EBOOK EXTRAS: v1.1
Downloads, Updates, Feedback

TAKE CONTROL OF YOUR APPLE ID

by GLENN FLEISHMAN

$7.99

Table of Contents

Read Me First

Welcome to *Take Control of Your Apple ID,* version 1.1, published in February 2019 by alt concepts inc. This book was written by Glenn Fleishman and edited by Scholle Sawyer McFarland.

This book offers all the information you need to manage your Apple ID, from setting up two-factor authentication to using it with Apple's various services and stores, including troubleshooting access to your account if (or, perhaps, *when*) something goes wrong.

If you want to share this ebook 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. Discounted classroom and Mac user group copies are available.

Updates and More

You can access extras related to this ebook on the web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

Basics

To review background information that might help you understand this book better, such as finding System Preferences and working with files in the Finder, I recommend reading Tonya Engst's ebook *Take Control of Mac Basics*.

What's New in Version 1.1

In version 1.0, I didn't cover comprehensively enough how to enable two-factor authentication (2FA) for an Apple ID when you don't use that Apple ID for iCloud with any current device under your control. This is now more fully documented in case you have such an Apple ID. See Set Up 2FA Without a Device.

This is particularly helpful for people in the Apple Developer program who have an Apple ID devoted to development but not iCloud, as Apple announced in early February 2019 that all Apple IDs used for development must have 2FA enabled.

I also explained more fully how to trigger sending a 2FA verification code via SMS or an automated voice call if you don't have access to a trusted iOS or macOS device. See Log In with 2FA by SMS or Voice Call.

Introduction

Your Apple ID is the center of your identity when it comes to managing Apple accounts and gear. It's your iCloud login. It lets you prove you own hardware devices. It's associated with purchases and subscriptions you make at Apple's various stores. It can also be used to lock a stolen or lost iOS device or Mac, protecting your data and turning the device into little more than an expensive doorstop. It can be used to track missing hardware, too.

But Apple's security for this important ID is so robust that it can sometimes trip you up. You may run into trouble if you forget a password or your password seemingly stops working; when you lose trusted devices or phone numbers; when a credit-card number expires or a card number is stolen and deactivated; when you can no longer receive email at the main address registered to your Apple ID; or when you move or travel from one country to another.

Additionally, Apple engages in strong automated account security monitoring that alerts it when people try to access your account without proper credentials, like your password. That means that even if you never have a problem entering a password yourself, someone else trying to hijack your account could lock you out.

Unfortunately, when something goes wrong with an Apple ID, you're often left to flounder. Apple's online and phone support may provide conflicting or incorrect information, or you may be told there is nothing they can do to help. That's where this book comes in.

This book covers how to manage an Apple ID on the Apple ID website, and in iOS, macOS, Windows (iCloud and iTunes), and Android (Apple Music). I'll help you navigate account security, especially enabling and managing two-factor authentication to reduce the potential that even a stolen password could offer up access to your account. I'll explain how to manage multiple Apple IDs (and why you might intentionally set more than one up). And you'll learn a lot about getting out of trouble if any of that lengthy list of issues above ever happens to you.

Apple ID Quick Start

Because an Apple ID gets used in so many different ways, you likely want to jump to specific chapters that address your immediate needs, and then read background information as appropriate.

Learn the basics:

- You can manage and modify your Apple ID settings from a number of places. Learn Where to Log In with Your Apple ID.
- From iTunes to iCloud, your Apple ID is the key. Explore the many ways Apple uses it in Understand Your Apple ID.

Take action to keep control of your account:

- Take a few precautions up front to Prevent Apple ID Problems.
- Make your account more secure by requiring a token to complete the Apple ID login process. Read Use Two-Factor Authentication.

Work with multiple Apple IDs:

- Many of us wound up with two (or more Apple IDs). I cover how to deal with that in Manage Multiple Apple IDs.
- If you're ready to stop sharing an Apple ID or need to create a new one, I walk you through the steps in Split or Migrate Apple IDs.
- Spend a lot of time abroad? Discover winning strategies for when you need to Work with Apple ID Across Countries.

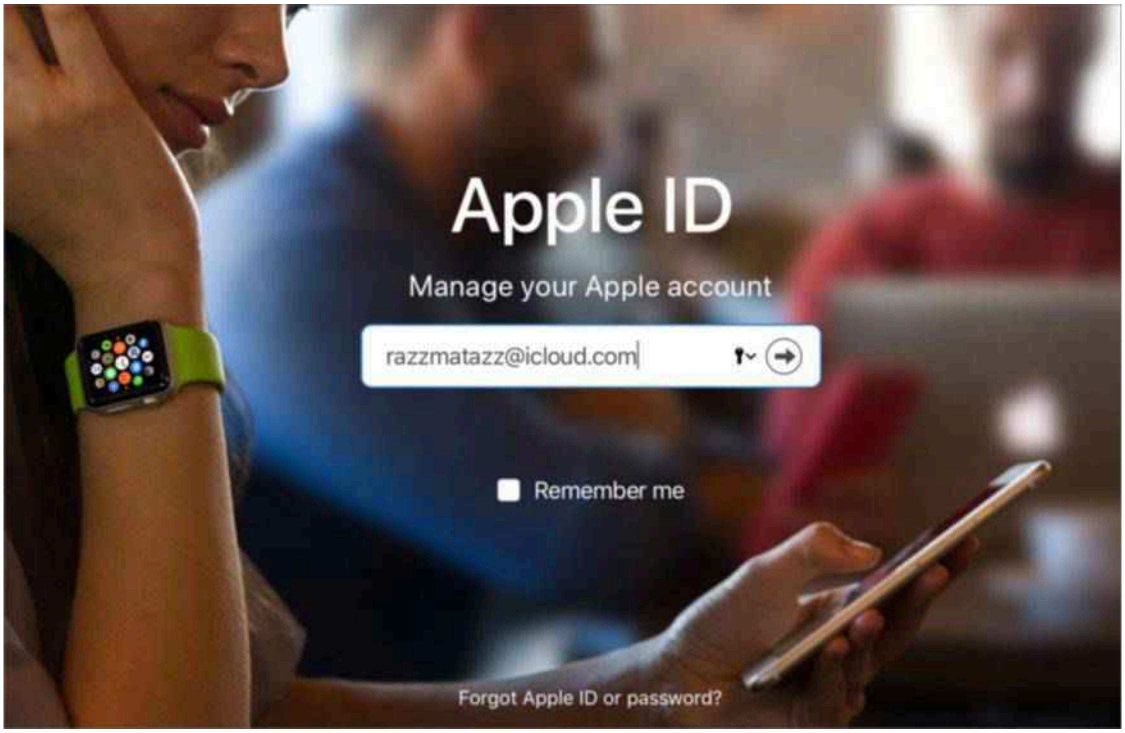
Solve problems:

- It can be particularly unnerving when hackers attack. I talk you through how to Cope with a Hack of Your Apple ID Account.
- From resetting your password to updating a credit card, learn how to Solve Common Problems.
- Used Apple products for ages? Your Apple ID may have some eccentricities. That's covered in Appendix A: Legacy Apple ID Issues.

Where to Log In with Your Apple ID

You can manage and modify your Apple ID settings, such as passwords and associated personal information, from a number of places. I'll refer to these throughout the book, but here's a summary of how to reach each one:

- **The Apple ID website:** Some Apple ID settings can only be dealt with at appleid.apple.com, like generating app-specific passwords with two-factor authentication, while most account details can be changed either at the site or in iOS or macOS (**Figure 1**).



razzmatazz@icloud.com

Figure 1: Use the Apple ID website for many account-related modifications and updates.

- **Apple's iForgot website:** Visit iforgot.apple.com when you need to reset a password or recover other lost account details.

- **Account settings in iOS:** Open Settings, tap your account name, and tap Password & Security for authentication-related stuff. The iCloud and iTunes & App Store sections control which account is registered for those purposes. You can also change which Apple ID you use for a particular service by going to, for example, Settings > Messages > Send & Receive or FaceTime > Settings.

- **iCloud preference pane in macOS:** Manage all iCloud settings for an associated Apple ID at Apple > System Preferences > iCloud.
- **iCloud app in Windows:** Windows users will find everything for iCloud in this app.
- **iTunes in macOS and Windows:** Manage which Apple ID you use in the iTunes Store to purchase and download media by going to Account > View My Account.
- **Books in iOS and macOS:** The Apple Books Store has its own Apple ID login. Find it in the app at Store > Sign In.
- **App Store in macOS:** The Mac App Store also manages its own Apple ID login at Store > Sign In.
- **Apple Music:** The Apple Music app in iOS and Android and Apple Music within iTunes for macOS and Windows all relies on an Apple ID.
- **Find My iPhone/iPad in iOS:** This app can help you find a lost or stolen device as well as recover a lost account password. I discuss how in Reset Your Password.

Understand Your Apple ID

Your Apple ID acts as a sort of informational and financial clearinghouse for all the ways in which you interact with Apple's hardware, apps, and services. As a result, it sometimes feels like 20 pounds of flour crammed into a 5-pound sack.

Fundamentally, Apple IDs are usernames with passwords attached, but because they're used in so many different ways, they've accrued a lot of disparate data and responsibilities. You see this as a user in the Apple ecosystem. You have to enter your Apple ID and password over and over (and over) again, because Apple oddly decided to not use some kind of centralized credential control systems for many of its different services. Every service seems to have its own login dialog and procedure.

In this chapter, I introduce how the Apple ID evolved, what the credentials are used for, and all the many places in which you might be called upon to enter one.

What's an Apple ID?

An Apple ID account always comprises two parts: a username that's in the form of an email address, which is also the primary way for Apple to reach you; and something that *authenticates* you—a way to prove you're the valid holder of the account.

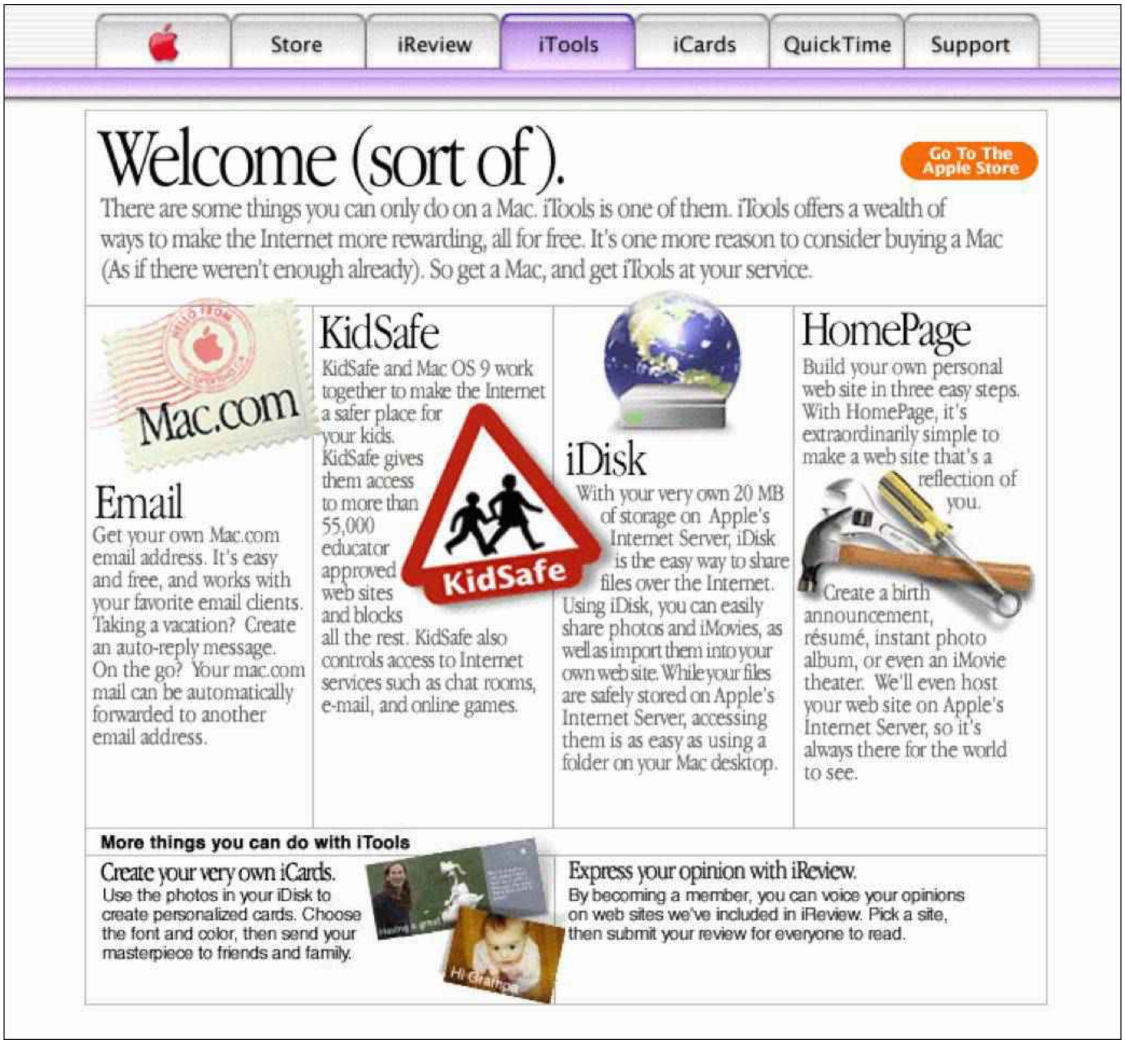
While an Apple ID can have multiple email addresses associated with it, for backup communications and rescue purposes, it only has a single password associated with it.

Depending on the way your account is set up, authentication may be through a password or a password plus a login token. I explain how login tokens work in Use Two-Factor Authentication.

From a Murky Past, Apple ID Emerged

Long-time Mac users will remember that Apple started offering cloud-based services many years ago, before the term *cloud* began to mean “a bunch of servers that appear like one entity and I don’t know where any of the hardware is.”

Apple started its internet-based offerings under the name iTools in 2000, not long after Steve Jobs resumed control of his company (**Figure 2**). It included some online storage and let you host a website.



Welcome (sort of).

There are some things you can only do on a Mac. iTools is one of them. iTools offers a wealth of ways to make the Internet more rewarding, all for free. It's one more reason to consider buying a Mac (As if there weren't enough already). So get a Mac, and get iTools at your service.

Email

Get your own Mac.com email address. It's easy and free, and works with your favorite email clients. Taking a vacation? Create an auto-reply message. On the go? Your mac.com mail can be automatically forwarded to another email address.

KidSafe

KidSafe and Mac OS 9 work together to make the Internet a safer place for your kids. KidSafe gives them access to more than 55,000 educator approved web sites and blocks all the rest. KidSafe also controls access to Internet services such as chat rooms, e-mail, and online games.

iDisk

With your very own 20 MB of storage on Apple's Internet Server, iDisk is the easy way to share files over the Internet. Using iDisk, you can easily share photos and iMovies, as well as import them into your own web site. While your files are safely stored on Apple's Internet Server, accessing them is as easy as using a folder on your Mac desktop.

HomePage

Build your own personal web site in three easy steps. With HomePage, it's extraordinarily simple to make a web site that's a reflection of you. Create a birth announcement, résumé, instant photo album, or even an iMovie theater. We'll even host your web site on Apple's Internet Server, so it's always there for the world to see.

More things you can do with iTools

Create your very own iCards.

Use the photos in your iDisk to create personalized cards. Choose the font and color, then send your masterpiece to friends and family.

Express your opinion with iReview.

By becoming a member, you can voice your opinions on web sites we've included in iReview. Pick a site, then submit your review for everyone to read.

Figure 2: The original Apple cloud service: iTools.

iTools also let users claim a unique account name—one that for many of us persists as at least one of our Apple IDs! A friend registered my

Prevent Apple ID Problems

It's likely you acquired this book to solve problems, but I want to start off by telling you how to *prevent* common ones. These issues mostly affect account access when you lose a device, forget or lose a password, experience a hacking attempt that leads Apple to lock your account, or otherwise need to regain access.

These options vary by how your Apple ID is protected. In advice below, I note in parentheses which account types you can use each bullet point with:

- ***(password)*** for accounts only protected with a password
- ***(2SV)*** for accounts relying on the older two-step verification method
- ***(2FA)*** for Apple IDs that use the newer two-factor authentication

For more information about two-factor and two-step logins, read Use Two-Factor Authentication.

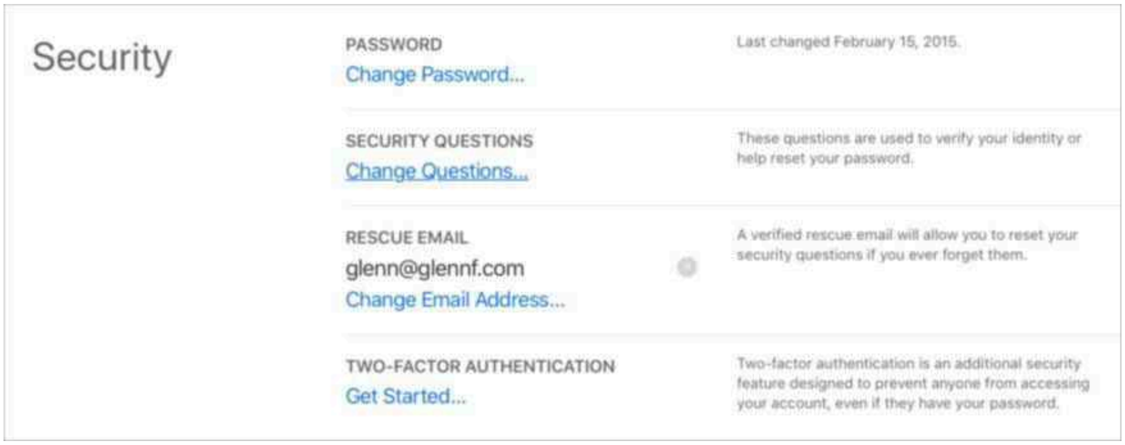
Make Sure You Can Self-Recover

Apple offers a fairly large number of methods that let you regain access to your account without having to convince someone at Apple that you're the legitimate owner of your Apple ID account. You can ease self-recovery by ensuring your account has extra recovery information in it before something goes wrong, like you losing a device, losing access to a phone number, or having to reset a password.

Here are several simple actions you can take:

- **Add rescue email addresses *(password)*:** These addresses provide an alternative if you can't receive email at your main Apple ID address. Add addresses to your password-only account on the

Apple ID site (**Figure 5**). (See this Apple support page for more details.)



Security

PASSWORD
Change Password...
Last changed February 15, 2015.

SECURITY QUESTIONS
Change Questions...
These questions are used to verify your identity or help reset your password.

RESCUE EMAIL
glenn@glennf.com
Change Email Address...
A verified rescue email will allow you to reset your security questions if you ever forget them.

TWO-FACTOR AUTHENTICATION
Get Started...
Two-factor authentication is an additional security feature designed to prevent anyone from accessing your account, even if they have your password.

Figure 5: Use the Apple ID site to manage rescue addresses.

- **Include "reachable at" addresses *(2SV, 2FA)*:** Apple lets you list other addresses that you're "reachable at," but these are only used by Apple in assisted account recovery, not in normal efforts to regain access. (Add these addresses via the Apple ID website, iOS, or macOS.)

- **Add trusted phone numbers *(2FA)*:** With two-factor authentication accounts, you can receive a verification token on an iOS device or macOS device associated with the same Apple ID, or via a phone number as a text message or automated voice message. It may be difficult to add trusted devices, because they can only be associated with a single account. Trusted phone numbers, however, can be reused across Apple ID accounts. You could employ a VoIP number, like Google Voice, or that of your partner, spouse, sibling, or other trusted person as a backup. (Add numbers using the Apple ID site or in iCloud settings in iOS and macOS. See Work with 2FA.)

- **Make sure you have your Recovery Key *(2SV)*:** Only used with accounts that use the older two-step verification method, the Recovery Key is a 14-character code that you use to restore access. If you can't immediately find yours, you can regenerate it. Do that now! Read more in Handle Two-Step Verification.

Use Two-Factor Authentication

If someone acquires the password to your Apple ID account, it can be game over. With a password in hand, a malicious party can log in to see your contacts and calendar entries, read your email and send email as if it came from you, access private photos (yes, people have stolen and distributed nude pictures), lock you out of your devices, and make purchases that they can download.

If you use your iCloud email as a login or a backup email for other services, the password lets an attacker reset your accounts elsewhere because they can receive password-reset emails.

But what if there were a way to keep your password from being the key to the castle? There is! It's called two-factor authentication (2FA). In this chapter, I'll convince you to use it.

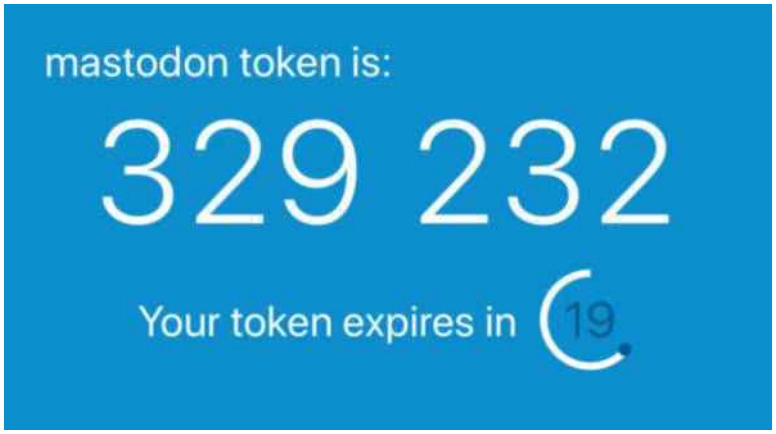
Note: I'll generally use 2FA as an abbreviation for this approach, because it gets tedious to read two-factor authentication over and over again!

How 2FA Works

In the security world, something that proves your identity is called a factor. We typically sort factors into three kinds of elements: something you *know*, something you *have*, and something you *are*:

- **Know:** A password, PIN, or other piece of knowledge you possess.

- **Have:** A device like an iPhone; an authentication app installed on a smartphone, tablet, or computer (**Figure 7**); or a dongle that generates codes in an LCD screen. This factor is something you physically possess or to which you have access.


mastodon token is:

329 232

Your token expires in 19

Figure 7: An authentication app, like Authy (seen here), generates tokens needed for secure login.

- **Are:** Your fingerprint, retina, handprint, and other *biometric* markers that are unique and are part of you. (These can be spoofed in some cases, but not casually.)

With 2FA, you combine two factors—typically a password plus a confirmation step that requires possession of a device. You "prove" you have that device because something appears on its screen or in an app registered on the device. For instance, Facebook and Google let you validate a login by opening their apps on an iPhone and confirming you are trying to log in to your account.

Note: Technically, a Touch ID or Face ID protected iOS device adds another layer of protection. Not only do you have to possess the device, but you also have to use a biometric marker to unlock it. This doesn't quite count as a factor because it's tied in with possession. However, it's yet another hurdle for attackers to jump. They might steal your hardware, but without a fingerprint or your passcode, they can't unlock it and obtain or confirm the second factor.

With two factors, someone who obtains your password is out of luck when they try to log in. They enter it, and then have to provide a code or use another method connected with a trusted device or trusted phone number. Without that, your account remains protected.

While you can enable 2FA for an increasing number of online services and accounts, Apple has its own system for Apple ID that's tied strongly to its hardware ecosystem.

Manage Multiple Apple IDs

Working with iCloud, Apple devices, and Apple's various stores and subscription offerings is easiest when you have a single Apple ID. But I'm not alone in having two for historical reasons, and many people have even more!

In this chapter, I talk about how to manage multiple Apple IDs in an efficient and consistent way.

Use Separate Accounts for Purchases and iCloud

Many of us who are long-time Apple ecosystem participants wound up with two Apple IDs, because at one point, Apple managed purchases separately from iCloud's predecessors (like MobileMe). When Apple fully embraced the Apple ID approach, all our legacy accounts converted. Apple didn't offer an opportunity to merge those accounts then and still hasn't many years later.

Dealing with the duplication wasn't as easy as shutting down one of the accounts. Purchases of permanently licensed digital goods—movies you bought (not rented), any apps, and non-subscription in-app purchases—are associated with an account. We couldn't just abandon an account without also losing all that. Likewise, because the other account was often associated with a mac.com or me.com address we'd used for data or as an incoming address, we couldn't abandon that one, either.

Apple originally didn't design iOS to manage that split of accounts well. Fortunately, that improved many releases ago, and Apple now lets you easily log in to iCloud with one account and the iTunes and App Store with another. In macOS, these services and features were always split across the MobileMe or iCloud preference pane and iTunes.

Use Two Apple IDs in iOS

When setting up an iOS device from scratch with two accounts:

1. Tap Settings > “Sign in to your *device name*.”
2. Enter the Apple ID and password you want to use for iCloud synchronization and other features. Confirm with a second factor if necessary.
3. Tap Settings > iTunes & App Stores.
4. The “Apple ID: *account email*” label at the top likely shows the same account name as in step 2. Tap it.
5. Tap Sign Out.
6. Log in with the Apple ID you associate with purchases, as in step 2.

If you’re not starting with a fresh device, first sign out from all the places you may be signed into an Apple ID on your iOS hardware using instructions you can find in Migrate from One Apple ID to Another.

Use A Different Apple ID with Messages or FaceTime

In this setup, Messages and FaceTime will also be logged into your iCloud-focused Apple ID from step 2. Go to Settings > FaceTime or Settings > Messages > Send & Receive, tap on the “Apple ID: *account email*” link, tap Sign Out, and sign in with your preferred Apple ID.

Use Two Apple IDs in macOS

It’s easy to use multiple Apple IDs in macOS without much fuss. Here’s how to do so with the most common apps and services:

- **iCloud:** Go to Apple > System Preferences > iCloud, type in your iCloud-oriented Apple ID, click Next, and follow steps to complete the login process.
- **iTunes:** Choose Account > Sign In, and enter your purchase-oriented Apple ID, and follow steps to finish.

Split or Migrate Apple IDs

The two scenarios I hear about the most from readers and friends are when two (sometimes more) people have opted to share an Apple ID to sync data and purchases, or when someone finally gives up on having multiple Apple IDs and wants to migrate as much as they can to a single Apple ID—sometimes a new one.

This chapter provides advice for both those tasks, although I want to warn you upfront that the results can be disappointing. Apple doesn't provide help for either process, which means any split or migration will be by necessity incomplete.

Split an Apple ID Between Two People

As the writer of a how-to column about Mac and iOS issues, I never expected to hear a lot about people's relationships, but that was apparently naïve. Our digital devices are, after all, part of our sometimes complicated lives. I frequently receive emails from people with a shared Apple ID who no longer want to share it. The cause can be a breakup, a sibling or child leaving home for school, or just the realization that an individual account will work better for them.

This section offers advice that helps in these cases:

- Permanently separating data (as with a breakup or divorce)
- Creating a second personal account that will continue to share some data, such as recurring calendar events or photos
- Sharing a single Mac currently (with one or more iOS devices shared or each), but with a plan to use separate Macs or have separate accounts in macOS that use different Apple IDs
- Using different Macs (or accounts on a single Mac) that are currently signed into the same Apple ID, but which will be signed into separate ones

The point of view of the instructions below is the person setting up or transitioning to a new Apple ID, thus “taking” data from the current Apple ID.

If you use your Apple ID *only* for purchases or free downloads, this section won’t help you. Apple has never offered any way to transfer ownership of digital assets purchased by an account, nor a way to mark data in an account that could be used to split it. Read the sidebar just below for one potential strategy.

Family Sharing May Offer a Solution

Apple’s Family Sharing option can be a solution for sharing Apple ID purchases and subscriptions among a group of people while letting them maintain separate Apple IDs. When enabled, a family “organizer” can add up to five family members.

This allows everyone in a family grouping—Apple doesn’t check your relationships—to share apps, music, TV shows, books, and movies. Family Sharing automatically creates a shared calendar, reminder list, and photo album. It also allows members to access a subscription to pooled iCloud storage. (The files you store aren’t shared; everyone just gets access to a block of storage at a lower cost than if they’d subscribed separately.)

There’s a proviso: Not all apps can be shared, as it depends on whether the developer allows it. Apps reveal in their App Store pages under the support section whether Family Sharing is included. Learn more about Family Sharing, including how to set it up, in *Take Control of iCloud* or *Take Control of Mojave*.

Manage Local Copies of Shared Data

Start by figuring out where you want all shared data to reside after a split. In all of the cases below, you already have synced copies. What actions you take depend on what you want to keep sharing and whether you’re using a single account on a single Mac or not.

Cope with a Hack of Your Apple ID Account

It's no fun when someone manages to hijack your account. That can be especially unnerving with an Apple ID, because of how it's used widely among Apple's devices, iCloud services, and purchases.

However, Apple has some built-in safeguards to protect your account. Even if someone obtains your password (when 2FA isn't enabled), you'll be notified of many kinds of activities, the hacker may be blocked (even if they have the password), and you should be able to reassert control.

Recognize an Attack in Progress

Be prepared to recognize the signs of an attack *before* someone manages to hijack your account. Here are some things to look out for:

- Apple alerts you when certain changes take place to your Apple ID account information. You'll be pinged, for example, when a new trusted phone number is added or an app-specific password is generated at the Apple ID website for a 2FA account. If you start seeing messages and you haven't made the changes or requests, something's afoot.
- You receive emails to an iCloud address that appear to relate to actions you're taking at other sites, but that you haven't done.
- Your email or other iCloud services stop working on any device or in any program.
- You start to receive two-factor alerts about logins that you didn't initiate.
- The phone company that manages your iPhone's account calls or texts you with a change in service you didn't initiate.

- You receive text messages, like authentication codes for non-Apple services, that you didn't request.
- One of your devices was put into Lost Mode or locked, which can only be accomplished using Find My iPhone/Mac.
- You start seeing charges on cards you own via apps that alert you to charges or email warnings, or you receive a call from a credit card company about suspicious charges.

Tell the Difference Between a Hack and Phishing

It's critical to tell the difference between emails coming from an attack in progress and *phishing*, where people attempt to fool you into providing your login information or financial details.

With phishing, an email message, a text message, or even a phone call originates from dubious sources. Look at the actual return address or Caller ID-provided number. Links are suspicious if, for example, they don't lead to a company's main site. For example, a link to Apple leads to something like apple.euiw098s-f08.90809808adsf8a0d.net instead of to apple.com.

You can also usually tell something's off when the message includes misspellings, weird logos, odd grammar, or strange requests you'd never expect of the sending company or service.

In a hijack, you'll receive emails that typically alert you of a problem *without* providing a link, because real companies know that a link may have you thinking that the email is a phishing attack!

If any of the above are true, it's time to take immediate action to see if you can stop a hacking from gaining control.

Stop an Attack in Progress

You may be able to stop an attack in progress. However, if you can't follow the steps in the first section below, I advise in the second section how to disable your account with Apple's help.

Solve Common Problems

You might encounter a few more tight spots with your Apple ID that you'll need help solving. This chapter rounds up the rest.

Set Up 2FA Without a Device

Apple requires the use of iCloud in macOS or iOS to convert an Apple ID from a regular password-only login into an account protected with two-factor authentication (2FA). But what I've heard from many people with multiple Apple ID accounts is that they only use one across all their iOS devices and Macs, and yet want to enable enhanced security on one or more accounts without messing up their current systems. (For more on 2FA, see Use Two-Factor Authentication.)

This is particularly nettlesome for software developers in the Apple ecosystem, who received notice in mid-February 2019 that after February 27, they could no longer use an Apple ID without 2FA enabled to access developer resources, including the Apple Developer website and the system that manages security certificates. Many developers posted on Twitter that they never use their developer ID with iCloud on any device.

There's a way around this that will work for as long as Apple allows users to opt to send a 2FA verification code to a phone, either as a text message or an automated voice call: set up a macOS account on your own computer or on a trusted Mac. It can even be temporary. Follow these steps:

1. Set up a new macOS user account on the target machine (in System Preferences > Users & Groups).

2. Log in to that account.

3. In System Preferences > iCloud, sign in with the Apple ID that you want to upgrade to 2FA. Follow the steps in Enable 2FA in macOS

to complete the setup. Make sure and include at least two phone numbers at which you can receive codes, and read the Avoid Losing Access section carefully, too.

4. Optionally delete the macOS user account when complete.

The next time you want to log in to any Apple service or site, click “Didn’t receive a verification code” in the dialog, click Text Me, and choose one of your trusted numbers. You can then use the code provided. (See a more detailed step-by-step for this method in Log In with 2FA by SMS or Voice Call.)

Reset Your Password

What happens when your password stops working? You may have forgotten it—it can happen!—or you may have it stored in a password manager and can’t retrieve it.

Whatever the reason, you’re not sunk. Apple lets you reset the password associated with your Apple ID, though how easy it is depends on how your account is set up: with just a password, with the older two-step verification, or with the newer two-factor authentication.

Tip: You can also recover your Apple ID account name, although it’s less likely you’d need to, because Apple typically prefills the account name anywhere you’ve previously entered it.

After resetting your password, you will need to re-enter your password on various devices and for various services.

Reset Your Password-Only Account

If your account is protected with only a password, follow these steps:

1. Visit Apple’s password recovery site, amusingly named “iforgot.”

2. Enter your Apple ID and click Continue.

3. Choose to reset your password.

Appendix A: Legacy Apple ID Issues

In this appendix, we address some legacy issues, including Apple IDs that don't have email addresses and managing two-step verification for an account that hasn't updated to newer versions of the operating system.

Deal with Accounts Without Email Addresses

Apple once allowed Apple IDs using any unique name—no email address required. While the company no longer lets you register those, it didn't disable old Apple ID accounts that relied on a name alone.

This arises as a problem when you want to use an old Apple ID with iCloud, which requires an email address. But it's easily solved. Log in at the Apple ID website using your existing Apple ID, and then change the username to an email address.

Handle Two-Step Verification

Before there was two-factor authentication (see Use Two-Factor Authentication), there was *two-step verification*. In practice, both these systems for protecting your Apple ID aren't radically different: each involve an additional component after entering the password to prove you have physical possession of a registered device or phone. But where the original two-step verification was a bit wonky and hacked to work with existing versions of Apple's OSes and services, two-factor authentication is fully integrated and better designed.

Apple hasn't eliminated two-step support; it's just deprecated its use. As a result, it's possible you may still have it active on an Apple ID. I did for a long while, because one of my Apple IDs was used entirely for purchases. Because I never logged in via iCloud, I was never automatically shifted to two-factor authentication. (I eventually upgraded.)

Note: You can even turn two-step verification *on* for an account that doesn't have two-factor authentication enabled. Visit the Apple ID website, log in, and click the link under Security to enable two-step.

You likely know if an Apple ID has two-step verification enabled, but if you don't, it's easy to find out. Log in at the Apple ID site, and in the Security section it will show a label, "Two-Step Verification," and have the word "On" beneath it. (Also, when you log in, you will have to use a code from an iOS device or via SMS, which is another hint!)

At this point, you have three paths forward:

- Leave it alone, and wait until Apple finally stops supporting it and forces you to change.
- Disable it, and rely on your password. I do not recommend this.
- Upgrade to two-factor authentication manually or automatically.

I explain each of these in turn.

Stay with Two-Step

You can continue to use two-step verification as long as you want. Apple hasn't announced any plans to discontinue it, and it won't automatically upgrade an account to two-factor authentication until it's connected to an iCloud account in iOS 11 or later or macOS High Sierra or later.

The downside with this is that you could wind up in a bind and lose access to your account if you lose the 14-character recovery key created when you set up two-step verification.

You have to have your recovery key if you can't remember your password or Apple locks your account for some reason, which can involve hacking attempts against your account. You also need it to log in if you lose access to all your trusted devices and phone numbers.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

Ebook Extras

You can access extras related to this ebook on the web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the "access extras…" link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the "access extras…" link above. Then, once you are logged in to your new account, add your ebook by clicking the "access extras…" link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control website, contact us.

About the Author

Glenn has written oodles of books over the last 25 years, first for Peachpit Press, and later for Take Control. Mostly recently, he did a complete update of *Take Control of Wi-Fi Networking and Security* for a world without AirPort hardware, and revised his self-published book *A Practical Guide to Networking, Privacy, and Security* for iOS 12. Glenn writes for the *Economist*, the *Atlantic*, *Smithsonian* magazine, *Fortune*, *Macworld*, and TidBITS on topics as varied as Bitcoin, the unique nature of sheriffs in America, buried time capsules, and 19th century printing and typographic history. (Photo credit: Lynn D. Warner)

Acknowledgments

Thank you to Joe Kissell for his constant encouragement, technical support, and for being a delightful advocate of fellow authors.

Shameless Plug

I wrote a book in early 2018 about the amazing typographic history of London told in two remarkable institutions there: the St. Bride Printing Library and The Type Archive. You can get a copy in print or as an ebook of *London Kerning*, a short and snappy book about London and type and printers directly from me at glog.glennf.com/london-kerning.

About the Publisher

alt concepts inc., publisher of Take Control Books, is operated by Joe Kissell and Morgen Jahnke, who acquired the ebook series from TidBITS Publishing Inc.'s owners, Adam and Tonya Engst, in May 2017. Joe brings his decades of experience as author of more than 60 books on tech topics (including many popular Take Control titles) to his role as Publisher. Morgen's professional background is in development work for nonprofit organizations, and she employs those skills as Director of Marketing and Publicity. Joe and Morgen live in San Diego with their two children and their cat.

Credits

- Publisher: Joe Kissell
- Editor: Scholle Sawyer McFarland
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK

More Take Control Books

This is but one of many Take Control titles! Most of our books focus on the Mac, but we also publish titles that cover other Apple devices, along with general technology topics.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the iBooks Store. But it's a better user experience and our authors earn more when you buy directly from us. Just saying…

Our ebooks are available in three popular formats: PDF, EPUB, and the Kindle's Mobipocket. All are DRM-free.

Copyright and Fine Print

Take Control of Your Apple ID
ISBN: 978-1-947282-32-2

alt concepts inc. 4142 Adams Ave. #103-619, San Diego CA 92116, USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM 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, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts inc. 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 alt concepts inc. 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.

It's just a name: Many of the designations in this ebook 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. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: 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 registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a complete list of Apple Inc.'s registered trademarks and service marks.