A Practical Guide to

NETWORKING, PRIVACY & SECURITY IN iOS 10

By Glenn Fleishman

Welcome

Welcome to an excerpt of *A Practical Guide to Networking, Privacy, & Security in iOS 10*, version 1.0.0, published in September 2016 by Aperiodical LLC.

Please enjoy this excerpt, which contains the table of contents, introduction, chapter openings, and a few sample chapters. You can purchase the entire book at **http://glennf.com/guides**.

This book was written by Glenn Fleishman. The cover illustration is by Christa Mrgan.

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

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.

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.

Once your iOS device joins a network, the network name and any associated login information is added to an internal network list. Unlike in Mac

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

Apple Watch Wi-Fi

The Apple Watch can connect via Wi-Fi to reach its paired iPhone when the phone is out of Bluetooth range, and to carry out a limited set of tasks when the iPhone isn't available at all. But there are a number of provisos:

- The network uses the 2.4 gigahertz (GHz) band. (See **Wi-Fi Troubleshooting**.)
- The iPhone with which the Watch is associated must have previously connected to the network.
- The iPhone connection must be active over Bluetooth when the Watch encounters the Wi-Fi network for the first time.
- The network doesn't have a portal or login page.

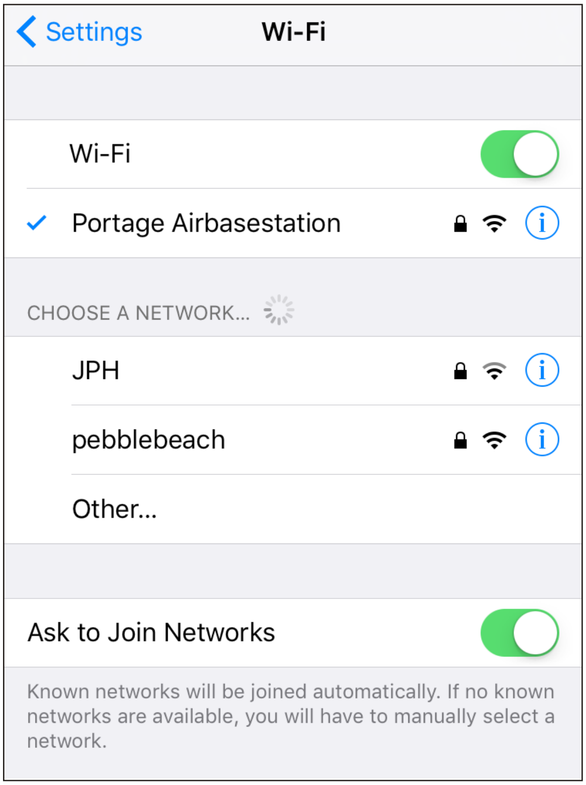
Since the release of watchOS 2 in 2015, the Watch can use Wi-Fi directly for many features.

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 has three elements, with optional fourth and fifth items:

- **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 Hotspot(s):** 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**.)



Wi-Fi

✓ Portage Airbasestation

CHOOSE A NETWORK...

JPH

pebblebeach

Other...

Ask to Join Networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

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—carefully, because it's a small target—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 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

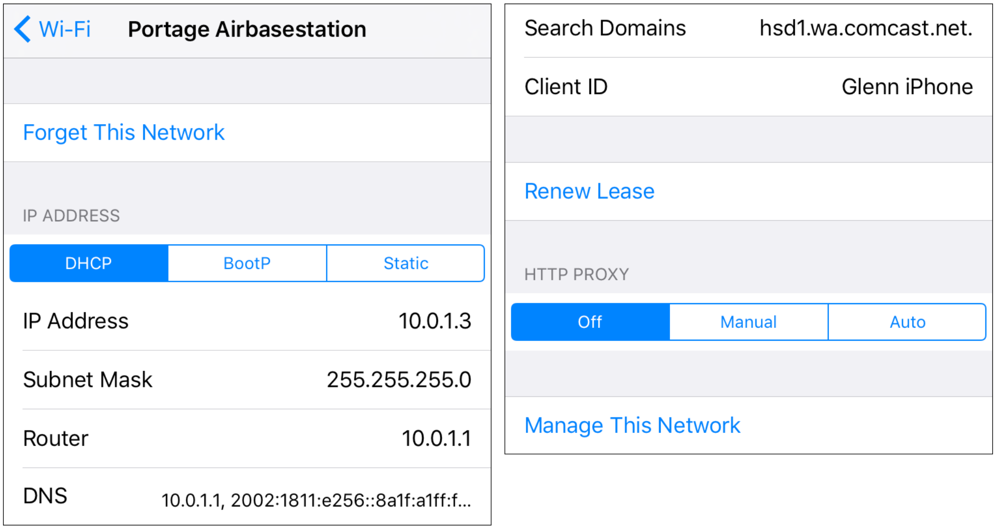
Apple added a fairly severe warning about using an unencrypted network connection in iOS 10. It displays "Security Recommendation" in the main Wi-Fi view, and then explains further in this details screen. And it has a link to follow to get even more information.

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-Login

As described in **Auto-Join and Auto-Login the Next Time**, these options appear only for hotspot networks for which the device has retrieved settings that allow it to make an automatic web-based login.



IP Address 10.0.1.3

Subnet Mask 255.255.255.0

Router 10.0.1.1

DNS 10.0.1.1, 2002:1811:e256::8a1f:a1ff:f...

Search Domains hsd1.wa.comcast.net.

Client ID Glenn iPhone

Figure 2: *You can view or set network connection values. (Top of view at left; bottom at right.)*

IP Address

The IP Address section covers TCP/IP values used for the Internet's addressing and routing system, divided vertically into sections. You start with three kinds of standard network connection methods, which you can see as the DHCP, BootP, and Static buttons near the top of Figure 2, above. Tap a button to display the related choices underneath. You should almost never need to change these values. 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. 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.

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`. The DNS field in the DHCP settings can be modified or added to. This can be useful if the network to which you're connected has poorly run or slow default DNS servers. Use a comma to separate multiple entries.

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 DHCP settings, if you set Client ID to a unique value, like `Glenn's iPad 4`, 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.

Tip: Unfortunately, you can't set DNS globally for iOS—you can set it only for individual network connections. It may not be worth the effort to set it for connections you use infrequently, but it's worthwhile for a network that you use often, such as your home Wi-Fi connection.

For certain network configurations that you will never have to enter for a public Wi-Fi network, you may need to tap the Static option and enter settings for IP address, subnet mask, router, and DNS. Those values would be provided by a system administrator or an ISP. Likewise, BootP is almost never used anymore, but remains for backward compatibility.

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.

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.)

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 Mac OS X since 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

You have an alternate way to pay for hotspot access. Boingo Wireless resells access at a flat monthly rate to over 400,000 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.

Boingo has two unlimited usage plans that each cost $9.95 a month (and half off on the first month), with only a monthly service commitment. The mobile plan lets you connect to any of its hotspots worldwide using up to two phones, tablets, cameras, or the like at a time. A North and South America plan allows two devices of any kind, including laptops, at a time.

Boingo also has regional and global plans, as well as an hourly and pay-as-you-go service. While Wi-Fi is typically free in America, elsewhere in the world Wi-Fi for a single night at a hotel or a few hours in a coffeeshop can cost more than the monthly plan.

Apple doesn't let hotspot apps run in the background to manage logins. You must launch the Boingo app before you connect, and it handles getting you in.

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, an option that is 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**).

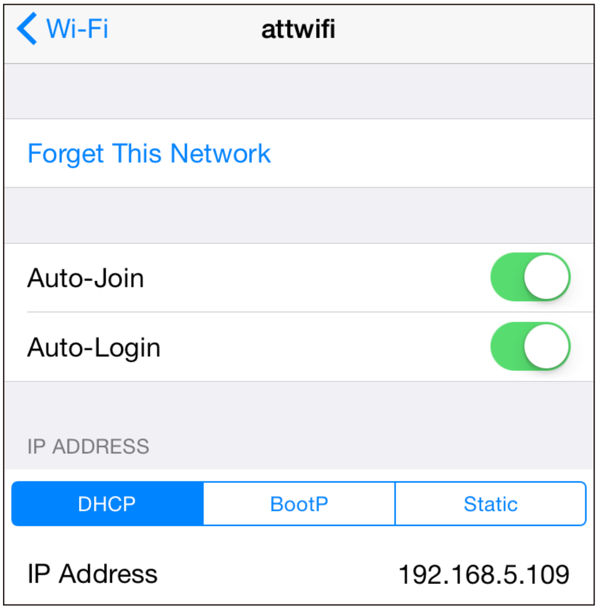
To turn off Auto-Join or Auto-Login, follow these steps:

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.



Auto-Join ●

Auto-Login ●

IP Address 192.168.5.109

Figure 3: *When you connect via a portal to a hotspot, the detail page provides additional options.*

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.

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. In this chapter, I look at how to clamp down on who can reach you and how to stop those you don't want to hear from.

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.

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.

iOS 7 added blocking, which extends to calls, iMessage, and FaceTime. iOS 8.3 added yet one more feature: the ability to sort incoming messages in iMessage by those in your Contacts and others.

How Does Blocking Appear to Blocked People?

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.

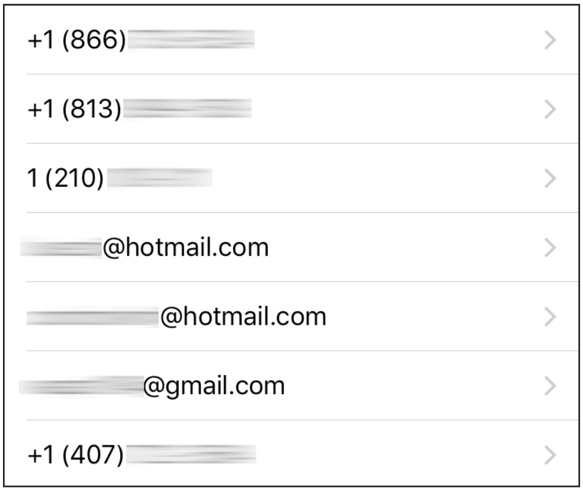
With FaceTime, a placed call rings indefinitely without the recipient being notified.

Blocking Phone Numbers and Email Addresses

You can block phone numbers and email addresses in multiple places:

- 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 69**). 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.



+1 (866)[redacted]

+1 (813)[redacted]

1 (210)[redacted]

[redacted]@hotmail.com

[redacted]@hotmail.com

[redacted]@gmail.com

+1 (407)[redacted]

Figure 69*: The Blocked list shows all banned emails and phone numbers.*

Starting in iOS 10, you can also use third-party apps to block calls and provide Caller ID lookup as a call comes. You control which are active via Settings > Phone > Call Blocking & Identification. They don't block jerks you know, but they can identify likely fraud and spam callers, and even auto-block them.

Sort iMessages by Whether in Contacts

Messages offers a subtle way to segregate incoming messages between people in your Contacts and those who are not. Enable it in Settings > Messages > Filter Unknown Senders.

Incoming iMessages that match any phone number or email address in Contacts appear in a Contacts & SMS tab, as well as any SMS/MMS messages, which are unfiltered. Conversations already underway appear in that tab, even if they're not in your Contacts.

Any future incoming iMessage messages 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.

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 half of the book, you'll get answers that will make you feel better when using a device in all situations.

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 two robust ways to secure a device: with a passcode and, for newer hardware, its Touch ID fingerprint-recognition system.

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 accepted, which unlocks the encryption keys needed to read stored information.

> **WARNING:** *If you lose the passcode and Touch ID isn't available (such as after a reboot), your data is lost forever.*

Set a Passcode

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

To set the passcode lock, follow these steps:

1. In Settings, tap Passcode. On Touch ID-equipped devices, the option reads Touch ID & Passcode.
2. Tap Turn Passcode On.
3. If you want to use the minimum, a four-digit passcode, tap it in and re-enter it when prompted.

You can also opt to tap Passcode Options and pick a six-digit code, a custom-length numeric code, or an alphanumeric password of letters, punctuation, and numbers (**Figure 97**).

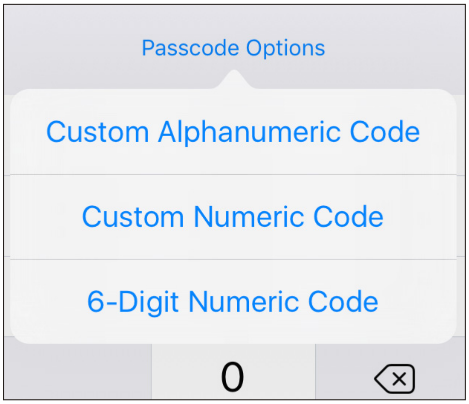


Figure 97: *You can opt for a longer or more complicated passcode.*

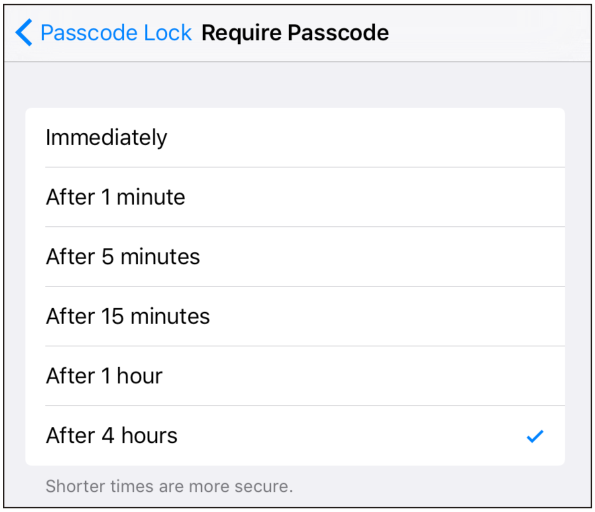
WARNING: *Many iOS security gurus say not only is four digits too few to resist cracking, but six isn't enough, either. They recommend picking a memorable short phrase that's easy to enter but impossible to guess.*

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 (**Figure 98**). 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.
- 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.



Require Passcode

Immediately

After 1 minute

After 5 minutes

After 15 minutes

After 1 hour

After 4 hours ✓

Shorter times are more secure.

Figure 98: *Choose the duration until you're asked for your passcode again.*

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 Erase Data to On. What do you lose? Only items created since the last backup and sync; see **Erase Device**.

Use Touch ID

Apple's Touch ID lets you turn to your fingertips to secure your device. Touch ID lets you train several later models of iPhone and iPad to recognize up to five fingerprints. It can be used not only to unlock your phone, but to use Apple Pay (on supported devices) and make iTunes and App Store purchases as well.

Tip: Touch ID in iOS can be used to authenticate third-party software. 1Password and my credit union's app are two I use that allow Touch ID for unlocking.

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.

Even with Touch ID enabled for all tasks, you will still 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 in more than 48 hours.
- Once five unsuccessful attempts have been made to unlock your phone or tablet via Touch ID.
- If you’ve put the device into Lost Mode via Find My iPhone.

There’s one more that requires more explanation. It was added quietly in 2015, and it appears designed to make sure you don’t forget your passcode! If you’ve only used Touch ID to unlock your device over a six-day period, an eight-hour timer starts every time you use Touch ID. If you don’t unlock with Touch ID within eight hours of the previous attempt, you’re prompted for your passcode. You’ll most likely see this when you wake up in the morning. This tries to ensure that even constant iOS users have to enter their passcode occasionally.

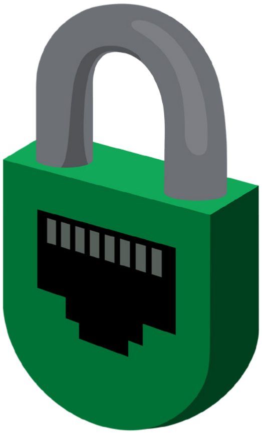
Note: Matthew Green, a well-known security researcher, **tweeted this cautionary tale** in November 2014: “I woke this morning to find my 7 y/o levering my finger onto the Touch ID sensor of my phone. Maybe time to go back to passwords.”

When using Touch ID, it’s important to remember that while 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, or other party—can force your finger onto the sensor, they can gain access to at least some of your information.

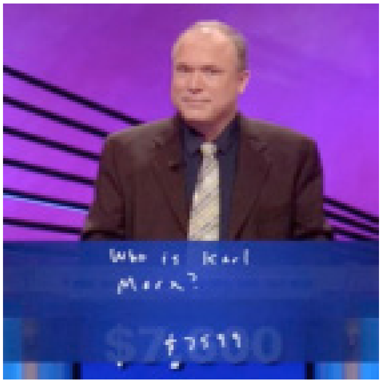
Acknowledgments

I dedicate this book to my wife, Lynn, and sons, Ben and Rex. They keep me sane and happy, and keep me from spending my entire day thinking about and using digital devices.

Many thanks to longtime collaborators Adam and Tonya Engst, who saw this book through earlier editions and offered ebook help on this one! Thanks to Charles Fleishman, Jeff Carlson, and Scout Festa for their varied editing assistance across three editions!



About the Author



Glenn Fleishman was trained as a typesetter, received a degree in art, and works as a journalist and programmer. Glenn writes two weekly columns for Macworld, where he also co-hosts the Macworld podcast and files reviews and features.

Glenn appears regularly in TidBITS, *Fast Company*, The Ringer, *The Atlantic*, and other publications. He writes articles on unusual and quirky topics directly for his patrons via **his Patreon campaign**, which you can join. Glenn writes about security, privacy, nanosatellites, copyright, punctuation conventions, crowdfunding, and much more. His blog is **http://glog.glennf.com**, and he overshares on Twitter at **@glennf**.

In October 2012, he appeared on the *Jeopardy!* quiz show and managed to win—twice! Alex Trebek seems like a very nice fellow, but you never get to really know him.

Copyright and Fine Print

A Practical Guide to Networking, Privacy & Security in iOS 10

ISBN: 978-0-9914399-8-0 (ebook)
978-0-9914399-9-7 (print edition)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112-2629 USA

http://glennf.com/guides

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

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

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

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

http://www.apple.com/legal/trademark/appletmlist.html