A Practical Guide to

NETWORKING, PRIVACY & SECURITY IN iOS 9

By Glenn Fleishman

Welcome

Welcome to an excerpt of *A Practical Guide to Networking, Privacy, & Security in iOS 9*, published in October 2015 by Aperiodical LLC. This excerpt includes the table of contents and a sample chapter. You can purchase the entire book at **http://glennf.com/guides**.

This book describes how to use your iPhone, iPod touch, or iPad with iOS 9 on Wi-Fi and cellular/mobile networks securely, making connections with ease while protecting your data and your privacy. It also covers Bluetooth networking, tracking an iOS device, the Apple Watch, Personal Hotspot and Instant Hotspot, two-factor authentication with an Apple ID, using AirDrop and AirPlay, and solving connection problems.

This book was written by Glenn Fleishman, edited by Jeff Carlson, and copyedited and proofread by Scout Festa. The cover illustration is by Christa Mrgan.

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 9 provides new 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

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, iTunes 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-step verification, 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! *Once two-step verification is enabled, 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.*

Factor in Apple's Security Changes

Apple used to call its two-factor approach "two-step verification" and stapled it on top of existing software and systems. Some Apple-controlled sites let you log in using an Apple ID that should be protected with a second factor using just the password. OS X didn't support it directly, which led to awkward interactions and round-trips through web sites to complete some tasks.

In iOS 9 and El Capitan, Apple engineered support deeply into both operating systems, while removing two elements that were problematic in practice, simplifying both logging in and account recovery.

If you've used a two-step protected Apple ID before, here's what's changed:

- A backup phone number can receive a code either by SMS or by voice, using an automated system that speaks the numbers to you.
- Before seeing a code on a trusted device, you're shown an approximate map and location from which the request has been made, and you have to click Allow to proceed.
- You no longer pick a phone number or trusted device at which to receive a code: all trusted devices get the code.
- A Mac can be a trusted device, not just iOS equipment.
- The Recovery Key, a linchpin of keeping account access, is gone, replaced by a human-interaction recovery process.

Turn On Two-Factor Authentication

You enable two-factor setup on your account through iOS or OS X 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 OS X's iCloud preference pane in Account Details > Security.

WARNING! *Apple said it will roll out two-factor authentication to Apple ID accounts through third quarter 2015, so you may not yet be able to follow these steps. You should receive an invitation for an existing account.*

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 Two-Factor Authentication and then tap Enable.
3. The Two-Factor Authentication screen provides a brief explanation and then offers a Continue button to tap (**Figure 77**).

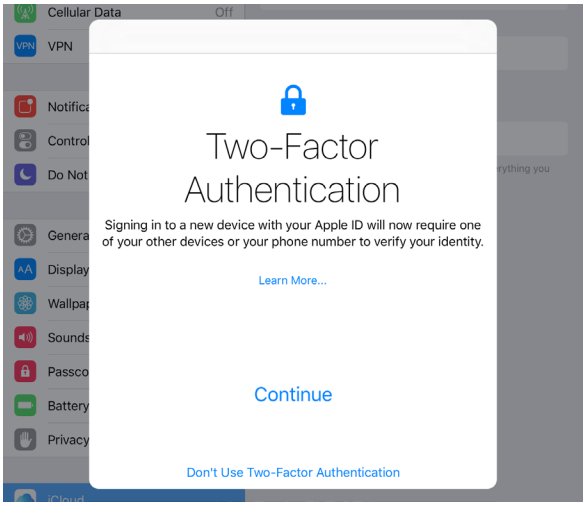

Figure 77: *The first screen lets you opt in or, in fine print at the bottom, opt out.*

4. You start by entering a phone number at which you can receive a text message or voice call; you can choose which (**Figure 78**).

Select your country, enter your number, pick Text Message or Voice 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.

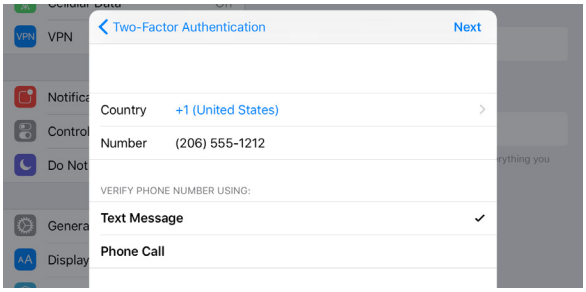

Figure 78: *The process starts with entering a phone number.*

5. Enter the verification code. When you enter the last digit correctly, setup is complete.

   The Password & Security settings now show two-factor authentication set to On, and list your Trusted Phone Number (**Figure 79**). 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.

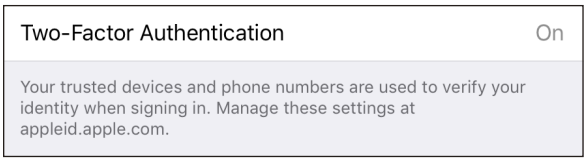

Figure 79: *iCloud settings show that two-factor authentication has been enabled.*

Disable Two-Factor

You can easily turn off two-factor authentication if you find it doesn't work for you, or you need to work with other iOS devices and Macs that don't support it.

From the **Apple ID site**, log in and then click Turn Off Two-Factor Authentication. Choose new security questions, and then click Continue.

You'll be asked to confirm one last time, and then you're back to normal password-only account protection.

Log In with Two-Factor Authentication

When you log in to iCloud in iOS or OS X, 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 OS X computer into a trusted device. For a web browser and iCloud.com, you can opt to trust the browser from then on (**Figure 80**).

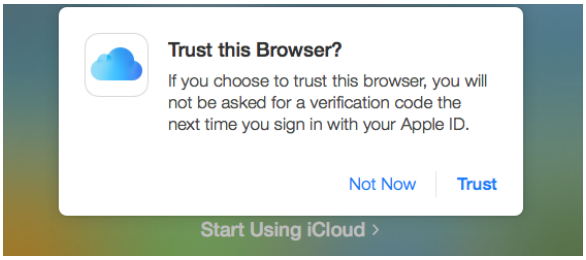

Figure 80: *Browsers can be trusted just like iOS devices and Macs.*

Note: Because OS X has separate user accounts, trusted device status is set for each user account individually. Each OS X user can be logged 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 81**). Click Allow to proceed.

> ***WARNING!*** *If you click Don't Allow, the remote login can't proceed, as no verification code is generated. However, from what I've tested, there's also no alert generated anywhere about an attempt to log in that you apparently didn't authorize!*

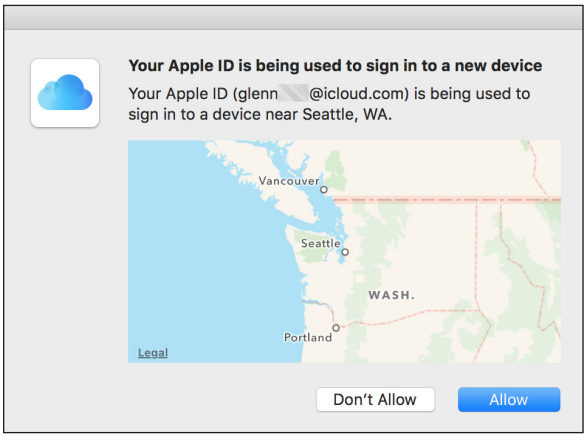

Figure 81: *To avoid unwanted logins, you're shown a geographic alert.*

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, then choose Text Message or Phone Call, before clicking Continue (**Figure 82**).

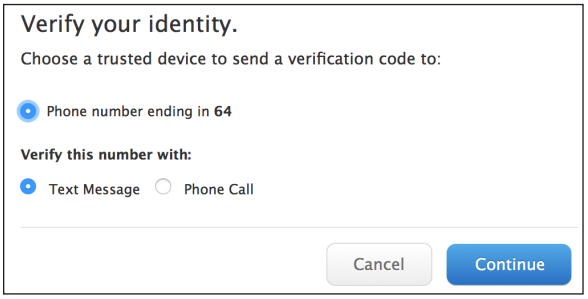

Figure 82: *You can opt to use a phone number instead of a trusted device.*

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, OS X, or the **Apple ID site**.

- OS X: Open the iCloud system preference pane, click Account Details, click the Security tab, and click the + (**Figure 83**).

Figure 83: *Trusted phone numbers can be managed in several places, including OS X.*

- iOS: Go to Settings > iCloud > *account name* > Passwords & Security, enter a phone number, and click Continue. Tap Add Trusted Phone Number.
- Apple ID site: In the Security section, click Edit at the far right, then click Add Trusted Phone Number.

  In each location, you enter a phone number, choose whether to send a text message or receive a voice 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 is a feature that first appeared in iOS 8.1 and Yosemite as part of Continuity. Because it forwards text messages, it can allow security codes to be received on your Mac. If you have any concerns about someone having access to your Mac when you're not around, disable SMS Forwarding.*

WARNING! *An SMS code can be seen on the lock screen of an iOS device unless you've disabled notifications on the lock screen.*

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.

Note: As of this writing, some features aren't fully available. Adding a notification email except in a setup stage may not be available until later.

You have to use the **Apple ID site** to manage this. To add an address, after logging in to your account:

1. In the Account section, click the Edit button at far right.
2. Under Reachable At, click Add an 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 calendaring (over CalDAV), contacts, and email can be used with non-Apple software, you can generate up to 25 app-specific passwords for use with this software via the **Apple ID site**.

WARNING! *App-specific passwords bypass two-factor protections and, if recovered, could be used to access contacts, calendars, and email. However, these passwords don't provide a way in to other account services, like changing your password.*

1. Click Manage Your Apple ID.
2. Enter your Apple ID and password, and click Sign In.
3. Enter the verification code that appears on other devices and click Continue.
4. In the Security section, click Edit at far right.
5. Under App-Specific Passwords, click Generate Password.
6. For each password you need to create (**Figure 84**):
   a. Enter a label that helps you remember for what purpose you created the password.
   b. Copy the password and paste it into the software with which you need to use it.
   c. Click Done.

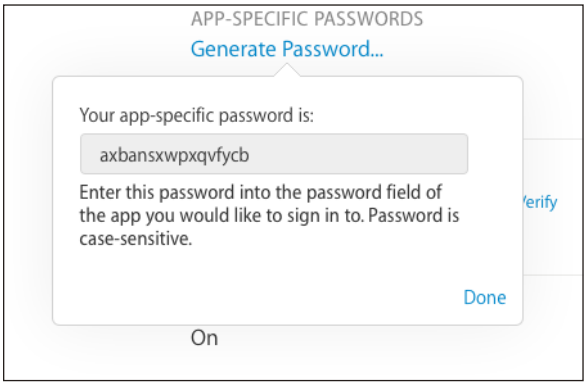

Figure 84: *App-specific passwords work with non-Apple software for a few specific services, like email and contacts.*

If you ever want to revoke an app-specific password, return to the Security section, and click Edit, 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, OS X, or the Apple ID site. Here are the instructions for iOS:

1. Tap Settings > iCloud > *account name* > Devices (**Figure 85**).
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.

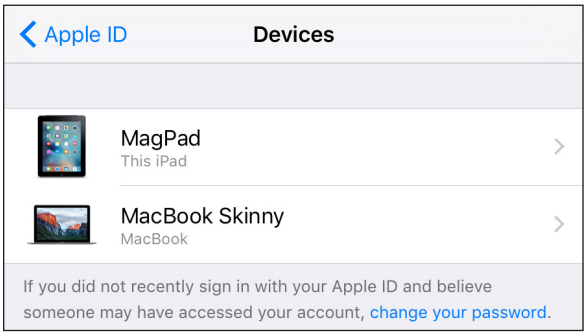

Figure 85: *All trusted devices are listed wherever you can log in to examine the details of your Apple ID account.*

Remove a Trusted Phone Number

Trusted phone numbers can be removed from iOS, OS X, or the Apple ID site. In Mac OS X:

1. Open the iCloud system preference pane.
2. Click Account Details.
3. Click the Security tab. (Enter your password if requested, and you may have to repeat steps 2 and 3.)
4. From the phone number list, select one and click the – button.

Recovering Account Factors and Access

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

Lost or Forgot Your Password

Visit **the iForgot site** and follow these steps:

1. Enter your Apple ID and click Next.
2. Confirm your trusted phone number by entering the entire set of digits; Apple displays just the last two (**Figure 86**).

Figure 86: *You have to confirm a phone number by entering it to reset your password.*

Can't remember the number? *Click Don't Know the Phone Number and proceed to* ***Lost Everything! Recovery****, below.*

3. Click Continue.
4. A notification is sent to your trusted devices. Follow that link.
5. If you don't have access to trusted devices, click Don't Have Access to *Device Name*, and then click Reset with Verification Code (**Figure 87**).

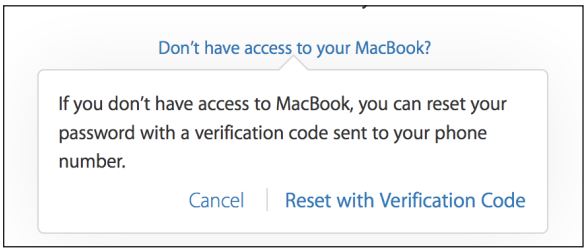

Figure 87: *If you don't have access to one or more trusted devices, you have to reset by receiving and entering a verification code.*

6. A code will be sent to your trusted devices, which isn't much use, but you can then tap Don't Have Access to Trusted Devices? and have the code sent to one of your phone numbers. Enter that code.

   If you don't have access to your trusted phone numbers, read on.

Lost One, but Not All, of Your Trusted Devices

You can manage your trusted devices as noted earlier via iOS, OS X, and the Apple ID site. If you lose a device, remove it from the account.

WARNING! *I'd heavily suggest adding new devices before removing old ones to avoid being locked out of your account if something goes wrong before you've tested the new setup.*

Lost a Phone Number

A phone number, not an actual phone, typically travels with an account; the phone contains a SIM (most global networks) or a similar module that is associated in your carrier account with your number.

If you lose your phone, you can get the number associated with a new one. Call your carrier and it will work through the details with you.

If you somehow manage to lose your phone number—such as giving up an old number and getting a new phone—there may be no way to recover it. It's vitally important to migrate all your records with Apple and any other company after changing your phone number, preferably before losing access to the previous number.

In iOS, in OS X, and at the Apple ID web site, you can add other trusted phone numbers and then delete one or more that's out of date.

Lost Everything! Recovery

Failing everything—the loss of access to all numbers and the loss of all your trusted devices—at step 6 above, keep going:

7. Click Don't Have Access to Any of These Numbers? and you can choose Try Again Later or Continue without Code (**Figure 88**).

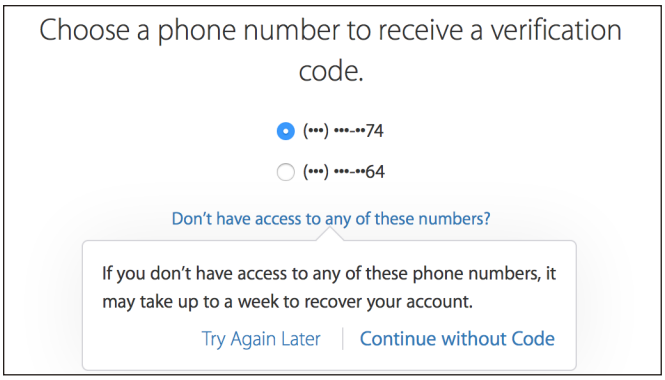

Figure 88: *If no trusted number is available, you can move towards account recovery.*

8. If you need to pick the latter option, click it and you finally see a Request Account Recovery? dialog (**Figure 89**).

> ***WARNING!*** *It might take a week to recover access to your account. This is intentional, to make it hard for those who might have some of your personal details to access your account.*

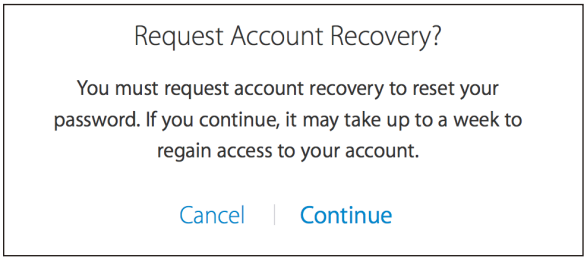

Figure 89: *Your last-ditch effort, after all other avenues are exhausted, is to request account recovery.*

9. Click Continue, and you start a new process, which may begin with you confirming credit-card billing information and other details. Apple hasn't disclosed all of what happens next, presumably for security.

Account Locked

In some cases, Apple will apparently lock your account when, based on factors that it doesn't disclose, it appears that your account is not under your control. In the past, this could happen when an outside party made a concerted effort to break into your account, however futile.

When your account is locked, you have to go through the same procedure as for a regular recovery, and it can take days. However, as long as you have most or all of your factors in hand, and all of your account-registration information (like your credit card number and the like), you should have an easier time of getting the account re-enabled.

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 podcast and files reviews and features.

Glenn appears regularly in the *Economist*, Boing Boing, TidBITS, *Fast Company*, *MIT Technology Review*, and Six Colors. Glenn writes about security, privacy, nanosatellites, copyright, Bitcoin, crowdfunding, and much more. His blog is **http://glog.glennf.com**, and he overshares on Twitter at **@glennf**.

He's part of the geeky **The Incomparable podcast network**, where you can hear him as a panelist on shows about sci-fi and fantasy books, movies, comic books, television shows, and much more. He also plays the recurring role of a highly fictionalized Nicola Tesla on **The Incomparable Radio Theater**.

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

ISBN: 978-0-9914399-6-6 (ebook)
978-0-9914399-7-3 (print edition)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112-2629 USA

http://glennf.com/guides