading on one device and continue reading on another.

Apple Pay in Safari requires that a web site can detect whether the browser can hand off a transaction. This leaks a tiny bit of information about you, and you can disable this.

Private Browsing

Not a preference but a mode: you can use Safari in a way in which all your normal settings are overridden and nothing is retained from the browser window you use once it's closed (**Figure 65**). Specifically, your history in that window is forgotten, the tab isn't synced with Safari on other devices through iCloud, Do Not Track is set to On, cookies aren't permanently stored, and local storage isn't accessed.

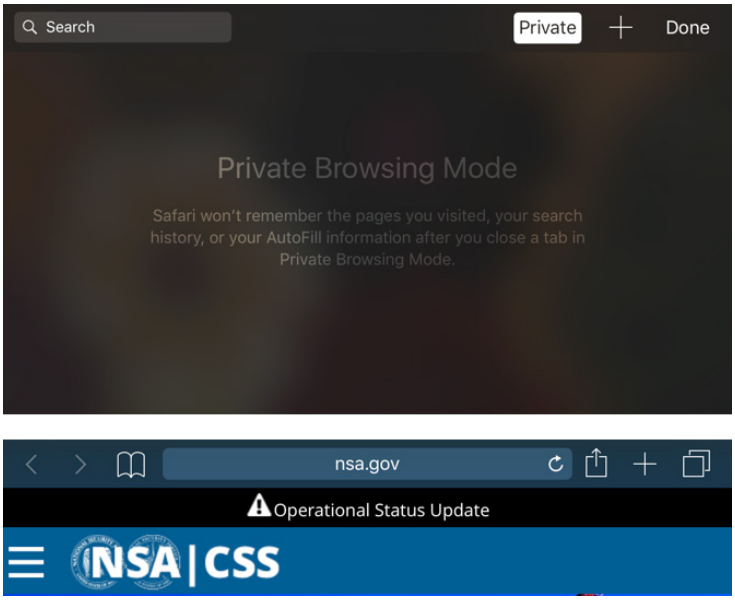


Figure 65*: The Private Browsing mode explains itself (top). A page loaded (bottom) keeps the dark top bar to remind you.*

In Safari, tap the Windows button and then tap Private at the bottom of the screen on an iPhone or iPod touch, or at the top of the screen on an iPad or on some iPhones in landscape mode. You can also hold down on the Safari windows icon and select New Private Tab.

The color scheme switches from light to dark to remind you that you're browsing privately. To exit the mode, tap the Windows button and tap

Private again. However, private browsing tabs remain in a paused state rather than closing when you exit. If you want those tabs shut, hold down the windows icon and choose Close This Tab or Close All X Tabs before you exit the mode.

Because history isn't retained from private sessions, it's a reliable way to zero out where you've browsed even if someone else were to obtain access to your device. This applies to "evercookies," persistent cookies that use insidious storage techniques, which are otherwise effectively impossible to delete.

Website storage

An improvement that was added several years ago to HTML and browsers allows web sites to store information in a database format in a browser. This is especially useful paired with JavaScript: a site can load and the JavaScript code can consult settings or other information stored locally without a round trip to the server, speeding up how a page might display.

In Settings > Safari > Advanced > Website Data, you'll see a list of sites that store information and how much data they're using. A selection of sites that use the most data initially appears; tap Show All Sites to view everything. You can swipe left on a site and tap Delete to remove the associated data, or tap Remove All Website Data to kill all local storage.

Location

iOS's ability to provide a set of coordinates that fairly precisely describes your current location on Earth works amazingly well. So well that you may have reasonable concerns about when, how, and to whom your location is shared. iOS offers a lot, lot, lot of settings and options. While most are centralized, Location comprises a lot of disparate things you have to consider when limiting what sees your coordinates.

Set Location Services to Off, and location information stops being gathered and fed to apps and the system. (The sole exception, Apple says, is to provide your location when someone uses the device to place an emergency call.)

Note: Apple has a full description **in a support document** of how iOS makes use of your location.

The How and Why of Location

Apple uses a combination of onboard radio systems to produce a set of standard geographical coordinates, sometimes with a margin of error when data isn't precise enough. Satellite navigation systems can provide location accuracy within meters, or even better with more satellites or when combining multiple systems. (Modern iPhones pull satellite data from four systems: the U.S.-operated GPS, Russia's GLONASS, Europe's Galileo, and Japan's QZSS.)

But iOS also uses Assisted GPS, which lets it plot satellite positions more rapidly and accurately, relying in part on data sent via a live Internet connection. It can also use cellular network information (because cellular network transmitters' exact positions are fixed and known), Bluetooth (to communicate with nearby base stations, if their locations are identified), and Wi-Fi (relying on a worldwide database, which Apple constantly updates, of the broadcast names and signal strengths of Wi-Fi networks).

iOS and apps make use of location for all sorts of purposes. Of course, advertisers want to target you, because they make more money in pushing things at you that relate to where you are. But your position can also be attached to photos (called geotagging), track a stolen iPhone or iPad, help you find a family member, bring up a list of restaurants near you, and tell you the current weather for the micro-climate you're standing in.

Opting In and Opting Out

iOS sometimes uses your location without prompting, but you can opt out of nearly all of those situations later; apps, however, must always request permission. Apps can offer three choices: Only While Using the App, Always Allow, and Never Allow. The first choice covers when an app is active in the foreground, but it also applies if the app provides a continuous background function, like Google Maps navigation.

Starting in iOS 11, apps must either show all three choices or only show the While Using and Never options. If an app offers all choices, it is never allowed to ask again. If it shows While Using and Never, the app can later ask for Always. Apple says this reduces background location gathering by

apps that don't truly need it, while also providing developers a two-step option to let users trust the app before it asks for background access.

Even after granting permission, iOS will prompt you occasionally for apps that update location in the background to make sure you still want them to do so.

When an app accesses your position, Apple indicates this through the status bar in one of a few ways:

- A hollow arrow when an app has recently requested location information
- A filled-in arrow if it's received your location in the last few seconds
- Blue double-height bar: the app is continuously accessing your location and that app isn't in the foreground

Set per-app permissions

iOS has a comprehensive panel for controlling what gets access to location even after you've authorized that access. And you can switch from restrictive While Using to Always if you want as well. In Settings > Privacy > Location Services, you'll see nearly everything associated with system-level and app-specific position permission.

At the top, a list of Apple and third-party apps appears alphabetically with a label about how the app may currently access your position.

Location privacy is split into apps and services. iOS marks each app or service with a location symbol (**Figure 66**):

Figure 66: *The arrow colors indicate how location services were recently used.*

- Purple, when in continuous use (filled in) or recently used (hollow)
- Gray, when used within the last 24 hours

- An outline, for an app that supports geofencing, which monitors when you leave or enter a defined location or area

  It also shows the specific text that the app displayed when you gave or denied permission as to how your position will be used, like, "We'll use your location to show movie times and theaters near you" for Fandango.

Location permissions for System Services

System Services, listed at the bottom, contains a host of very specific permissions for how iOS makes use of location. Some of them allow the hardware to function more accurately, such as Compass Calibration. Some are useful, like setting your time zone automatically based on location. Let's go through the list for clarity's sake:

- Cell Network Search, Compass Calibration, and Motion Calibration & Distance help hardware function more effectively.
- Find My iPhone/iPad/iPod touch is covered in **When Your Device Goes Missing**. It requires entering your iCloud password to disable.
- Location-Based Alerts enable geofencing.
- Location-Based iAds is discussed earlier in **Disabling Information for Ads**.
- Location-Based Suggestions is covered above in **Safari**.
- Setting Time Zone...sets your time zone.
- Share My Location is covered earlier in **Share My Location**.
- Wi-Fi Networking sends continuous snapshots about Wi-Fi networks picked up from your location to improve Apple's positioning database.
- Significant Locations tracks your regular haunts, and Apple says the data is stored only locally, to help with "predictive traffic routing" and other services. It requires authentication, like Touch ID, to access.

iBeacon

Apple created a short-range location-based system that allows apps you've installed to recognize "iBeacons," which are Bluetooth-equipped transmitters that can contain coupons, kiosk-style information, or other installation-specific details.

iBeacon only works with specific apps, it requires permission via iOS, and it only works over short ranges. Turning off Bluetooth disables iBeacon. You can also use the Privacy > Location Services settings for each app to disable or enable iBeacon access.

Share My Location

The most consensual of all position-providing services, Share My Location, lets you send details of where you are to people you know, either on a one-time basis (as a map) or on a dynamic basis as your current position for a period of time or indefinitely. You can use the Messages app, Find My Friends, and Family Sharing to send your location or control who sees where you are (**Figure 67**).

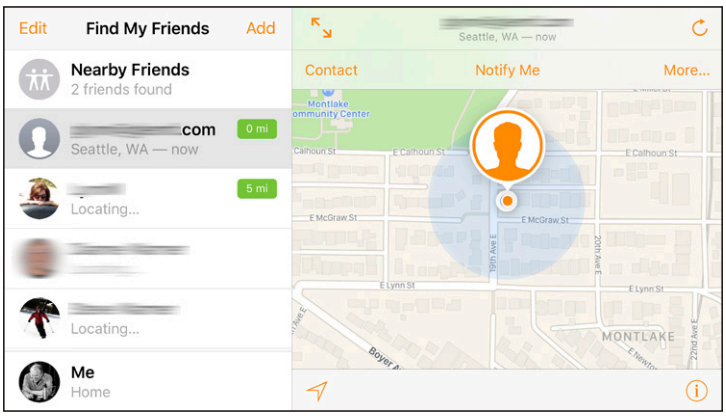


Figure 67*: In the Find My Friends app, you can see the current position of everyone who has shared their location with you and currently has that sharing enabled.*

Because the feature is exclusively opt in, you can't accidentally share your spot with people you didn't choose to. However, you can suspend sharing by setting Share My Location to Off, and then no one with whom you're connected can track you; when you re-enable the setting, the connection to them resumes as before.

You can remove people from the Friends list (and Family list with Family Sharing enabled). Tap the name, and then tap Stop Sharing My Location.

With Messages, you can opt to share your location with people over iMessage or SMS in one of two ways. Begin by starting a conversation

with someone or, if you have a conversation in the Messages list, by tapping their name. Then tap the info ⓘ button. You can either tap Send My Current Location, which sends an image of a map slice and a pin for your current spot on the map, or tap Share My Location, which lets you pick one hour, till the end of the day, or indefinitely (**Figure 68**). You can then manage that connection from the Share My Location settings.

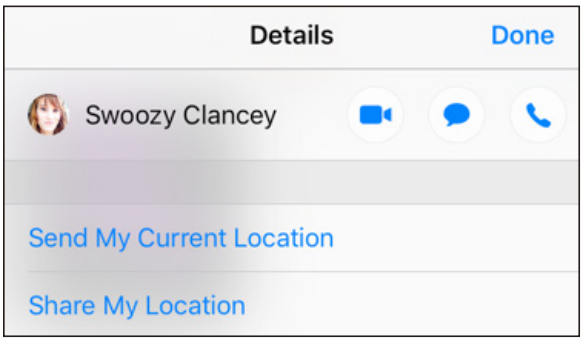


Figure 68: *You can share your location as a static map of where you are, or as a constantly updated position for a short or long period of time.*

Note: Find My iPhone is an incredibly powerful feature, but once you have it enabled, all someone needs to track your motions is access to your iCloud account and password (unless you've got two-factor authentication enabled). It's useful to consider leaving the feature off if you have any concerns about having total access to your account credentials.

Tip: You can access Share My Location's settings from Settings > Privacy > Location Services, or in Settings > account > iCloud > Share My Location (at the very bottom).

Tracking You in Maps

Apple says it goes to great lengths to prevent information about your whereabouts and trips from being connected with you and your devices. Its Maps app (as distinct from the Google Maps app) doesn't require a login to use, and relies on what Apple describes as a frequently reset random identifier to tie your current use with its servers—think of it like a browser cookie that's regularly deleted. Apple also says it doesn't collect trip segments.

The one exception to this is the Location Services > System Services > Improve Maps setting. When enabled, it lets Apple connect the address stored with your Apple ID with GPS data, albeit in an anonymous form. That is, it's trying to improve the accuracy of your address's coordinates, but it doesn't associate you with that data. Disable that behavior by setting the switch to Off.

Privacy Settings and Allowing Access

There's one more section to talk about, which is the main Settings > Privacy screen, where you manage disabling access to apps that you've previously given permission to.

Apple controls access to many kinds of personal data and device hardware by prompting you the first time an app wants to use either data or hardware, letting you confirm or reject it. This came about after apps would access your contacts list and upload it to their server for processing, including inviting other people to use the app or their service!

If you confirm access, iOS creates an entry in the Privacy settings in the appropriate category. You can visit any category and disable access on a per-app basis. You can't delete the app from the list except by uninstalling the app.

When you've disabled access for an app, the next time you use that app and try to employ a feature that requires one of these iOS caches of data or a hardware element, you'll be told that the app currently lacks access. You're directed back to Privacy to change the setting so it will be re-enabled in the app.

Keeping Creeps Away

The Internet can be an unfortunately vile and random place at times. Many communications tools, like iMessage, are designed to be open by default. Others, like phone numbers, are routinely abused. In this chapter, I look at how to clamp down on who can reach you.

Blocking Contacts by Phone, IM, and Video

When iMessage first appeared, it was a great addition to instant-messaging offerings built by other companies, such as AOL. AOL Instant Messenger (AIM) was the basis of IM for OS X in iChat; Apple registered one's .Mac, MobileMe, and iCloud account with AOL automatically. Over time, iChat added Google Chat and other options. But with the introduction of Messages in iOS and then in OS X, Apple offered its own, in-house unified mobile and desktop IM.

But there was a problem. iMessage allows us to use any phone number connected to an iPhone (even if we have multiple iPhones) and any email address. This meant, however, that not only could acquaintances who knew any of those email addresses or phone numbers reach you, but anyone could.

The same problem existed for phone calls, of course, as well as FaceTime audio and video. Yet people's concerns seemed to center on iMessage, because a phone number can be harder to obtain, and people engaged in forms of harassment don't typically want video evidence of it, either, which is easy to gather within FaceTime.

And until iOS 7, there wasn't anything you could do to stop them, which was truly horrible for those being harassed, stalked, or just subject to boring unwanted attention. The only options were to stop using iMessage or disconnect your known email addresses, and even change your phone number.

Starting with iOS 7, Apple has added several anti-harassment and blocking tools that have started to become meaningful: manual call and message blocking, which extends to phone calls, iMessages, and FaceTime; sorting incoming iMessages by those in your Contacts list and those who aren't; and third-party call-blocking apps that can flash an alert about a caller or block certain numbers altogether, as well as SMS filtering apps that try to mark and remove spam.

Carriers have also taken steps. An AT&T app for iOS works at the phone network level, blocking calls *before* they reach your phone.

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.

Call-Blocking Apps

There's a special place in hell for telemarketers who acquire numbers illegitimately, and an even worse place there for those who try to defraud. (I don't much like legal and legitimate marketing calls from companies I do business with, either.)

Fortunately, many flimflammers seem to re-use the same phone numbers as they appear via Caller ID. That makes Apple's extensions for blocking and identifying incoming calls extremely handy. Starting in iOS 10, Apple lets app developers hook into the incoming call framework to either modify the Caller ID label or block the call entirely.

Several apps and systems already existed for Android, and some companies had pre-existing relationships for licensing user-contributed databases of spammy, scammy, and scummy calls to phone carriers. You can find a variety of free, one-time fee, and subscription call-blocking apps in the App Store. Hiya, which I've used since the introduction of iOS 10, is free and simple (**Figure 69**). (Hiya sells its services to carriers, and uses the free app to continuously improve its database.)

Once installed and launched in iOS, you use Settings > Phone > Call Blocking & Identification to enable one. (Or more! Let them fight it out!)

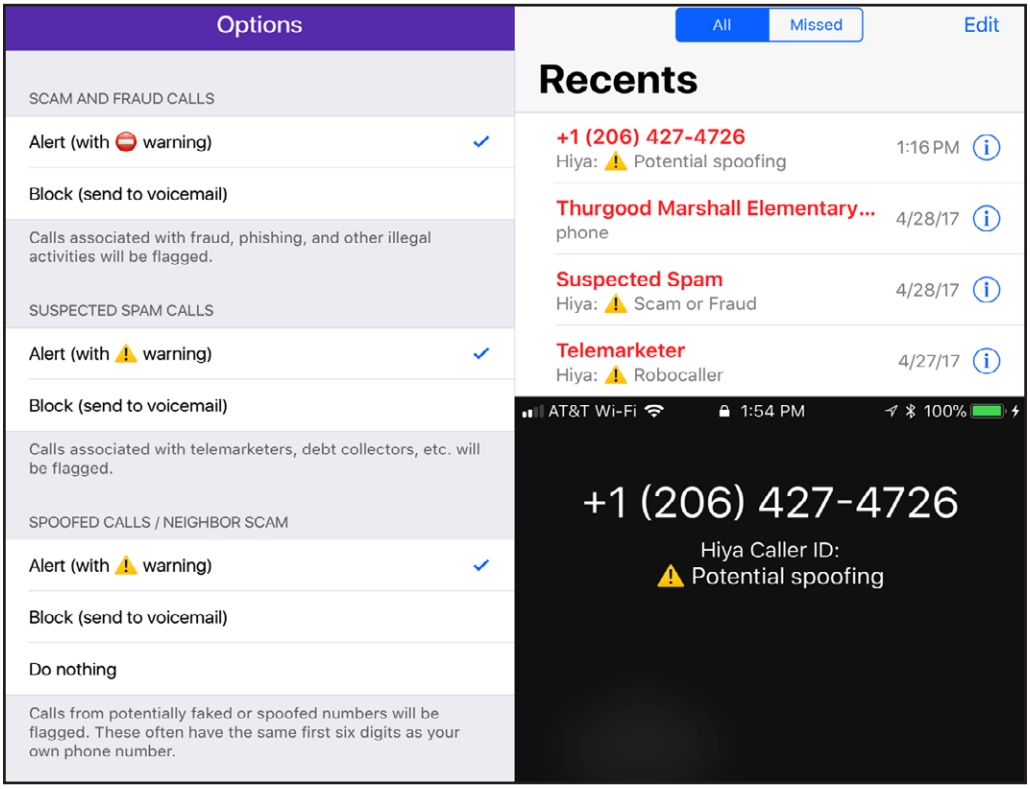


Figure 69*: Hiya lets you configure identification or blocking (left). You can see what the incoming Caller ID looks like in the Recents list (upper right). Hiya identifies the "similar number" scam (lower right).*

Then you can configure options in the app for whether you want alerts, which are inserted into the Caller ID message, or outright blocking.

> **Note:** Sometimes the first time I try to enable a call-blocking app in Phone settings, iOS tells me the action failed. Trying again or visiting the app and then returning to Settings often fixes whatever weirdness was happening.

These apps don't collect incoming phone numbers. Rather, they have to download their databases to iOS, which results in regular updates to keep pace with newly added scam numbers. If you use these apps, you can report missed scams or add details about calls you answer, which does then submit that number to their database.

A relatively new calling scam, in which Caller ID is used to spoof a number very similar to yours—the first six digits are often the same—had

been bypassing call-blocking apps. Hiya released an update not long before I wrote this edition that looks for that number pattern and can mark or block similar-number calls. The only trouble is if someone legitimate, but not in your Contacts, calls from a similar number!

An alternative to iOS-level call blocking is to use a carrier-provided tool that blocks and adds the label at the network level, not on your phone. Only AT&T and T-Mobile offer this in the U.S. (Verizon has an app that they charge for and which only modifies Caller ID.)

With AT&T Call Protect (powered by Hiya), free with AT&T accounts, calls that AT&T is confident are fraudulent never ring your phone. You can optionally receive a push notification every time a call is blocked.

> ***WARNING**: Hiya, AT&T Call Protect, and other apps require access to your Contacts list in order to ensure those numbers aren't blocked. Without allowing access, the app won't function. While these companies all promise to not use your data for any other purpose—and AT&T can already obtain all the phone numbers you call or receive calls from—this might be a privacy nonstarter for some people.*

Manually Block Numbers and Email Addresses

You can block phone numbers and email addresses one at a time in multiple places in iOS:

- 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 Details, tap the info ⓘ button, tap the phone number or name (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.

  Once you tap and confirm with Block Contact, all associated information is added to the block list (**Figure 70**). The list of blocked phone numbers and addresses appears the same whether accessed from Settings > Phone, FaceTime, or Messages. You can tap an entry to view all associated details, or swipe left and tap Unblock to allow them access to you again.

Figure 70: *The Blocked list shows all banned emails and phone numbers.*

How Does Manual Blocking Appear to Those Blocked?

When a blocked phone number's owner places a call, the line rings once, they hear a generic message about the person being unavailable, and they are dumped into voicemail. If they leave a message, it's listed separately at the bottom of the Phone > Voicemail list. The recipient isn't notified of the call.

Messages are shown to the sender as Delivered, but are dropped into the memory hole: the recipient doesn't see and isn't informed of them. Regular SMS and MMS text messages are likewise swallowed up without the sender knowing otherwise. With FaceTime, a placed call rings indefinitely without the recipient being notified.

Filter iMessages

Apple has two methods of filtering incoming messages: one for unknown parties in iMessages; another lets third-party apps filter SMS messages.

Sort iMessage by Whether in Contacts

Messages offers a subtle way to segregate incoming iMessages between people in your Contacts and those who are not. Enable it in Settings

> Messages > Unknown & Spam > Filter Unknown Senders. Incoming iMessages that match any phone number or email address in Contacts appear in a Contacts & SMS tab. Conversations already underway appear in that tab, even if they're not in your Contacts.

All SMS/MMS messages show up there, too, because many text messages are confirmations, second-factor codes, and other information that would otherwise go missed.

Any new incoming iMessages after you change that setting that don't match a contact go into Unknown Senders. Such messages don't trigger your usual notifications flags, and you have to remember to review it occasionally to see if you've missed anything.

Tap Report Junk from an unknown sender to send details to Apple.

Filter SMS with third-party apps

There's one final option that I have mixed opinions about. Starting in iOS 11, apps (including Hiya) can process text messages from any party that isn't in your Contacts and analyze them for spam. This means that confirmation codes for logins, which often come from unique SMS numbers, could pass through a third-party's servers.

With this enabled, the Messages app's right-hand head at the top changes its label to either Unknown & Junk (with iMessage Contact filtering enabled) or SMS Junk.

Apple says SMS/MMS messages stop being sent to the filter from numbers that you add to Contacts or that you reply to three times.

I find shipping off SMS messages poses too great a risk for a general recommendation, regardless of the honesty and integrity of the company on the other end. You might feel differently if you're subject to an enormous amount of text-based spam or harassment.

Content-Blocking Safari Extensions

Developers can create custom add-ins that monitor and block Safari-based connections for items on web pages known as content-blocking Safari extensions. Why block content? To reduce the time it takes to load a page that's otherwise laden with advertising and trackers, to decrease bandwidth consumed over cellular connections, to suppress unwanted advertising, and to prevent the easiest ways of tracking your activities.

It's not all about ads and behavior, though. Specialized blockers, and settings within more sophisticated blockers, can remove the display of comments on sites by blocking major content systems, keep popover boxes from obscuring your screen, remove social-network-related widgets and buttons, or blacklist entire categories of sites (such as those that show adult-oriented imagery).

> ***Is it ethical?*** *Many web sites depend on advertising to pay the bills. Blocking ads from displaying, even if you never click them, can reduce revenue, because it makes the site's audience reach seem smaller. Thus, by blocking the ads, you're indirectly taking revenue. The flip side? No site* fully *discloses how you'll be tracked and information about you sold and traded.*

How Content Blockers Work

Starting in 2015, Apple let developers create apps that can block content from particular URLs or from patterns that match URLs. The app pro-

vides the interface, if any is required. Some apps are just a set of filters you can't manipulate, while others have extensive options and customization. These filters apply to pages both in Safari and pages in browsers embedded in apps. (In 2016, Apple extended the feature to macOS.)

Content blockers don't analyze what is on a web page, nor do they examine other media and files referenced by a web page, such as Cascading Style Sheets (CSS) documents, images, video, JavaScript, and the like.

Rather, a blocker has a list of filters, which comprise these elements:

- A specific URL or a pattern that can match a range of URLs.
- A behavior: block the item entirely, block just associated browser cookies from being set, or block specific page elements (named items in CSS).
- An optional content type to match: document (which is generic), image, style sheet (for CSS), font (fonts can be quite large), raw (anything not specified), SVG document (a browser-rendered vector image format), media (images, audio, and video), and pop-up windows.
- An option to block only if it's fed from the "first party" (the web site you're visiting) or only from a third party, typically used for tracking.

> **Note:** You can find the full technical details about how content-blocking extensions work at the **Surfin' Safari blog**, a site maintained by Apple's WebKit team.

Filters are set by the app, and then compiled by iOS every time they're changed, so that they are handled very quickly in Safari. Apple created these as opposed to allowing JavaScript-based extensions, which are available in Safari for macOS, because JavaScript imposes a much heavier load per page, delaying viewing pages and burning battery life.

As noted in the list above, blocking behavior doesn't have to keep an item from loading entirely: there are two alternatives.

Browser cookies are one way to feed to 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.

These identifiers can be shared across networks and persist, so that everything you do among sites that use the same tracking or advertising service is associated. Blocking cookies can prevent many kinds of tracking by companies that comply with industry rules, government regulations, and ethical standards. Some content-blocking apps will include cookie filters.

Block that tracker: *Apple changed how Safari manages cookies, opting to limit cross-site tracking cookies by default. See* ***Block Cookies*** *for details.*

The other kind of page-specific blocking allows a filter to suppress CSS. This might sound a bit obscure if you don't design or develop web pages, but it's straightforward. HTML defines the bones of a page, like the girders of a skyscraper, and contains the innards—text and images and other stuff — just as an office contains workers and furniture and printers.

CSS is the glass and metal panels covering the skyscraper, while also painting the outside and creating the walls and cubicle barriers: it defines how things appear, including the dimensions and placement of both fixed layout areas and boxes that can seemingly float above the page.

A CSS "selector" defines the scope of what style definitions apply to. They can be used to attach to an HTML element (a tag), reused for multiple parts of a page (a class), or define a specific structure (an identifier or ID), which is used for those floating boxes among many other purposes. By allowing a blocking filter to strip out specific selectors, it can suppress advertising overlays or other annoying or intrusive behavior.

Tip: Apple lets you set Automatic Reader View for web sites starting in iOS 11 and Safari 11 for macOS. This bypasses loading most of the content of a page, showing just crisply formatted text and some images, which has the effect of "blocking" most non-text content. For options, hold down on the Reader List icon while viewing a page.

Blockers in Action

Apple allows any combination of content-blocking extensions to be enabled at once via Settings > Safari > Content Blockers (**Figure 71**). And

you can override all content filters by holding down the reload button for a few seconds and choosing Reload Without Content Blockers. Instead of a simple reload, it becomes a "reload without filtering." Some blockers provide even better bypass options through the Share option.

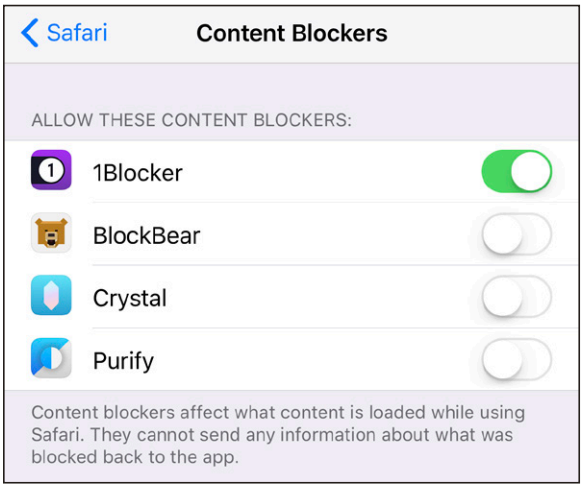


Figure 71: *You can enable and disable any combination of content blockers.*

> **Note:** Apple's notes on these filters indicate that if they take too long to process, Safari may ignore them. In practice, this should apply only to URL patterns that are complicated and require too much processing time to find matches.

Content-blocking apps come in several forms:

- Simple. The app will have no controls, and you'll rely on rules, set by the developer, that can be updated in the background or through app updates.
- Selectable. Many apps will offer an interface to select among the kind of content you want to block and how you want to block it, but provide little information about what's in the filters beyond that.
- Customizable. Some apps will be entirely devoted to seeing everything that they're blocking and will let you create your own rules; some of the selectable apps will also include limited customization.

1Blocker is my Safari filter of choice, and I've been using it since it was first released. There are *plenty* of other options, but I find it the right mix of customizable and preconfigured. I'll walk through how it approaches filtering content.

For each of several categories for which the app offers control, you can not only enable and disable blocking (**Figure 72**), but also tap the category name and see every item in the list (**Figure 73**). You can then opt to disable specific items.

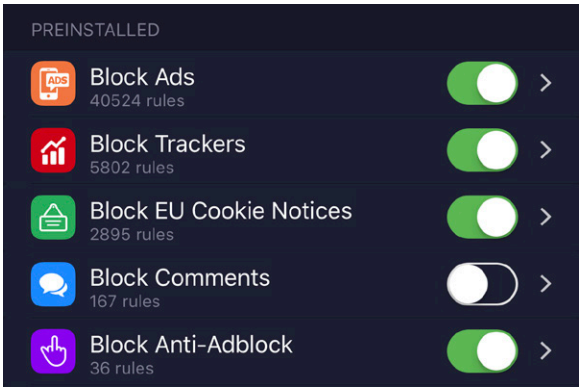


Figure 72*: 1Blocker offers a lot of separate settings for kinds of things to block.*

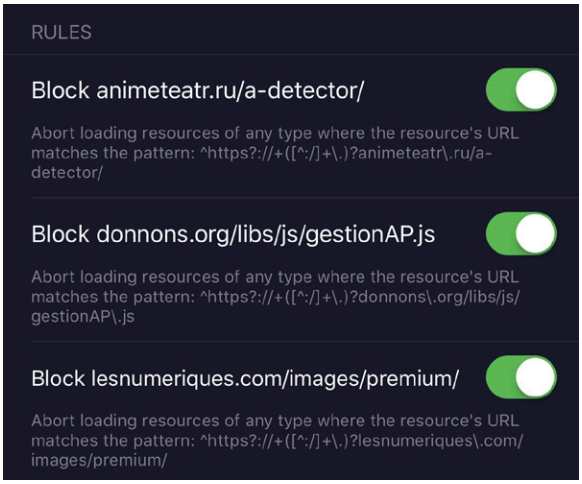


Figure 73*: You can see individual filters and disable them in 1Blocker.*

The app also lets you whitelist sites, specify blocking parameters for URLs, cookies, and page elements or CSS, and require a secure (https) connection (**Figure 74**). I configured a rule for CSS that prevents the *Washington Post*'s site from popping up a remaining articles warning (**Figure 75**).

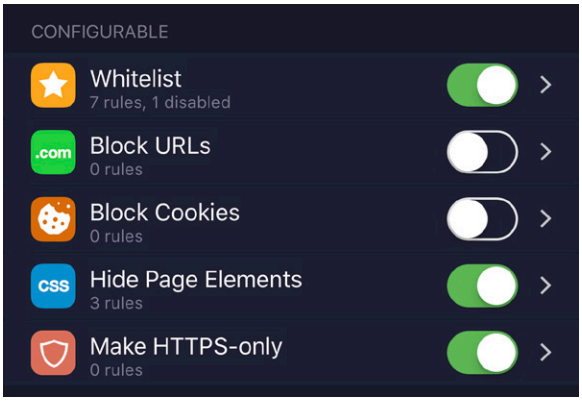


Figure 74: *You can use the Configurable section create simple and complicated exceptions, such as whitelisting an entire site or blocking page elements on one site.*

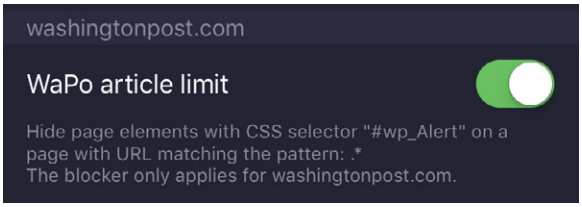


Figure 75: *As an example, I block a subscription pop-up on the* Washington Post*'s site (I'm a subscriber, but it still appears in some embedded iOS browsers).*

And 1Blocker offers an advanced configuration option via its web site, letting you create filter items that draw from every option Apple offers, which you can then transfer to your installed copy of the app in iOS.

1Blocker lets you manage things on the fly, too, with the Share sheet (**Figure 76**). If you're viewing a web page that displays poorly or that tells you to disable ad blocking in order to view it, invoke that.

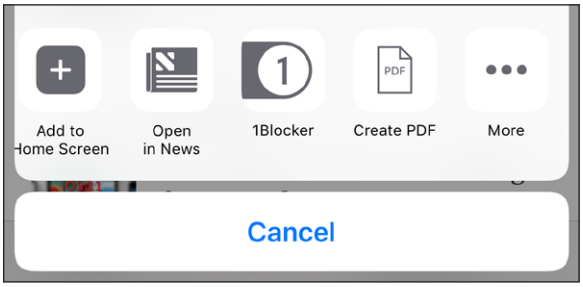


Figure 76: *As an example, I block a subscription pop-up on the* Washington Post*'s site.*

Then in the Share popup, you can do certain kinds of simple manipulations, including whitelisting the domain (**Figure 77**).

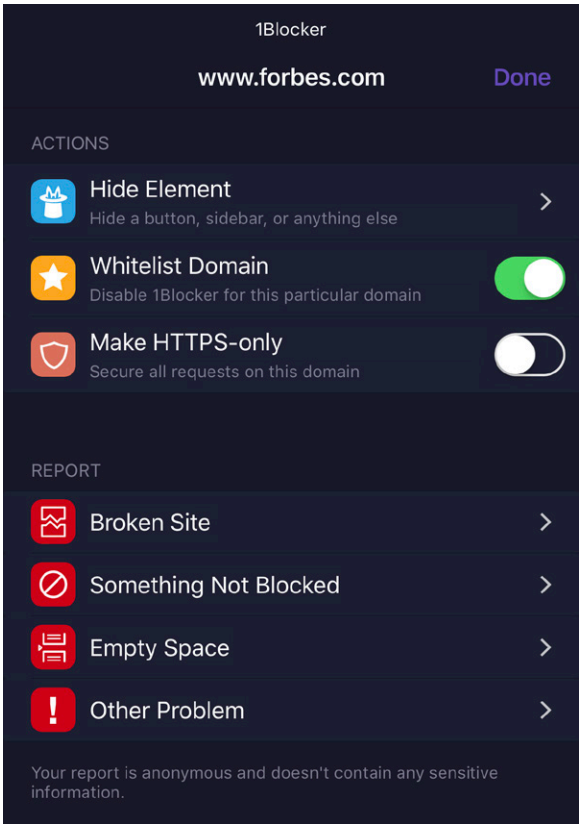


Figure 77: *Forbes really hates ad blockers, so to read it occasionally, I have it whitelisted, despite the huge array of ads and trackers it throws up.*

SECURITY

Security encompasses many forms: 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? In this part of the book, you'll get answers that will make you feel better when using a device in all situations.

Connect to a Secure Wi-Fi Network

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 iOS 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* **Transfer Data Securely** *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 iOS. 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 ⓘ 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 iOS 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. You have to persist at removing the network until it "sticks."*

What's Behind Simple Wireless Security

The best or only practical security method for connecting to a Wi-Fi network in a home or office is Wi-Fi Protected Access 2 (WPA2), supported by more or less every device sold with Wi-Fi for nearly 15 years.

WPA2 comes in two forms: personal and enterprise. (I talk about enterprise just after this section.) The personal part refers to protecting the network with a password—sometimes called a passphrase since it can comprise multiple words. It can be up to 63 characters long and include punctuation, letters, and numbers. The passphrase is run through mathematical churns to produce something stronger.

A base station's administrator sets the passphrase and then provides it to anyone who needs to connect to the network. If you've set up the network yourself, you're the person who picks the passphrase.

Security on a Base Station

If you're setting up a base station, pick a good passphrase. The best WPA2 passphrases are at least 12 characters long; 20 is better.

The current best password advice is to pick a set of words that are unlikely to appear together, but that you can easily remember. For instance, if you make up a story about a rabbit flying an airplane to Canada, you could use the passphrase `rabbit-airplane-canada`.

While that seems too easy, the odds of someone cracking that password because of its length and improbability are just as low as a difficult to type shorter password full of upper- and lowercase letters, numbers, and punctuations that you can't remember.

Some password-management software, like 1Password, has an option to create word-based passwords with sufficient randomness and complexity. And those generators produce good poetry, too.

Note: If you'd like to read more about using words in passphrases instead of incomprehensible nonsense, read my *Fast Company* article from 2015, "**Everything You Know About Passwords Is Wrong**," in which I talk to one of the most expert security researchers on password selection and cracking.

Share Network Access with a QR Code

In iOS 11, Apple added a nifty way to share network details with people you know with a minimum of fuss: you can use a QR Code—effectively a barcode, but in two dimensions— and the Camera app! Originally developed in the Android world, Apple also supports this hotspot sharing format, which encodes the network name and its password.

To create a Wi-Fi QR Code, you have to use a web site or an app; Apple doesn't have a built-in tool. I suggest **QiFi**, which uses JavaScript to create the code entirely in your browser without sending your credentials off to a server to create the code.

You can join a network via a QR Code by just pointing your iPhone or iPod camera at it (**Figure 78**). (Settings > Camera > Scan QR Code has to be turned on, which it is by default.) iOS alerts you that you can join the network, and then you tap to accept.

The password isn't encrypted! It's just encoded in dots. So you don't want to post this online or leave it lying around. It's great for public hotspots, however.

WARNING! *Some base stations also allow WPA, a temporary predecessor to WPA2. Don't use it: it hasn't been considered secure for many years.*

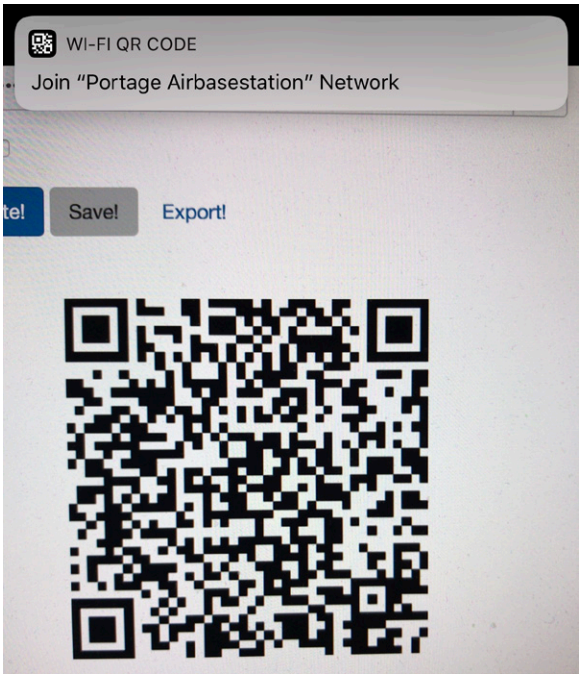


Figure 78: *Join a Wi-Fi network (or share one) via a QR Code. (Not my real password!)*

Connect to a Corporate or Academic Network

There are stronger ways to secure a network, and if you use an iOS device in corporate or academic settings, you will likely encounter WPA2 Enterprise. This flavor puts up a wall that lets you interact only in a limited fashion with the network to provide login details before your device is granted full access to the network and, typically, the Internet beyond.

WPA2 Enterprise networks are most frequently secured by a username and a password. However, a digital certificate (described below) can also be used for login. iOS supports these and other types of WPA2 Enterprise. Let's look at each option in more detail.

Username and password login

In the simplest setup, you must enter a username and a password provided by the network administrator or IT department to connect your device to a WPA2 Enterprise network. Often, these are the same creden-

tials you use for file service, email, and other network resource access, such as your email mailbox name (the part to the left of the @) or full address (`user@domain.com`) for that network.

To connect to a WPA2 Enterprise network of this sort, select the network, enter your username and password, and tap Join. It's that easy. If you get an error, check your entries. If they are correct, then contact network support: you won't be able to troubleshoot this any further, because there are no settings to tweak in iOS.

> ***WARNING!*** *Some networks may have policies that limit these sorts of logins to specific days and times, among other parameters. That's rare outside of high-security corporate networks, though.*

Certificate-based login

Some networks rely on digital certificates to handle logins. A digital certificate combines an encryption key with information that helps to validate the identity and integrity of that key. That is, the certificate lets a system make sure that the key hasn't been tampered with, and that it was created by the party that the certificate says created it. Digital certificates are used to provide a verified identity for server software, like a mail server, or for an individual.

In the case of WPA2 Enterprise, a certificate is used as an alternative to a username and login because the certificate can't be written down on a sticky note or extracted in some fashion.

Typically, an IT worker creates and provides you with a certificate and installs it for you. However, an iOS device can receive a certificate via email, and install it when you tap it as an attachment.

Outdated Methods

Wired Equivalent Privacy (WEP) was the first Wi-Fi security method, born in the same standard that unleashed Wi-Fi on the world (as 802.11b in 1999). But the standard had severe security compromises that were widely exploited.

As a result, since 2003, WEP hasn't been a reliable way to secure a network. Apple started phasing out WEP in iOS, macOS, and its base stations years ago, and it's unlikely you'd can connect to a WEP network today.

Plain WPA (not WPA2) replaced WEP, allowing hardware made as long ago as 1999 to upgrade one step, and some base stations are configured to handle older WPA and newer WPA2 at the same time, which I noted earlier should be avoided.

Viewing an Apple Base Station's Stored Passwords

If you've configured an Apple base station and can't recall or find the wireless password you set up, Apple's AirPort Utility software can reveal these in plain text so long as you have the administrative password that allows configuring the base station.

In iOS

1. Launch AirPort Utility. (It's a free app, if you don't already have it.)
2. Tap the base station in the graphical view.
3. If this is the first time you've used the app, or you opted on a previous use to not save the password and it's been a few minutes since the last time you entered it, the Enter Password link appears. Tap it, enter the password, and then tap OK.
4. Tap the Edit button and then go to Advanced > Show Passwords. The Show Passwords view displays the network password at top and then the base station password (which you had to know to get this far).

> **Note:** If you tap the network password, the WPA Pre-Shared Key is revealed. Wait…the what? It's the full underlying hexadecimal encryption key that your passphrase is converted into. I've never, ever had to enter this 64-character string into anything.

In macOS

1. Launch AirPort Utility (found in Applications/Utilities).
2. Select your base station and click Edit.

   An edit dialog appears in the main window.

3. From the Base Station menu, choose Show Passwords.
4. From the dialog that appears, write down or copy the text for the WPA Password (**Figure 79**).

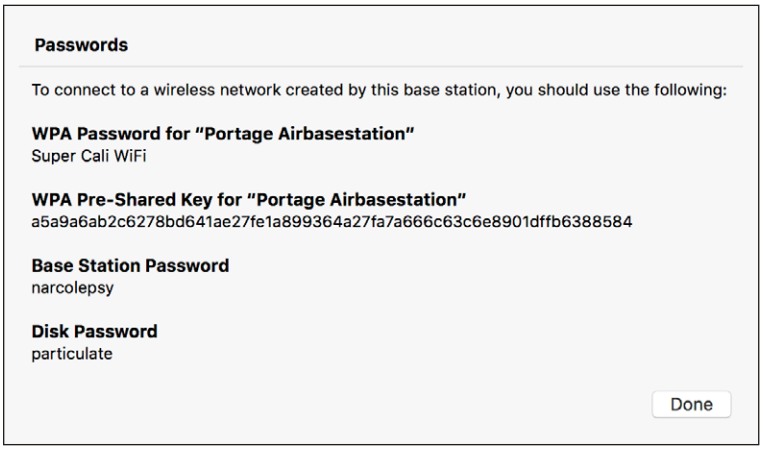


Figure 79: *The Equivalent Network Passwords dialog gives you the hex key value of a text network key.*

Now that you have the password, you can enter or paste it on your iOS device in order to join the Wi-Fi network. If logged into iCloud on both your Mac and the iOS devices, copying it on the Mac will put it into the iOS pasteboard.

Use Two-Factor Authentication

Apple's two-factor authentication 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 two-factor authentication, how to secure your extra pieces against discovery or loss, and how to reset an account.

Dancing a Two-Step

Apple lets you tie in an Apple ID for several purposes in iOS: for iCloud synchronization, 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, and 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 to use what Apple calls 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 physically—such as a phone, a smartcard, or other hardware—or something *you are*, like a fingerprint or personal characteristic. Usually there's an emergency backup, too: a one-time-use code or set of codes 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 iOS devices or Macs.

WARNING! *If you're running versions of macOS, iOS, watchOS, tvOS, or iTunes for Windows, you may have trouble using 2FA. See the complete compatibility list at Apple's 2FA FAQ.*

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.*

Apple Stepped Back from Two-Step

Apple had a previous two-factor approach that it called "two-step verification," which was stapled on top of existing software and systems. The two-step method was awkward, didn't allow confirmation via a Mac, and required using Apple's Apple ID site to manage.

Apple has allowed existing two-step users to keep the protection in place without upgrading to 2FA. However, that appears to be at an end. The moment you log into an iCloud account that uses two-step from any Mac with 10.13 High Sierra or any iOS 11 device, Apple upgrades your account to 2FA.

Turn On Two-Factor Authentication

You enable two-factor setup on your account through iOS or macOS by logging in using an account that's been approved for 2FA; by tapping an opt-in button through Settings > iCloud in iOS; or by clicking an opt-in button in macOS's iCloud preference pane in Account Details > Security.

WARNING! *Apple warns that you can't turn off 2FA after enabling it on "some accounts created in iOS 10.3 or macOS Sierra 10.12.4 and later." Apple ID accounts created earlier can all have 2FA disabled. Factor that in before turning it on.*

Enable Two-Factor

1. Go to Settings > iCloud > *account name* > Password & Security. You may be prompted to enter your password when you tap *account name*.
2. Tap Turn on Two-Factor Authentication and tap Continue.
3. You start by entering a phone number at which you can receive a text message or voice call; you can choose which (**Figure 80**).

   Select your country, enter your number, pick Text Message or Phone Call (to get an automated call speaking the code number), and tap Next. A code arrives. (If no code shows up, tap Didn't Get a Verification Code?, which lets you re-send it.)

   Tip: You can add additional trusted phone numbers later.

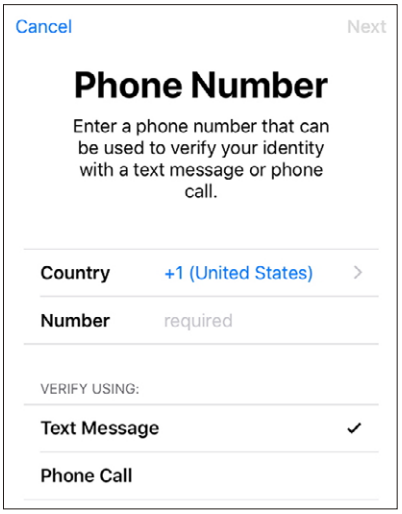


Figure 80: *The process starts with entering a phone number.*

4. Enter the verification code and setup is complete.

The Password & Security settings now show two-factor authentication set to On, and list your Trusted Phone Number (**Figure 81**). As you add phone numbers and devices, they appear here, as well as at the Apple ID web site. You can also remove trusted devices and phone numbers.

Figure 81: *iCloud settings show that two-factor authentication has been enabled.*

Disable Two-Factor

As noted earlier, Apple doesn't allow 2FA to be turned off on all accounts. And it removed an explanation in settings about how to disable it.

If 2FA isn't fitting your needs, and you want to try to turn it off, visit the **Apple ID site**, log in, click Edit next to Security, and then see if you have a link labeled Turn Off Two-Factor Authentication. If so, click it, choose new security questions, and click Continue. You'll be asked to confirm one last time, and then you're back to a password-only account.

Log In with Two-Factor Authentication

When you log in to iCloud in iOS or macOS, log in via a web browser, or attempt to purchase an item via iTunes, iBooks, or the App Store from a device that hasn't previously been used, you'll be prompted to validate your password-based login with a code sent to a trusted device.

When logging in via Settings > iCloud or the iCloud system preference pane, you're also simultaneously turning that iOS device or macOS com-

puter into a trusted device. For a web browser and iCloud.com, you can opt to trust the browser from then on (**Figure 82**).

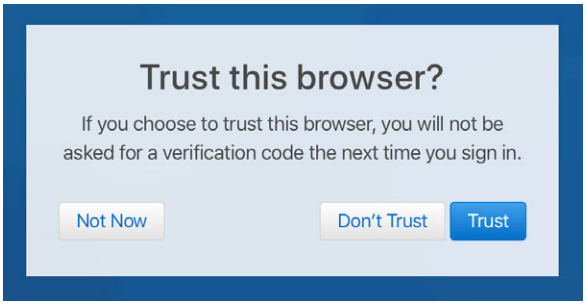


Figure 82: *Browsers can be trusted just like iOS devices and Macs.*

Note: Because macOS has separate user accounts, trusted device status is set for each user account individually. Each macOS user can log in to a different iCloud account.

Two-factor authentication presents itself in different ways in different places. In practice, you typically enter an account name (if not already filled in) and password, and then receive the code at all your trusted devices, which you then enter where prompted.

Let's say you're adding a Mac as a trusted device.

1. Open the iCloud system preference pane, and click Log In.
2. Enter your user name and password.
3. At all your other devices, you're prompted with an Apple ID Sign In alert, which shows the account name, the nearest city, and a zoomed-out map, along with Don't Allow and Allow buttons (**Figure 83**). Click Allow.

   If you click Don't Allow by accident, you can obtain a new verification code in iOS (iCloud's Password & Security) or macOS (the Security tab in the iCloud account settings). Click or tap Get Verification Code.

WARNING! *If you choose Don't Allow, the remote login can't proceed, and Apple prompts you with a warning where you chose that option. It says, "If you think someone is trying to sign in to your account, you should change your password."*

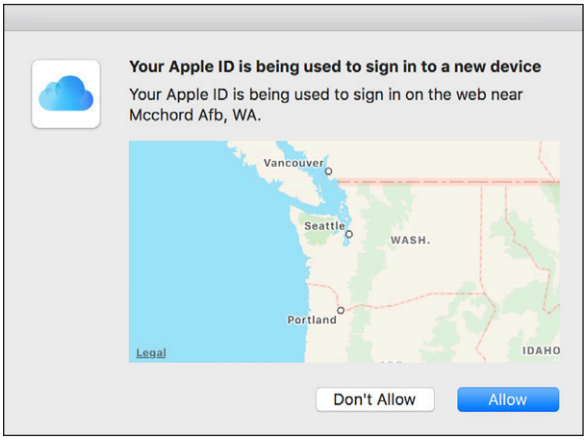


Figure 83: *To avoid unwanted logins, you're shown a geographic alert. It might not be that accurate—I'm many miles from McChord Air Force Base.*

4. On the device from which you clicked Allow, a Verification Code alert appears. Enter the verification code on the requesting device. If entered correctly, access is approved—in this case, the Mac is now trusted.
5. Tap OK or click Done on the trusted device on which you clicked Allow.

If you don't have access to a trusted device at the time at which you want to log in, you can use a trusted phone. Follow these steps instead:

1. Open the iCloud system preference pane, and click Log In.
2. Enter your user name and password.
3. On the requesting device or browser, click Don't Have Access to Trusted Devices.
4. From the Verify Your Identity dialog, select a phone number if you have more than one, and then choose Text Message or Phone Call, before clicking Continue (**Figure 84**).
5. Enter the number you receive via text or by automated voice call into the requesting device or software, and you're done.

Add a Trusted Phone Number

Trusted phone numbers can be added via iOS, macOS, or the Apple ID site.

- macOS: Open the iCloud system preference pane, click Account Details, click the Security tab, and click the + (**Figure 85**).

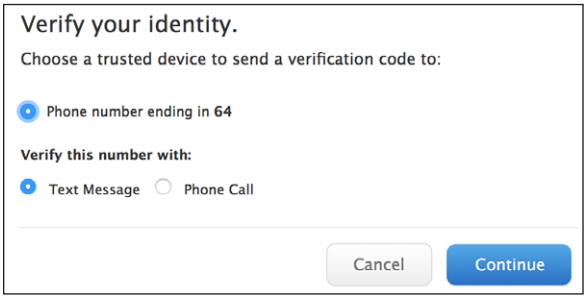


Figure 84: *You can opt to use a phone number instead of a trusted device.*

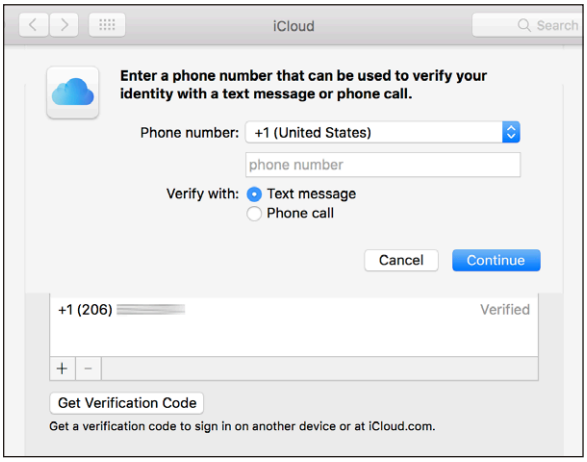


Figure 85: *Trusted phone numbers can be managed in several places, including macOS.*

- iOS: Go to Settings > *account name* > Passwords & Security, tap Edit next to Trusted Phone numbers, and then tap Add a Trusted Phone Number.
- Apple ID site: In the Security section, click Edit at the far right, and then click Add Trusted Phone Number.

  In each location, you enter a phone number, choose whether to send a text message or receive a phone call, and then enter the verification code.

  If you don't get the verification code immediately, you can go to any of the above configuration locations and click Verify to try again.

WARNING! *SMS Forwarding, part of Continuity, forwards text messages to macOS and iOS devices, including security codes. If you have any concerns about someone having access to your Mac, disable SMS Forwarding.*

Manage Your Notification Email

In addition to the email associated with an Apple ID, you can have a notification email that's used for critical messages, and that will aid you if you need to unlock or recover a two-factor account.

You have to use the **Apple ID site** to change this address or remove it. After logging in to your account:

1. In the Account section, click the Edit button at far right.
2. Under Notification Email, click Change Email Address.
3. Enter an email address and click Continue.
4. Apple will send you an email with the six-digit verification code. Check your email, and then enter that code and click Verify.

   You can later remove this address by returning to the same location, clicking Edit, and clicking the X next to the address.

Logins at Other Sites

Because calendar events, contacts, and email can be used with non-Apple software, Apple lets you create special *app-specific passwords* for use with third-party apps. You can generate up to 25 app-specific passwords via the **Apple ID site**.

> ***WARNING!*** *App-specific passwords bypass two-factor protection and, if recovered, could be used to access contacts, calendars, and email.*

1. Enter your Apple ID and password, and click Sign In.
2. Enter the verification code that appears on other devices.
3. In the Security section, click Edit at far right.
4. Under App-Specific Passwords, for each password you need to create:
   a. click Generate Password.
   b. Enter a label that helps you remember for what purpose you created the password and click Create.

c. Copy the password that appears and paste it into the software with which you need to use it (**Figure 86**).

d. Click Done.

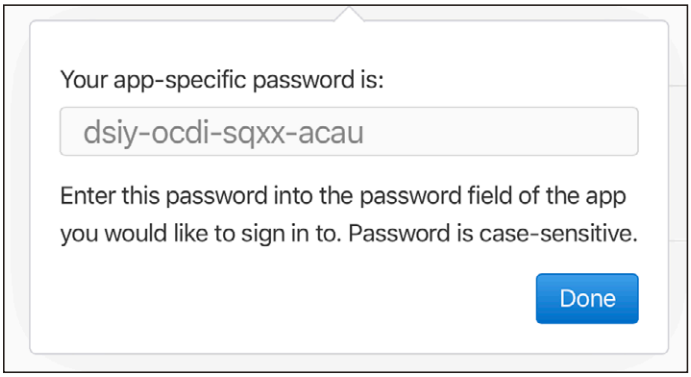


Figure 86: *I can show you this password because I immediately revoked it.*

If you ever want to revoke an app-specific password, return to the Security section, click Edit, and then click View History. If you've lost track of which passwords are used for which services (even with your labels), the date and time created appear next to each. You can click an X next to each one to revoke it, or you can click Revoke All to start over.

Tip: These app-specific passwords can't be recovered. If you can't recall one, just generate a new one and revoke the old one.

Remove a Trusted Device or Phone Number

When your device is sold, given away, lost, or stolen, you need to uncouple it from your account. The same is true when you stop using a given phone number or lose access to it.

Remove a Trusted Device

You can remove a trusted device via iOS, macOS, or the Apple ID site. Here are the instructions for iOS:

1. Tap Settings > *account name* and swipe up (**Figure 87**).

2. Tap a device.
3. Tap Remove From Account.
4. At the prompt, tap Remove to complete.

You can add a device back by logging in to iCloud on that device. It will then rejoin the set of trusted devices.

Figure 87: *All trusted devices are listed wherever you can log in to examine the details of your Apple ID account.*

Remove a Trusted Phone Number

Trusted phone numbers can be removed from iOS, macOS, or the Apple ID site.

In iOS:

1. Tap Settings > *account name* > Password & Security.
2. Next to Trusted Phone Numbers, tap Edit.
3. Next to a phone number you want to remove, tap the red remove icon.
4. Tap the Delete button that's revealed.
5. Tap Done.

In macOS:

1. Open the iCloud system preference pane.
2. Click Account Details.
3. Click the Security tab.
4. From the phone number list, select one and click the – button.

Recovering Account and Access

So you need two factors to log in: a password and a verification code. But what happens if you forget your password or you lose access to your trusted phone numbers and devices? Apple has responses for each.

> ***WARNING!*** *Apple used to let you easily reset your password with a trusted phone number, but now buries that option.*

Reset Your Password with a Trusted Device

You can reset your password from any trusted device without having the password. Follow these steps in iOS (must be iOS 10 or later):

1. Tap Settings > *account name* > Passw ord & Security > Change Password.
2. Enter your passcode and tap Done.
3. Enter a new password and type it again in the Verify field.
4. Tap Change.

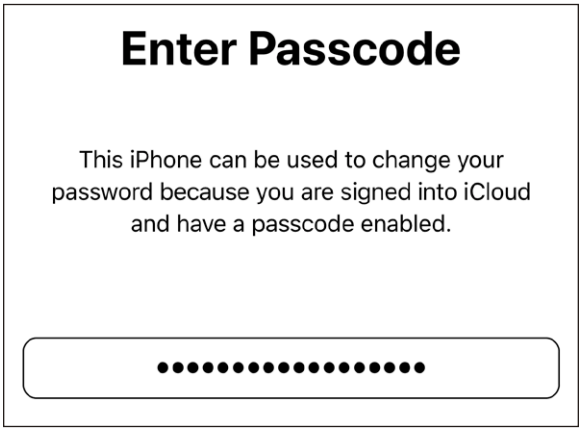


Figure 88: *You can reset your Apple ID password via a logged-in iOS device.*

On a Mac, you follow a fairly different process, because it forks:

1. Open the iCloud system preference pane and click Account Details.
2. If you are prompted to enter your password, click Forgot Password and then click Reset Password.

If you are not prompted to enter your password, click the Security tab and then click Change Password.

3. Enter your macOS username and password and click OK.
4. Enter your new password and then enter it again in the Verify field.
5. Click OK.

Recover via Find My iPhone with a Phone Number

If you can't access a trusted device—say they were all lost in a fire or stolen—you can use Find My iPhone from another iOS device to try to reset your password using a code sent to a trusted phone number.

1. Launch Find My iPhone. (If logged in, tap Sign Out.)
2. Enter your email address in the Apple ID field and then tap Forgot Apple ID or Password? You can also leave it blank and enter your email address on the next screen.
3. Depending on what you entered, you will see one of three screens:
   - Enter Passcode. This shouldn't appear, because it means you're logged into a trusted device! If so, you're good: enter your device passcode and you can reset your password.
   - Forgot Password? Tap Next to continue. You should be prompted to enter in full one of your trusted phone numbers, tap Next, and then tap Reset with Phone Number, which sends a verification code.
   - Recovery Key. If you had a Recovery Key set (described next), you can use it here.

If you can't complete any of these operations, proceed to Lost All Trusted Devices, which explains how to use account recovery.

Use a Recovery Key in Limited Cases

If you were using two-step verification and then upgraded to iOS 11 or High Sierra, Apple upgrades your account security to 2FA. It also offers you one unique additional option to reset your password.

The two-step method had a last-ditch account reset option that required a uniquely generated Recovery Key. The 2FA system doesn't use it, but

folks who were automatically upgraded have the option of creating a fresh Recovery Key. However, if you create a Recovery Key, Apple disables all other recovery methods, including the last-ditch one described next. Consider that tradeoff.

To generate a Recovery Key in iOS, go to Settings > *account name* > Password & Security and tap Recovery Key. On a Mac, go to the iCloud system preference pane, click Account Details, and click Security. Then click Turn On in the Recovery key section. Follow the steps in both places to complete the process.

> ***WARNING!*** *Do not lose your Recovery Key. It's really the only way after it's enabled to regain access to your account if you lose access to all your trusted devices.*

Lost All Trusted Devices

Apple offers one last-ditch effort to come back from the brink of despair, in which you have no access to trusted devices or phone numbers. It calls this *account recovery*. It warns that it could take several days or longer to get you back into your account, as it uses a combination of information it requires from you and time to dissaude people trying to hack your account from succeeding.

You can start account recovery from an iOS device or on a Mac that you use, or you can use Find My iPhone on anyone's iOS device.

- In iOS, the device has to be signed out.
  1. Go to Settings > Sign into your iDevice.
  b. Tap Don't Have an Apple ID or Forgot It.
  c. Tap Forgot Apple ID.
  d. Enter your Apple ID and tap Next.
  e. The next instructions vary depending on what access you still have.
- In macOS, you also need to be logged out.
  1. In the iCloud system preference pane, click Forgot Apple ID or Password.

2. Enter your Apple ID and click Continue.
3. Fill in a trusted phone number and click Continue.
4. The next instructions vary depending on what access you still have.

- In Find My iPhone, follow the steps earlier for *Recover via Find My iPhone with a Phone Number*.
  1. In Step 3, for Forgot Password?, after entering a trusted phone number, tap Don't Have Access To Your Trusted Number?
  2. Tap Start Account Recovery.
  3. Instructions now vary—follow them!

  Once you initiate account recovery, here's what happens:

- Apple sends an email confirming that the process has started, and tells you when it expects to be completed.
- You can go to iforgot.apple.com and check on progress. You might be prompted to enter your credit-card details for the account, which can shorten the recovery period.
- If you remember your Apple ID and password and log in anywhere, or you regain access to a trusted device that's already logged in, account recovery cancels atuomatically.

Transfer Data Securely

The data that travels to and from your iOS device 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.

Encrypting our data in transit enables us to make decisions about how our data is being used and who sees it, preventing criminals, relatives, and government agencies from overstepping our rights.

In this chapter, I help you understand what's encrypted and what's not, and how to secure individual services and your whole network connection.

TLS and SSL and what they mean: *You'll read the term TLS (Transport Layer Security) a number of times in this chapter. It's a way of securing a connection for both ends with strong encryption. TLS is a successor to SSL (Secure Sockets Layer), and when both older and newer protocols were used side by side, you'd see SSL/TLS or TLS/SSL as a label. However, SSL is now considered definitively broken from an encryption standpoint, so it's important to look for TLS only.*

Protect Particular Services

Nearly every kind of service you can think of offers an encrypted option, and, fortunately, most modern services employ some kind of encryption by default. Here's a laundry list of what you should consider:

- Email. There's no good reason not to employ TLS. If your mail host doesn't provide secured email for your incoming email (POP or IMAP; almost always IMAP in iOS) and for your outgoing email (SMTP), find a new host. Without security, email programs may send passwords in the clear or with weak encryption, and likely send all data in the clear. iOS will always attempt to configure your mail settings securely.
- Secure access to web sites. A huge movement in the last couple of years has shifted a large percentage of all web sites to use secured connections for all requests, not just for commerce or banking.
  - If you're not sure a connection is secure, look in the security settings for a web site where it notes something like "Always use https" or "Always use secure connection" and check that box. (A login is almost always secure, so your account name and password is rarely at risk.)
  - For other web sites, try to always use the secured flavor by typing in or bookmarking `https` instead of `http` as the start of the URL. Many sites offer TLS sessions as an option reachable just by entering the URL in this fashion.
- Transfer files securely. When making an FTP connection, use only a secured alternative to plain FTP, such as the SSH-based SFTP or one of several TLS-protected methods. FTP programs otherwise send passwords and data in the clear. **Transmit for iOS** is the app of choice for secure file transfer ($9.99).

> **Tip:** On a Mac, enable Remote Login and File Sharing in the Sharing preference pane to allow SFTP over a local network or via the remote Back to My Mac service.

What's protected without any extra effort?

- iMessage and FaceTime. Apple builds in end-to-end encryption in such a way that even the company can't decipher your messages. In fact, it's so secure, governments around the world—including both the U.S. and China—aren't happy about it.
- Other instant-messaging and audio/video chat services have various levels of protection. Signal from Whisper Systems is the best. Whatsapp from Facebook can be configured and used very securely.
- Apple started upping the requirements to use secured connections in iOS apps for nearly everything in iOS 9. But you can't easily check. And

developers can include exemptions to access services that aren't yet available in encrypted form or that use older security protocols. Apple will likely clamp down on that over time.

Umbrella Protection with a VPN

A virtual private network connection is a nifty way to prevent any sniffing of your local network hookup. A VPN encrypts all the data coming from and going to a device—such as an iPad or iPhone—creating an encrypted tunnel that extends between the device and a VPN server somewhere else on the Internet. This lets your information traverse any local network and hubs with protection as well as every node on the Internet between the two points.

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.

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 a "VPN for hire," letting you pay for a fixed period of time or a recurring subscription. The connection you make, as noted above, runs from your iOS device through the local Wi-Fi or cellu-

lar network, then goes through any intervening local area network routers and higher-level backbone routers, and finally winds up at one of the company's VPN servers located in a data center.

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.

I start with trying to find a reputable company, rather than seeing what features are offered in a VPN app, which are mostly comparable, or comparing pricing. Follow links from a company's App Store listing and then research the firm to see how long they've been in business, whether their reviews and Facebook page are riddled with negative comments and reviews, and how easy it is to find their technical support.

Wirecutter looked into providing a recommendation for a specific service, and gave up, but several computing and mobile magazines and sites have run products through their paces and checked privacy policies. If you're looking for reviews, avoid sites named something like TopBestThings or TheBestVPNApp—these are typically paid-placement sites masquerading as offering reviews. Instead, go to PCWorld, PC Mag, Ars Technica, or other sites.

I'll provide a single recommendation, because I've used the service off and on: **Encrypt.me** (known as Cloak before it was acquired). Encrypt.me is run by an established company, has good pricing, and routinely updates and improves its app. I'll use Encrypt.me as an example in the rest of this chapter.

Set up a VPN app

To get set up in iOS, you download a service's app. Most apps offer a free trial period. On first launching a VPN, during the setup process for creating an account, you will be asked at some point to add a VPN configuration that includes all the server and connection details required. This is nice because you don't need to deal with the fiddly bits described in the manual setup section below. And if the profile needs to be updated because the service's details change, they can push a fresh one through their update, rather than asking you to reconfigure by hand.

1. Launch the app, which will detect during setup that no profile is available and request to install it (**Figure 89**).
2. Tap Allow.
3. Enter your passcode or use Touch ID or Face ID when prompted in the Settings app.

   The profile is installed and you're returned to the app.

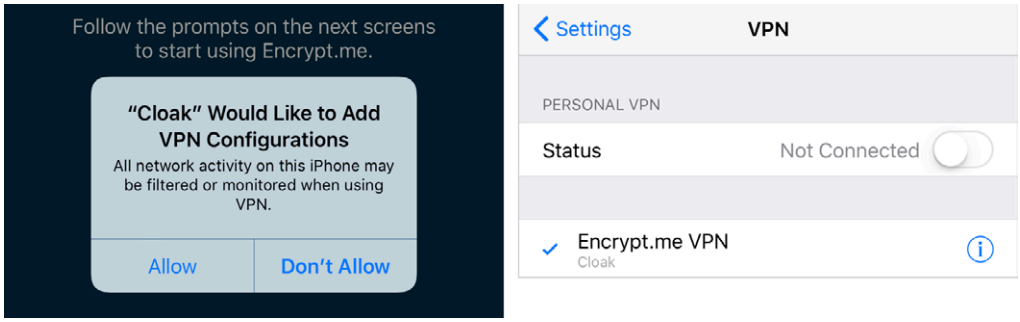


Figure 89: *Launch the app, and you're prompted to add a VPN configuration (left); on devices with Touch ID or Face ID, you use that method to approve.*

After installing a profile, you can use the app or Settings > VPN to start or end a connection. A VPN label will appear in the status whenever the connection is active. You can find more information about these options in **Make a VPN Connection**.

VPN services like Encrypt.me can initiate a VPN connection "on demand," too: go to Settings > VPN, tap the info ⓘ button, and then turn the Connect on Demand switch on. However, it's usually better to set up connection defaults in the app.

Encrypt.me lets you set it to connect automatically when you join Wi-Fi networks, as well as pick trusted Wi-Fi networks to bypass. You can also choose to trust or distrust the cellular connection by default: when trusted, the VPN won't engage when you switch from Wi-Fi to cellular; untrusted, and it always engages.

Country-hopping with a VPN

There's one more trick up the sleeve of VPNs: they can let you seem to be accessing a service from a country other than the one that you currently occupy. This can be handy when you want to access a service as if

you are in the same country as the one in which the service operates, or when you might distrust the Internet infrastructure of an ISP, cellular network, or entire country that you're in. (This isn't a joke: many countries routinely monitor and suck down data that's sent, in the clear and otherwise.)

It used to be useful as well to evade certain per-country licensing limitations on free and subscription online video streaming and other services. These services started tightening requirements in 2016, and it's now very difficult to bypass them with these workarounds. Further, BBC iPlayer, free to those paying a television license in the United Kingdom, will soon start requiring a login in addition to a UK network address.

Finally, you can pick a part of the United States with some services, which you use to reduce latency. While VPN services try to pick the closest "topological" location—the data center on the Internet the fewest hops and shortest latency from where you are—you might want to force the matter by picking San Francisco or Miami.

In Encrypt.me, you tap a location icon in the lower left, pick a location from its Transport menu, then click Done. The next time you connect, the app will try to route you through that country or region.

Pricing options for VPN apps

Every VPN service is paying not just for servers and the overhead of staff and the like, but for the bandwidth you consume as well: every gigabyte you send through a VPN is one gigabyte inbound and outbound, and that has to be paid for somehow. Some users will consume 500 GB a month; others, a trickle.

As a result, plans may seem expensive, but they're typically priced very reasonably relative to both the value and the hard costs the company has to pay to keep its software and security up to date. If you want to use a VPN on multiple devices, especially an iPhone plus a laptop, find a plan that lets you use the same service across an app and a desktop client.

Encrypt.me's pricing at this writing is reasonable and typical: $10 a month ($100/year) for unlimited use across all devices as either a subscription or a non-renewing pass; a $3/month mini plan with 5GB maximum usage; and a non-renewing unlimited week pass for $4.

Configure a VPN Manually

There are several kinds of VPN protocols, and iOS supports the most popular: IKEv2, L2TP/IPsec (listed as L2TP), and Cisco IPsec (listed as IPsec). The first two are generic, widely used standards. The last is a Cisco VPN flavor proprietary to its systems. Other corporate standards can be provided via VPN apps.

> **Note:** Apple long supported PPTP, but dropped it for security reasons: it's too easily broken and has no advantages over newer VPN flavors.

Almost any server operating system that offers VPN software at all can support one of these protocols, including macOS Server and Microsoft Windows Server.

Set up a VPN profile

Start by making sure you have all the server settings provided by your VPN host or network administrator at hand, since you'll need to enter several pieces of data.

To set up a VPN profile, follow these steps:

1. Launch the Settings app, and tap General > VPN. (If you've configured a VPN before, it may show up in the top level of Settings.)
2. Tap Add VPN Configuration. The Add Configuration view appear.
3. In the Add Configuration view, tap Type if the default IKEv2 isn't what you want. L2TP, PPTP, and IPsec are also available. The choice here affects which options appear for configuration.
4. Then, fill in the settings:
   - The description appears in the VPN view after you create the configuration; enter something short and expository.
   - Server (all), and Account and Password (all but IKEv2) tell iOS which Internet host to connect to using which credentials.
   - Remote ID is exclusive to IKEv2 and required; Local ID is also part of IKEv2, and required.
   - RSA SecurID (L2TP and PPTP) should always be off unless your employer provided you with a physical key fob.

- Secret (L2TP and IPsec) is a shared bit of text that's used as an extra level of security.
- Use Certificate (IPsec only) is enabled when you have a stored certificate to validate your identity.
- User Authentication (IKEv2 only) can be set to Username, in which case Username and Password appear; or to Certificate, and then a certificate needs to be selected.
- Group Name (IPsec only) is set if a network admin provides a group.
- Encryption Level (PPTP only) is typically left set to Auto.
- Send All Traffic (L2TP and PPTP) is typically left on. If it is off, you can filter which traffic is not encrypted and which is.
- A Proxy option can be ignored unless you've been told otherwise.

5. Tap Save.

   You now have a configuration profile that you can use.

Make a VPN Connection

Go to Settings and tap the VPN switch to connect using the configured VPN profile. If there's more than one VPN profile, the one that's used will have a checkmark next to it. (In some cases, you may see VPN Configurations and Personal VPN as separate lists, each of which will have a separate switch for enabling and disabling.) Good VPN apps will also let you enable the connection in the app.

> ***WARNING!*** *VPNs can be disrupted when you move between networks. If this happens to you, toggle VPN on to off to on to reset the connection.*

You can tell that a VPN connection is active in two ways:

- A VPN indicator appears in the status bar.
- A Status entry appears in the Settings app that reads Connected.

To get more information about the status of your VPN connection, tap the info ⓘ button to the right of the currently active VPN configuration profile in Settings > VPN. This provides a variety of technical details (**Figure**

90). The Server IP Address field provides a clue to the facility at which your VPN terminates. You can also switch on or off Connect On Demand in this view.

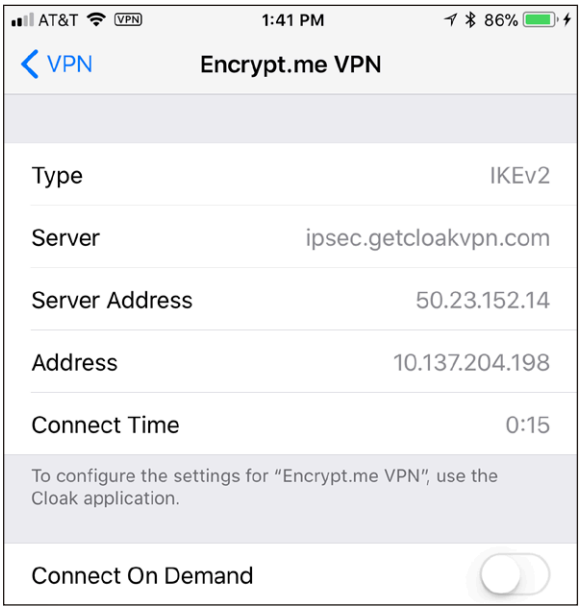


Figure 90: *Connection details reveal where the VPN terminates.*

You can cancel a VPN connection in process (before the connection is completed) by tapping the Cancel VPN Connection button that appears in the VPN view. To turn off a VPN connection, set VPN to off in Settings > VPN; or use the app, when that's an option.

Protect Your Device

Now that you know how to keep your data from being intercepted in transit, how can you prevent your stored data—on an iOS device—from being rifled if your device is out of your control?

Apple has three robust ways to secure a device: with a passcode; for newer hardware, its Touch ID fingerprint-recognition system; and Face ID, which is exclusive to the iPhone X as of late 2017.

All devices that support iOS 8 and later include 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 91**).

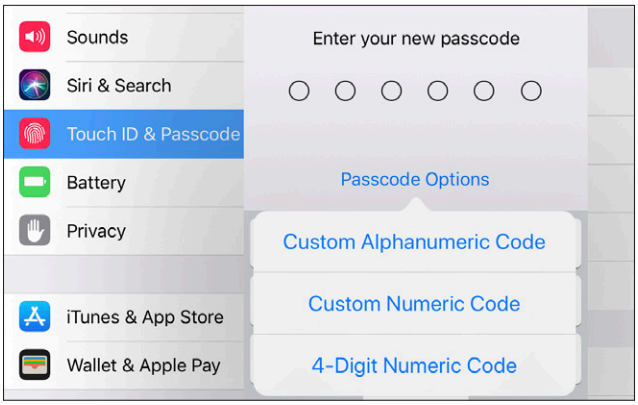


Figure 91: *You can opt for a more complicated or shorter passcode.*

> ***WARNING:*** *Many iOS 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.*

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 Passcode Lock screen offers a few additional security options. You can set the time after which you must enter a passcode at intervals from Immediately to After 4 Hours:

- Immediately means you're asked for the passcode any time the device wakes up. You can put your handheld to sleep manually, of course, by pressing the Sleep/Wake switch, but you can also set it to sleep automatically, with the Settings > General > Auto-Lock. This is the only option for Touch ID and Face ID.
- Longer intervals let the device be unlocked without a passcode for up to the time duration you've chosen from the list.

You can also set which services are available when your device is locked in this view, which is a good way to prevent leakage of information, such as appointments, being able to present barcodes for scanning at stores or an airport, or using Messages to reply.

As a nuclear option, you can set your device to self-destruct—destroy its data, at least—if there are more than ten failed attempts to enter the passcode correctly by switching on Erase Data. What do you lose? Only items created since the last backup and sync; see **Erase Device**.

When a Passcode Is Required

Apple wants to make sure that someone can't easily coerce you to unlock your phone with your finger or your face, and that you will remember your passcode by requiring it at frequent-enough intervals it won't disappear from your brain.

You will be prompted to enter the passcode in a number of circumstances:

- After your iOS device has been powered up or restarted.
- If you haven't unlocked your device with Touch ID or Face ID in more than 48 hours.
- Once five unsuccessful attempts have been made to unlock your phone or tablet via Touch ID or Face ID.
- If you've put the device into Lost Mode via Find My iPhone. (If you didn't set a passcode, you set one to enable Lost Mode.)
- As an extra memory aid, after six and a half days, iOS goes into an four-hour timer mode. If you haven't unlocked with Face ID or Touch ID in that period, the next time you unlock, you're prompted for your passcode.

Turning on a Passcode for Safety

There will be times when you will want to revert to a passcode instead of Touch ID or Face ID for personal safety, for extra security, or in certain legal situations. In the United States, while the law isn't yet fully established, it appears that in criminal proceedings, the government can compel the use of a fingerprint but can't compel you to give up your password.

If you want to force iOS to disable Touch ID or Face ID, you can:

- Use Settings: turn off iPhone/iPad Unlock, Apple Pay, and iTunes & App Store, and then you're prompted that Touch ID or Face ID will be disabled.
- Power down your device. On restart, it's disabled.
- Starting in iOS 11, five presses in a row of the Wake/Standby button lets you make an emergency call, but also disables Touch ID and Face ID.
- With an iPhone 8, 8 Plus, or X holding down either volume button and the Wake/Standby button disables Touch ID and Face ID, while bringing up the Slide To Power Down option. On earlier phones, it just brings up the power-down slider.
- Make five bad login attempts with your finger or face.

Use a Biometric Login

Biometrics refers to using some part of yourself that can be uniquely identified to authenticate that you should have access. That includes fingerprints with Touch ID and, starting with the iPhone X, your face with Fade ID. Both methods share a lot in common.

> ***WARNING:*** *When using biometric ID, remember that although it increases the relative security of your data while improving the speed and simplicity of use, you also open yourself up to your device being unlocked via coercion. If someone—a government agent, criminal, abusive spouse, etc.—can force your finger onto a Touch ID sensor or force you to look attentively into an iPhone X, they can gain access to some of your information.*

Touch ID and Face ID unlock your phone and also authorize Apple Pay payments, make iTunes purchases, and make App Store and in-app purchases. Third parties can also tie into both to unlock themselves or allow a login, such as with banking and password apps.

Now let's look at how you set up and use both kinds of biometric ID.

Use Touch ID

Apple's Touch ID lets you turn to your fingertips to secure your device, training your iPhone or iPad on equipped models to recognize up to five fingerprints.

You select which of the Touch ID associations you want in Settings > Touch ID & Passcode and then tap Add a Fingerprint. iOS guides you through enrolling a fingerprint. When it's finished, it names the entry Finger plus a number. As this isn't descriptive, tap that entry, then name it with something you remember. In that way, if iOS "forgets" your fingerprint, you can delete the appropriate entry and retrain it.

Touch ID allows fingers from different people, which is convenient, as you and others could all use Touch ID to unlock the same phone or tablet, or you could enroll a partner's fingerprint as an emergency fallback if they need to access your device.

Note: Matthew Green, a well-known security researcher, **tweeted this cautionary tale** in November 2014: "I woke this morning to find my 7 y/o levering my finger onto the Touch ID sensor of my phone. Maybe time to go back to passwords."

Use Face ID

Face ID uses an infrared laser and sensor to project and measure 30,000 separate data points on a person's face to create a profile while also capturing other flat views. Subsequent logins repeat those tasks and add randomization to compare to the stored profile and defeat face forgery.

For the initial release and for the foreseeable future—based on Apple's public statements—only the iPhone X will offer Face ID *and* only one face can be enrolled.

Enrollment uses a similar process to Touch ID: you use Settings > Face ID & Passcode, and choose Enroll Face. The process has you move your head in a circle framed onscreen, until enough information has been gathered.

Apple says it tracks and retains temporary updates when it finds a good match that falls outside its ideal parameters. These temporary updates are good for only a "finite" number of unlocks, which is a little vague. Maybe it's to cope with temporary clothing choices or eyebrow plucking? A change in glasses? It's also unclear at what poiint you'll have to re-enroll your face, though that process is far less tedious than Touch ID, so it may not feel like as big a deal in practice.

Face ID relies on an "attentive" expression when you log in. This prevents unlocking the phone when you're just glancing past the lock screen, and it requires someone to have their eyes open. Apple says you can unlock wearing sunglasses. The emitters and sensors are designed to be used in all lighting conditions, indoors and outdoors.

Early users report Face ID being delightful, as you merely raise the phone to wake it and while glancing attentively, the phone unlocks. It apparently feels seamless.

With Apple Pay in a store, you have to invoke the Wallet before tapping: double-click the side button, glance, and then tap to pay.

Although I recommend setting a strong passcode, you may wind up entering your passcode more frequently with Face ID than with Touch ID for a few reasons:

- Face ID is good but not perfect, especially in situations with bright light.
- Some models of sunglasses and some brands of sunglasses use optical filters that apparently prevent a good or reliable match.
- When the sensors can't perform as exact a match as required, they defer to the passcode. This appears to happen routinely but not constantly.
- You cannot use Face ID to confirm an Ask to Buy request, used for parents or guardians to approve children's purchase requests in iOS. While Touch ID may be used, with an iPhone X, only a passcode works at this writing.

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.

Find My iPhone (and Other Devices)

Find My iPhone has a name that belies its utility: it works with every kind of iOS device, the Apple Watch, AirPods—and with Macs, too (as Find My Mac in the iCloud preference pane).

You can find the last reported position of any iOS device or Mac by enabling the feature, which requires an iCloud account. You can also play a sound on the device, lock the device or mark it lost, or delete all its data!

Finding a device's current location and taking a remote action can be accomplished via the iCloud web site or the free **Find My iPhone** app.

> ***One name for clarity:*** *For simplicity's sake in the text ahead, I'm calling the service Find My iPhone.*

With Family Sharing turned on, anyone in the family 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 iPhone features are available through other Family Sharing members' accounts.

Note: The four major 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.

How It Works

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 iOS devices and Macs running 10.7 Lion or later use the built-in Wi-Fi; iPhones and cellular iPads add cellular radios and GPS.

With Find My iPhone active, a device with GPS and cellular regularly sends updates 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.

All iOS (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. This system approximates a position based on network details that it knows about from previous scans sent by other devices, including the name and some less-apparent unique hardware identifiers. The position is inferred based on the relative signal strength of the Wi-Fi base stations detected.

That lookup requires an active connection, which is fine for a cellular device with an active cellular data plan. But a Wi-Fi–only device must be connected to a Wi-Fi network to retrieve and send Wi-Fi–based position information, as well as to respond to queries from Apple's servers.

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.

Enable Find My iPhone

Find My iPhone requires an active Apple ID associated with iCloud. You likely set this up when upgrading or setting up your iOS device or Mac.

To enable Find My iPhone on an iOS device, if you haven't logged in with an Apple ID account yet, go to Settings > iCloud and do so. Once you're logged in, that view shows the Find My iPhone switch, which you can set to On or Off.

> ***WARNING:*** *Apple added a feature a few releases ago called Activation Lock that prevents your iOS device from being erased and then used by someone else. An erased, locked phone requires the passcode of the device to proceed. You can disable this by entering your iCloud password to disable Find My iPhone before erasing. However, it obviously also disables tracking.*

> **Note:** To enable Find My Mac, enable the Find My Mac checkbox in the iCloud system preference pane. If your Mac has Wi-Fi turned off with an active Internet connection (such as cabled Ethernet), it can still be contacted to perform actions, but it probably won't display a location.

View Your Device's Location

To view your device's location, you can choose between two similar tools: the Find My iPhone web app on the iCloud site or the Find My iPhone app on an iOS device. Because the two options have nearly identical interfaces and features, you should use whichever one is easier for you to access.

> ***Lost a second factor, too?*** *Apple lets you use Find My iPhone with an account with two-factor authentication enabled even if you can't access a second factor to log in—say, all your devices were stolen! At iCloud.com, after entering your account name and password, you'll see Find My iPhone as an option below the area to enter a six-digit 2FA code. This is also a security loophole, as I describe later in this chapter.*

Find My iPhone on the web

To find your devices via a web browser, follow these steps:

1. Go to **https://icloud.com/#find**.
2. Log in with the correct Apple ID.
3. Select one of your devices from the All Devices menu (**Figure 92**).

> ***Apple is smart about unattended machines:*** *iCloud.com allows you to stay logged in, but prevents unauthorized access to Find My iPhone by asking for a password even when you're already logged in to another part of the site. The Find My iPhone login times out after 15 minutes.*

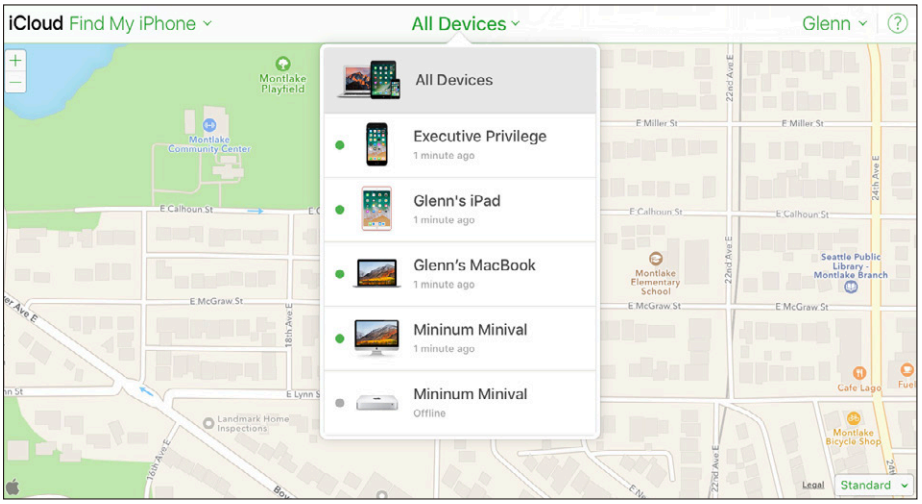


Figure 92: *The Find My iPhone web app shows devices in a drop-down list at center and their locations on a map.*

In the All Devices list, the dot beside each device name indicates the status: gray ● means trying to connect or offline. With AirPods, they also have to be out of their case and near any of your iOS devices. A device offline for more than 24 hours displays as Offline.

A green ● means online, and it shows the last time it was located. AirPods show the location of only one of the earbuds at a time. It may take Find My iPhone up to 3 minutes to fix a precise location for a device.

> ***Battery life:*** *The web and iOS app show the battery life remaining on hardware with batteries, including setting the icon green if it's charging.*

Find My iPhone shows the location of the device on the map as a green dot. For GPS-enabled devices that have obtained a strong location fix, only the dot is shown.

When the GPS information isn't good or it's a device without a GPS, the green dot is surrounded by a green outline, the radius of which indicates the amount of confidence in the location (**Figure 93**). With hardware that relies on a GPS signal, the outline may appear briefly while a better fix is being obtained.

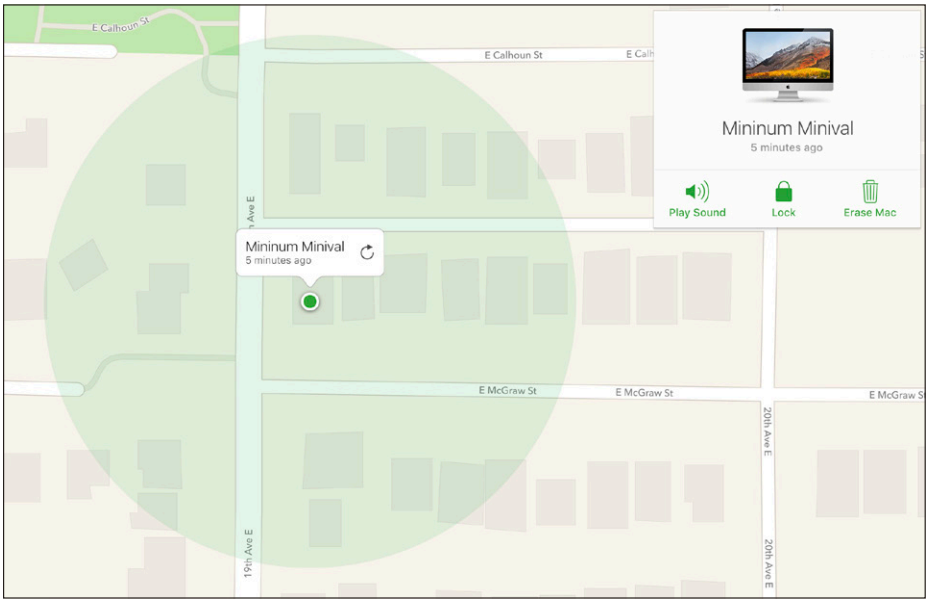


Figure 93: *The shaded green circle shows the degree of confidence. In this case, my MacBook Air might be half a block away (though the green dot is just one house off).*

With All Devices chosen, click the All Devices label or click anywhere on the map to hide the drop-down, and then click any green dot on the map. A popover menu appears with options for actions, described a few paragraphs ahead, and the last time a fix was made on the location.

If the device was previously found but can't be found now, you may get a message that says, "Your device is no longer locatable." The last-known location of the device should be displayed for 24 hours, along with the time showing the last moment it was known to be located there. Clicking the green dot on the map representing the device brings up a popover with a Refresh button you can click to force another attempt to locate it.

Find My iPhone app

You don't have to use a web site to run Find My iPhone. Instead, you can download the free **Find My iPhone** app to an iOS device, launch it, and then enter your account and password. (It's labeled "Find iPhone" in iOS search and on the Home screen.) The app works almost identically to the Find My iPhone web app, although its interface layout is a little different when a device is selected.

The default view shows all devices in a list at the bottom (**Figure 94**) and their locations in a map shrunk to fit them all at the top. Tap any device in the list, and it's selected and zoomed in on in the map (**Figure 95, left**). Tap the All button at the upper left to return to the full device list.

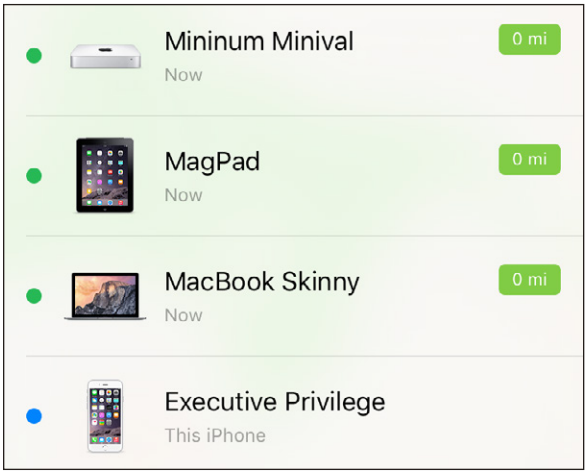


Figure 94: *The Find My iPhone app shows all your connected devices in a list (as well as plotted on a map, not shown).*

Tap the device in its green circle, and three options appear at the bottom:

- A Location icon, which lets you tap to cycle through showing a map with the current device location centered, with your location centered, and with your location centered and oriented by the device's compass.
- An Actions button to reveal actions you can take, discussed next.
- An info ⓘ button lets you choose miles and kilometers for measurements, as well as select a schematic map, a satellite view, or a hybrid.

Tap the Actions button at the bottom and the map pivots to show a close-in view that's canted back to reveal a bit of 3D (**Figure 95, right**).

You can tap the automobile icon at lower right, and the Maps app is launched with the device's location preloaded as a destination.

Next, I'll explore each of the possible actions.

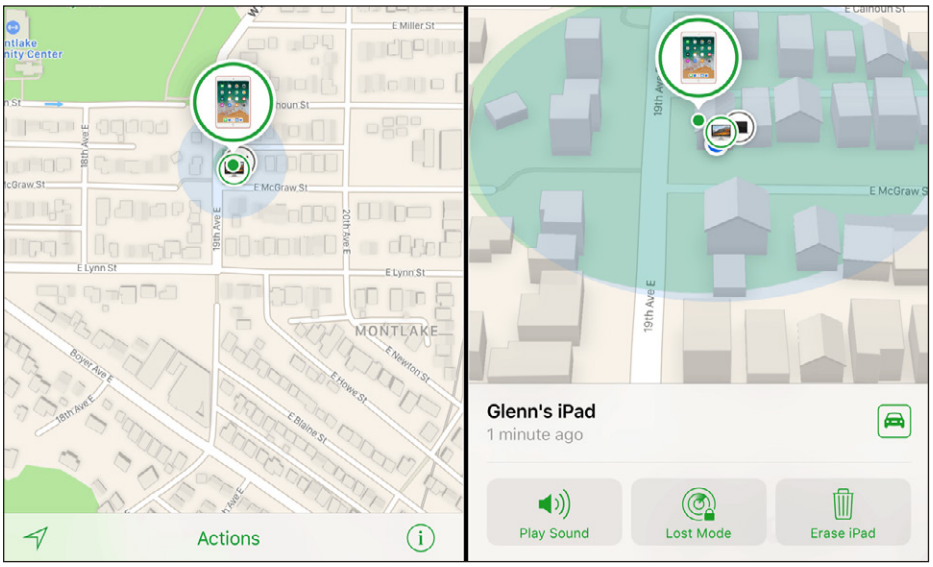


Figure 95: *Tap a device and you see it on a map (left); tap Actions, and the map tilts back for a 3D effect, zooms in, and reveals options.*

> ***Password not stored:*** *The app doesn't save your password—it caches it briefly. If you borrow someone's iOS device to run Find My iPhone, you don't have to worry about that person finding your iOS devices in the future. And, to reverse the situation, if a thief steals your iPad, the thief can't use the app to locate more of your devices or figure out where you are!*

Take Remote Action

You can now take action on your remote device, with three options that vary in utility based on whether your device has fallen behind a couch cushion, or has been misplaced or stolen (**Figure 95, above**). Whatever action you take, iCloud sends an email message to your Apple ID address.

Tap one of the options and see the section below that corresponds to Play Sound, Lost Mode, and Erase *device*. (For Macs and iOS 5 devices, the earliest ones supported, Lost Mode is replaced with Lock.)

WARNING! *If you know your device was stolen, consider taking location information to the police—call an officer if you have a report already opened—before trying to entice the thief to give it up.*

Offline Actions When Back Online

Pick any of the following actions when a device is shown as offline, and iCloud triggers that action when it comes back online and it still has Find My iPhone active. If the trigger happens, you get an email message. While thieves try to keep hardware off networks, they can easily slip up.

Devices that can't be found right away: *If a device's location can't be found quickly in the Find My iPhone web app or iOS app, you can't queue an action for when it's available. However, you can be told when it shows up: select it from the Devices list and then check Notify Me When Found (**Figure 96**). If it ultimately provides its location, you will receive an email message, see a banner when you sign in to the Find My iPhone web app, and get a pop-up alert on iOS devices with Find My iPhone installed.*

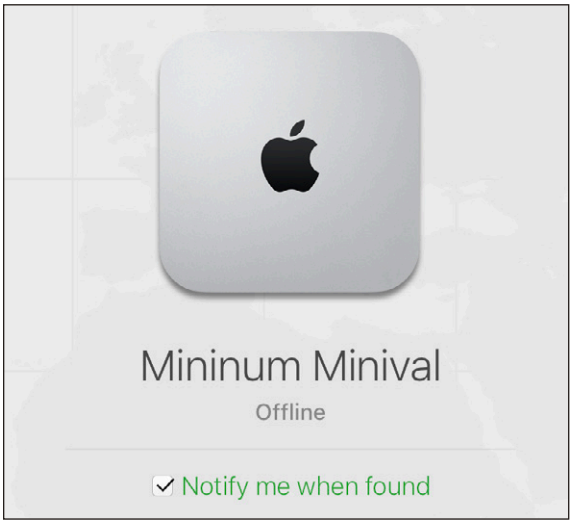


Figure 96: *Devices without a location can trigger alerts when they acquire a location.*

Play Sound

When you can't find a device but think it may be nearby, the Play Sound option should help you locate it. Tap or click Play Sound, and a loud

pinging noise will play for 2 minutes on the device, which also displays the message "Find My *Device* Alert" as a notification if locked or as a dialog box (**Figure 97**).

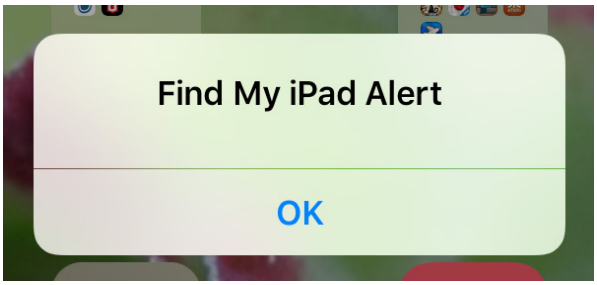


Figure 97: *iOS shows this message when Play Sound is triggered.*

The sound will override any mute settings on the device. The sound can be stopped on the found iOS device by tapping OK if it's unlocked; otherwise, unlock it and then tap OK.

Lost Mode

This option helps you recover a lost or stolen device. You can offer a reward and provide your phone number. It also puts the finder on notice that you know approximately where it is. ("I'm a block away. There's a reward.") Were your hardware stolen, this is a way to tell a thief that you have her location and other data, and advise her to give it up.

> **Note:** Lost Mode immediately disables Apple's side of Apple Pay for devices that are both capable of it and have the feature enabled, even if it's offline. Thus, if your device is lost and someone has the passcode and attempts to unlock the phone when it's not connected to a network to pay for something, Apple will not pass the transaction on for approval. You can log back in to iCloud on the device if it's recovered, and any credit and debits cards are once again available for use.

This Lost Mode option has up to four steps:

1. After tapping or clicking Lost Mode, you have to confirm by tapping Turn On Lost Mode (**Figure 98**). (Click Cancel to back out.)
2. If a device doesn't have a passcode set, you are prompted to enter and verify a passcode (**Figure 99**).

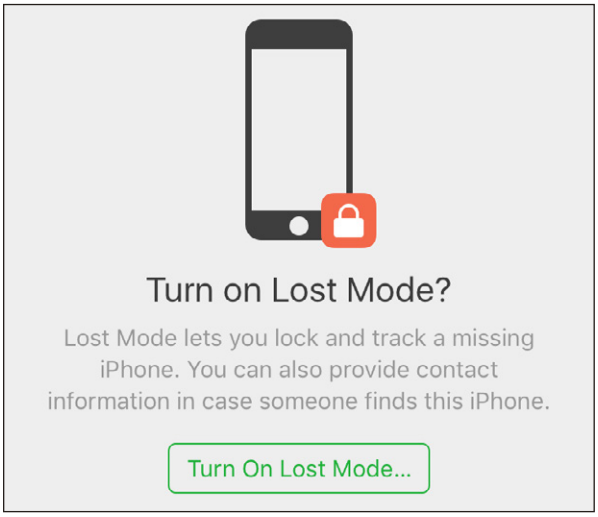


Figure 98: *Lost Mode doesn't involve a mysterious island.*

Figure 99: *Without a passcode in place, you are prompted to enter one and verify it.*

3. Optionally, set a phone number for a call back (**Figure 100**). On an iPhone, the phone may be used to call *only* that number. On other devices, the call-back number is displayed but can't be used.
4. Optionally, enter a message to appear on the device (**Figure 101**). In this step, the dialog shows that a passcode has already been set and will be used to lock the device.

   After you activate Lost Mode, the action is passed to the device, and an email message is sent to the email address for the Apple ID account you're using for Find My iPhone, confirming what you've done.

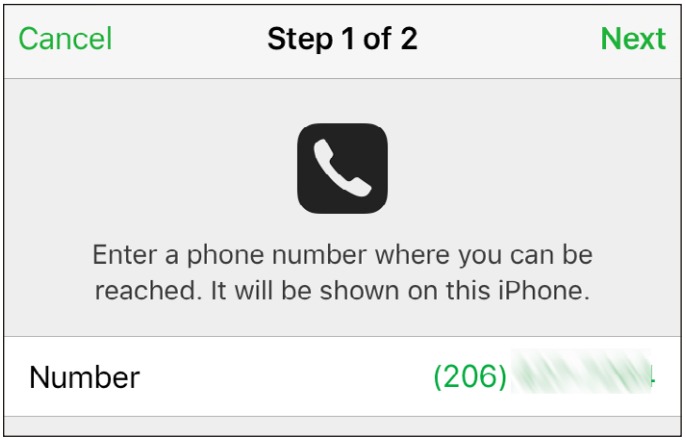


Figure 100: *You can opt to enter a call-back number.*

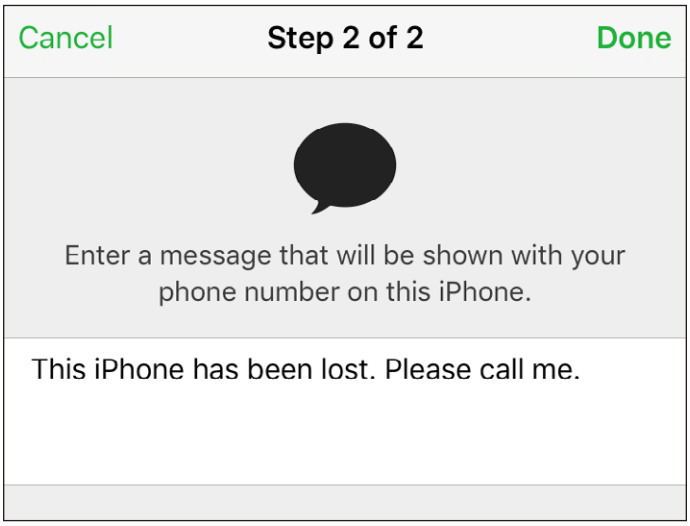


Figure 101: *Choose to add a message.*

Once the action is sent, one of the following behaviors occurs:

- If the device is connected to a wireless network and asleep, the next time it's woken, a passcode must be entered to gain access.
- If the device is online and in use, iOS drops the user into the Lock screen where the passcode-entry dialog or keypad is shown.
- If the device is offline, the next time it accesses any network with an Internet connection, the passcode lock is put into place.

Lost Mode also enables tracking the next time the device is online. A tracked path appears in a map as a dotted red line (**Figure 102**). This lets you see wherever a device has gone—so long as it remains online. Even neater, if Location Services has been turned off, Lost Mode re-enables it so that you can track your device.

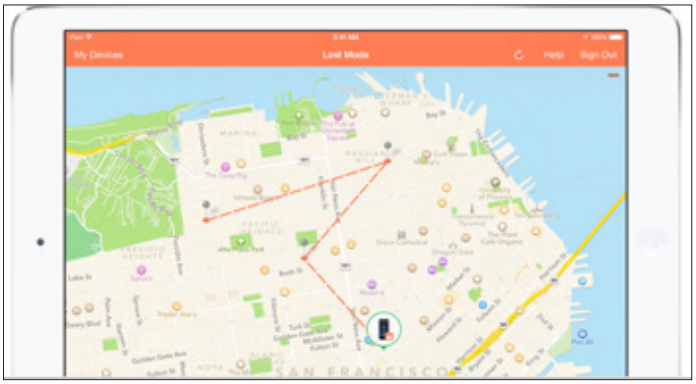


Figure 102: *While Lost Mode is enabled, the path a device takes as long as it has connectivity is recorded and shown as well. (Figure via Apple.)*

Note: The Lock mode for Macs makes a user set a six-digit code to unlock it. If the Mac has a Recovery disk partition installed, Find My Mac causes macOS to shut down immediately, no matter what's happening! Then the computer restarts from the Recovery disk, and will only unlock when that six-digit code is entered (**Figure 103**).

WARNING! *If someone can obtain your iCloud account name and password, even if you have two-factor authentication enabled, they can use Find My iPhone—and lock your device or erase it! If you had no passcode, you could lose access to your iPad or iPhone forever because of Activation Lock.*

With a Mac, they try to hold your machine hostage, because only the party using Lock knows the code. If this happens to you, an Apple Authorized Service Center can unlock your Mac. Don't pay the ransom.

Change your iCloud password if you can't remember the last time you did or if it's fewer than 13 characters long. *Your password should be memorable, long, and unique to iCloud.*

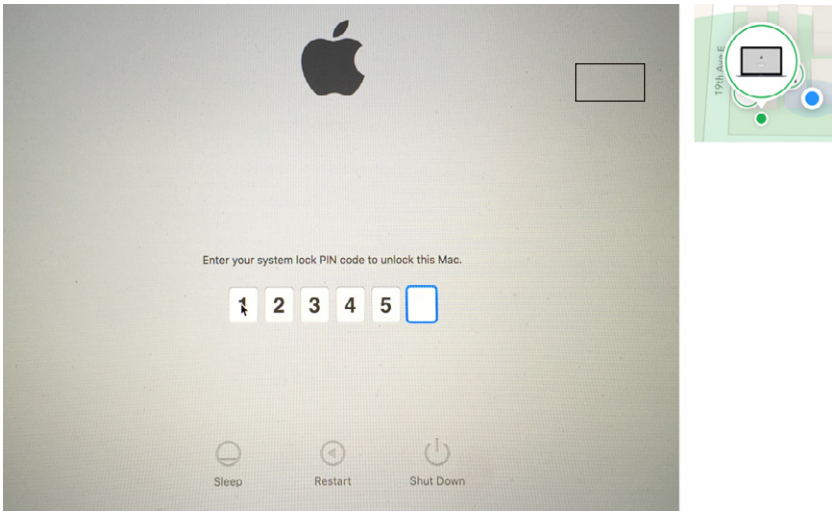


Figure 103: *A Mac reboots into a special locked mode. Find My iPhone even shows a neat "locked Mac" icon to indicate its status.*

Erase Device

The last resort in some cases (or first in others) is a remote wipe, in which all the user data on the iOS device is erased.

An erased device that has Find My iPhone enabled before erasure and remains associated with an Apple ID cannot be unlocked without the account password—the Activation Lock feature mentioned earlier. The Erase Device option lets you provide a phone number and message so that a person who found (or stole) your device can get in touch. The iOS device is essentially useless to them without the password.

> ***WARNING!*** *After erasing a device, Find My iPhone can no longer provide location information.*

> **Note:** You can remove a device from your Find My iPhone list after erasing it by following Apple's instructions **in a support note**.

It's a multi-step process to prevent accidental erasure:

1. In the web app or the iOS app, tap Erase (web) or Erase *Device* (iOS).

2. You're warned that everything is about to be erased. Tap or click Erase, but there are more steps ahead (**Figure 104**).

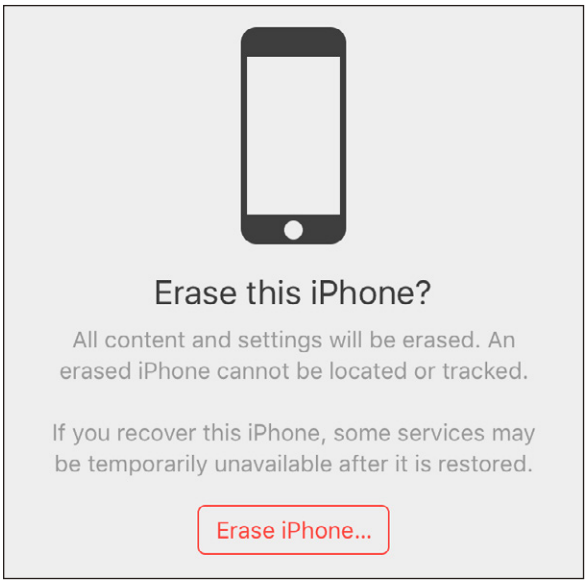


Figure 104: *This step seems like you're about to erase your device immediately, but there are more steps ahead.*

3. Tap Erase. (If you're using **two-factor authentication**, the device is removed from your set of trusted devices.
4. Enter your Apple ID password. (If this is another member's device, accessible via Family Sharing, enter her or his Apple ID password.)
5. Enter a phone number at which you can be reached after it's erased, and tap Next.
6. Enter a message you want to appear along with the phone number. You'll notice there's a Done button. Tap that, and the remote device is erased—there's no going back!

   If the device is online, the Erase action immediately wipes all your data off it. If it's offline, the erase begins as soon as it next comes online through any networking method.

   The erasure happens quickly. To "erase" all the device's stored data, an encryption key that protects your iOS device at a hardware level is thrown away and a few other settings rewritten. Everything is now completely unrecoverable.

Note: Macs with FileVault enabled in the Security & Privacy system preference pane can similarly have their boot drives rendered unreadable: an encryption key is deleted, making the drive's encrypted contents irretrievable. (The drive can still be erased and a new system installed, however.)

However, wiping your device isn't as bad for your data as it sounds. All iOS devices are set by default to back up the unique data that's stored on them, like settings, passwords, and documents created by or associated with apps. These backups can be either local to iTunes on a particular computer or remote to iCloud.

Tip: You can also make both kinds of backups by manually switching between the options in iTunes when an iOS device is connected. Tap Back Up Now in Settings > iCloud > Backup, then switch in iTunes to make a local backup (or the opposite).

Any media and apps kept on an iOS device are not stored in the backup. Instead, they are stored in some combination of a copy of iTunes (for your own music, videos, ebooks, and purchased movies) and iCloud (all apps or any media that you've bought from Apple, all apps, and your own music uploaded or matched using iTunes Match).

If you erase your device, and then either recover it or obtain a new device, you can restore from your most recent backup. If you were syncing any items to your device through iTunes, you can then sync them back to the device. Or, for items stored in iCloud, the restore process downloads them again.

Tip: In iOS 11, you can accelerate restoring by placing one iOS device near another, and your device being restored can pick up your settings from the other!

If you were syncing any data wirelessly through iCloud or an Exchange account, such as calendar or contact information, you likely won't have lost any of that data up to the moment the device was lost or disconnected from a cellular or Wi-Fi network. You will lose any changes made on the device between the last sync (push, fetch, or manual) for each account and the remote wipe.

Updates

version 1.0 (September 2017)

Initial release.

version 1.1 (December 2017)

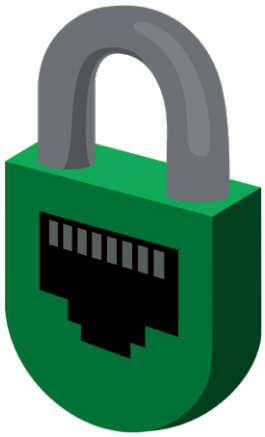
- Minor updates for iOS 11.2.
- Control Center now switches to white (no longer gray) for its disconnect icon and added popup explanations.
- Changed to include the unique gesture and status bar elements with the iPhone X, and more information about Face ID added.
- AirPlay 2 is now released, and the book reflects that.

Acknowledgments

I dedicate this book to my wife, Lynn, and kids, Ben and Rex. They keep me sane and happy, and keep me from spending my entire day thinking about and using digital devices.

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 the previous three!

Many thanks to longtime collaborators Adam and Tonya Engst, who saw this book through earlier editions and offered ebook help on this one, and Joe Kissell, who helped distribute this edition.



About the Author

Glenn Fleishman was trained as a typesetter, received a degree in art, and works as a journalist and programmer. Glenn appears regularly in Macworld, the *Economist*, TidBITS, *Fast Company*, *Wired*, and other publications.

Glenn writes about security, privacy, nanosatellites, copyright, punctuation conventions, crowdfunding, and much more.

He spent 2017 as the Designer in Residence at the School of Visual Concepts in Seattle printing a letterpress book of his writing, a Walt Whitman poetry folio, and other projects. 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

A Practical Guide to Networking, Privacy & Security in iOS 11

ISBN: 978-0-9994897-0-3 (ebook)
978-0-9994897-1-0 (print edition)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112-2629 USA

http://glennf.com/guides