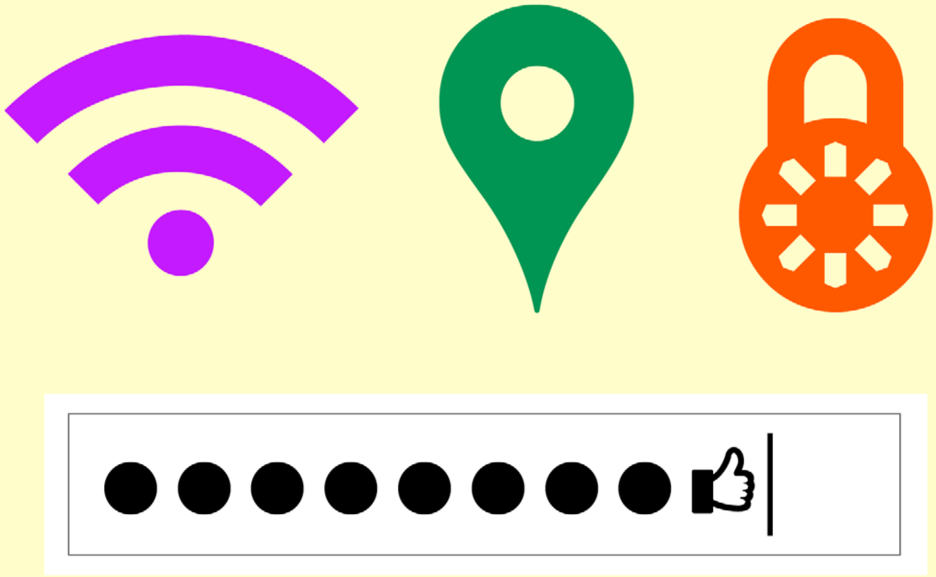
A Practical Guide to

NETWORKING, PRIVACY & SECURITY IN IOS 11



BY GLENN FLEISHMAN

Welcome

Welcome to an excerpt of *A Practical Guide to Networking, Privacy, & Security in iOS 11*, version 1.0, written by Glenn Fleishman, and published in October 2017 by Aperiodical LLC.

Please enjoy this excerpt, which contains the table of contents, introduction, and a sample chapter. You can purchase the entire book 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

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.

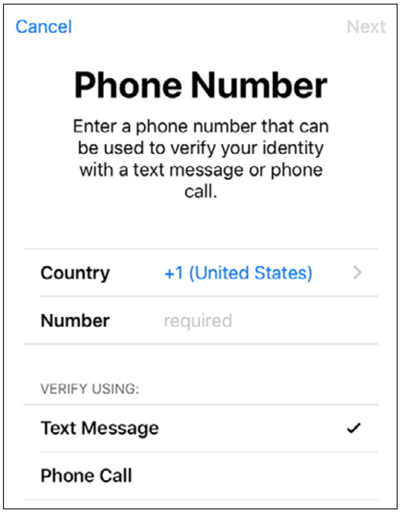
WARNING! *Apple warns that you can't turn off 2FA after enabling it on "some accounts created in iOS 10.3 or macOS Sierra 10.12.4 and later." Apple ID accounts created earlier can all have 2FA disabled. Factor that in before turning it on.*

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.



Phone Number

Enter a phone number that can be used to verify your identity with a text message or phone call.

Country +1 (United States)

Number required

VERIFY USING:

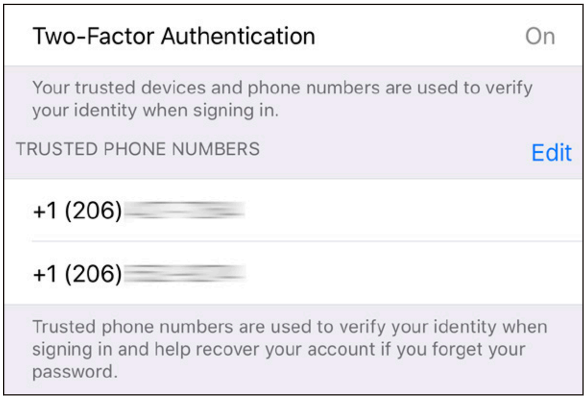
Text Message ✓

Phone Call

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.



Two-Factor Authentication On

Your trusted devices and phone numbers are used to verify your identity when signing in.

TRUSTED PHONE NUMBERS Edit

+1 (206)[redacted]

+1 (206)[redacted]

Trusted phone numbers are used to verify your identity when signing in and help recover your account if you forget your password.

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

Disable Two-Factor

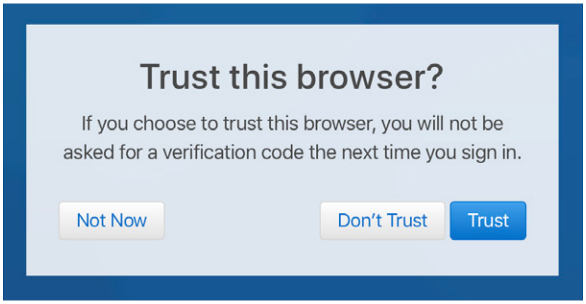
As noted earlier, Apple doesn't allow 2FA to be turned off on all accounts. And it removed an explanation in settings about how to disable it.

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



Trust this browser?

If you choose to trust this browser, you will not be asked for a verification code the next time you sign in.

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.

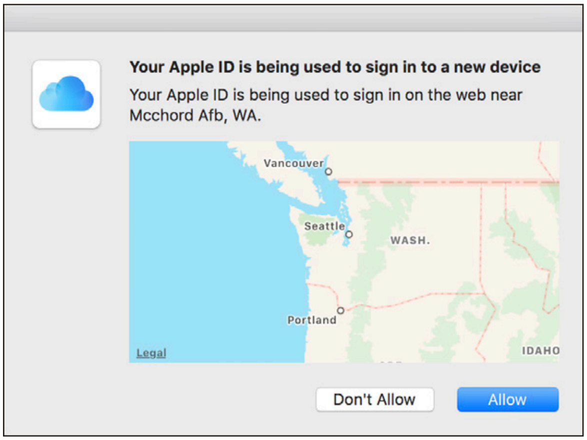
Two-factor authentication presents itself in different ways in different places. In practice, you typically enter an account name (if not already filled in) and password, and then receive the code at all your trusted devices, which you then enter where prompted.

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."*



Your Apple ID is being used to sign in to a new device

Your Apple ID is being used to sign in on the web near Mcchord Afb, WA.

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.

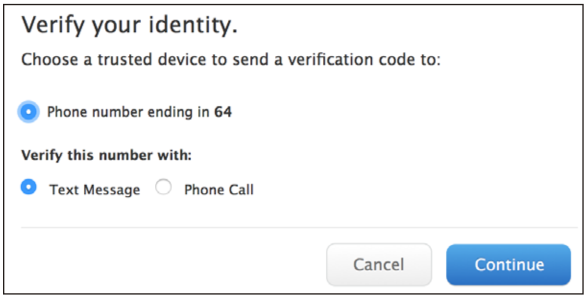
   If you don't have access to a trusted device at the time at which you want to log in, you can use a trusted phone. Follow these steps instead:

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**).



Verify your identity.

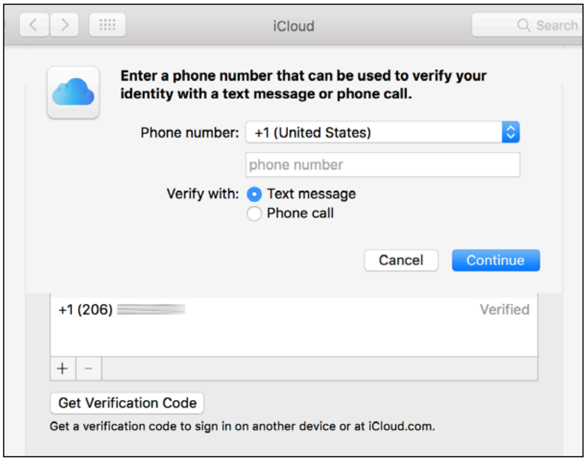
Choose a trusted device to send a verification code to:

● Phone number ending in **64**

Verify this number with:

● Text Message ○ Phone Call

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



Enter a phone number that can be used to verify your identity with a text message or phone call.

Phone number: +1 (United States)

phone number

Verify with: ● Text message
○ Phone call

+1 (206) [redacted] Verified

Get a verification code to sign in on another device or at iCloud.com.

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

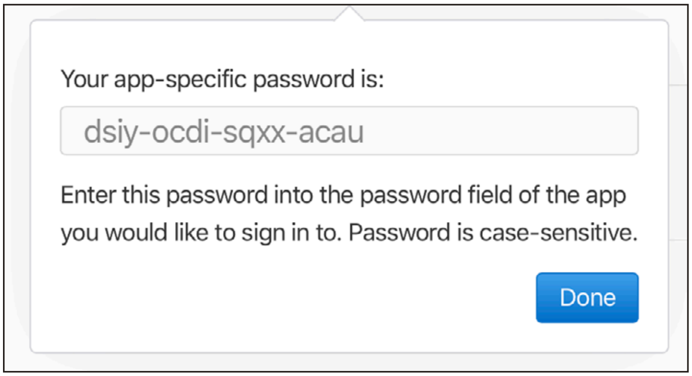
Because calendar events, contacts, and email can be used with non-Apple software, Apple lets you create special *app-specific passwords* for use with third-party apps. You can generate up to 25 app-specific passwords via the **Apple ID site**.

> ***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.



Your app-specific password is:

dsiy-ocdi-sqxx-acau

Enter this password into the password field of the app you would like to sign in to. Password is case-sensitive.

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.

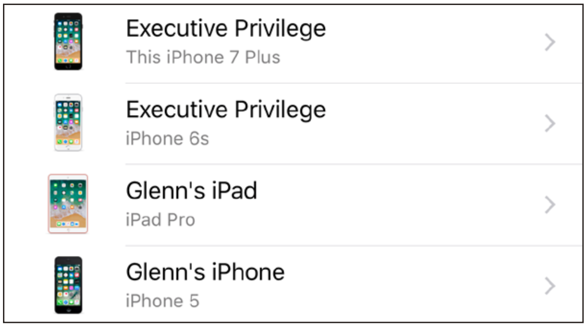
Remove a Trusted Device

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.



Executive Privilege
This iPhone 7 Plus

Executive Privilege
iPhone 6s

Glenn's iPad
iPad Pro

Glenn's iPhone
iPhone 5

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

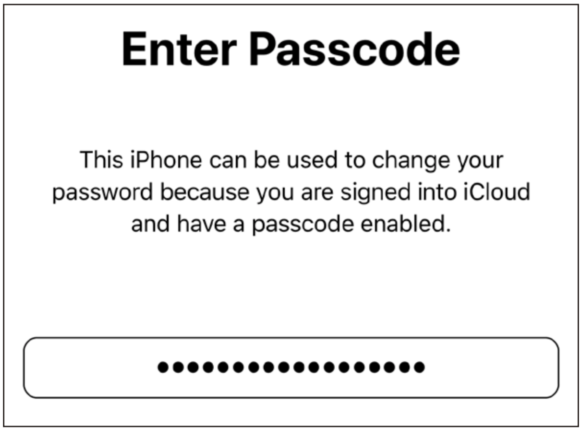
So you need two factors to log in: a password and a verification code. But what happens if you forget your password or you lose access to your trusted phone numbers and devices? Apple has responses for each.

> ***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.



Enter Passcode

This iPhone can be used to change your password because you are signed into iCloud and have a passcode enabled.

••••••••••••••••••

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.

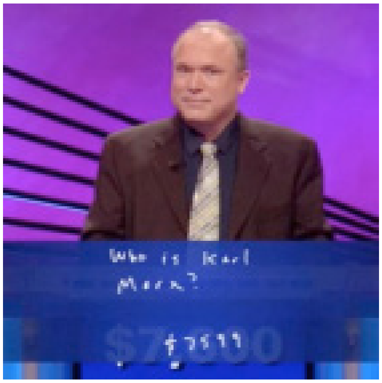
- In Find My iPhone, follow the steps earlier for *Recover via Find My iPhone with a Phone Number*.

    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.

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

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

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