TAKE CONTROL OF

Securing Your Apple Devices

by GLENN FLEISHMAN

$14.99

Table of Contents

Read Me First

Welcome to *Take Control of Securing Your Apple Devices,* version 1.1.1, published in September 2025 by alt concepts. This book was written by Glenn Fleishman and edited by Joe Kissell.

This book helps you understand all the points of risk and weakness in iPhones, iPads, and Macs, whether using apps on them or accessing the internet, and offers detailed strategies and directions on securing your Apple devices against outside intrusion, including deterring malware, data theft, and account hijacking.

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 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.
- Access the book in both PDF and EPUB formats. (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.

What's New in Version 1.1.1

Apple hasn't fully documented all the changes to FileVault Key Recovery storage in macOS 26 Tahoe. I've discovered and been informed of some additional details, and have updated FileVault Protection (Mac).

I also added a couple of notes to distinguish between the FileVault Recovery Key, created within macOS to aid recovery of your locked startup volume, and the Apple Account Recovery Key, created on one of your devices to aid recovery of your Apple Account!

What Was New in Version 1.1

Since the previous release of this book, Apple released iOS 26, iPadOS 26, and macOS 26 Tahoe. This new year-based numbering system is sequentially after iOS 18, iPadOS 18, and macOS 15 Sequoia. This version updates the book to account for a number of minor changes, largely relating to the new Liquid Glass interface.

Here's what else was new or changed:

- **FileVault on by default:** Starting in macOS 26 Tahoe, FileVault is enabled after you upgrade to that version or in fresh Tahoe installations. See FileVault Protection (Mac). Changes appear throughout the book as well.
- **No more iCloud escrow for FileVault Recovery Key:** To reduce the risk of criminal and government attacks on Macs, Apple no longer offers iCloud-based FileVault Recovery Key storage. See Consider Security and Integrity with the Recovery Key. Changes appear elsewhere in the book related to this.
- **Disable Touch ID or Face ID:** I added a short section that explains how to disables these features on demand or entirely. See Disable Touch ID or Face ID.
- **Consistency on external hardware control:** Apple harmonized its interface and options for iOS/iPadOS and macOS for the

choices you have about external hardware plugged in or inserted, such as via USB or an SD Card slot. See Control Plugging in Hardware.

- **Automatic idle iPhone restart:** I document a security feature added in 2024 to iOS that automatically restarts an unlocked iPhone if it's been idle for four or more days. See Automatic Restart After Four Unlocked Days.

Another sad update is that the world has become more authoritarian in the last year than perhaps any one-year period in modern times. As a result, I recommend you ratchet up your risk level when considering the integrity and privacy of your data while at home and particularly while traveling, even within a country you reside in, are a citizen of, and that you formerly never thought there would be a data privacy risk traveling within.

What Changed from a Previous Book

This book replaced a previous title, *Take Control of Securing Your Mac*, bringing it up to date with macOS 15 Sequoia and coupled with a full expansion to cover iOS and iPadOS security.

If you read any edition of the previous title, here's what was new:

- **Protecting your iPhone & iPad:** A new chapter covers three issues unique to iPhone and/or iPad. In this chapter I cover Apple's Stolen Device Protection feature for iPhone that deflects thieves who extract your passcode through coercion or misdirection. See Protect Your iPhone & iPad.

- **Centralizing Mac features:** This overhauled edition now locates highly Mac-specific security and data privacy features into a single section, Fortify Your Mac.

- **Gatekeeper tightens further:** Apple added protections to their Gatekeeper technology to make it harder to launch "unsigned" apps from running—ones that developers didn't pass through basic Apple oversight. See Override Gatekeeper.

- **Apple improves Private Wi-Fi address:** A feature designed to deter tracking of your devices by their unique network adapter addresses, used by routers when you connect on a network, was improved in the latest releases. I explain the feature in this version of the book. See Ways to Protect a Wi-Fi Adapter's Address
- **Sequoia adds system extension removal help:** Before Sequoia, it was a real pain to find and remove system extensions required by certain hardware and software, like RAID drives, video source extenders, and anti-malware software. Now, you can find them all in a list in System Settings. See Manage System Extensions.

Introduction

Apple's operating systems are not impregnable. Every operating system has flaws that can be exploited through hardware and software, locally and remotely. An attacker might break in to scoop out your personal data, erase files or entire volumes, or install spyware.

Apple never shirked their need to find these holes and plug them. But over the last decade, they have increasingly increased the difficulty of staging successful attacks. They not only backfill problems as they are discovered and build better replacements for vulnerable components, but they have also become better at predicting potential points of failure and erecting thick walls ahead of time.

This book covers everything you should know about what you can configure and what Apple has quietly set up for you, whether you can change those settings or not. This will help you tune your security profile to fit your needs, including whether or not you need to enable some tools useful for people potentially under dire threat. But you'll also learn what Apple doesn't help you with so you can supplement those areas with other software or changes in how you work.

iOS and iPadOS were designed from the start to have protections against installing arbitrary software. Initially, Apple didn't lock down iPhones and iPads sufficiently (to the company's liking), allowing them to be *jailbroken*, and have different operating systems or third-party software installed. That's no longer a thing, and Apple has focused enormous efforts on hardening both platforms. Often, we see security upgrades first in iOS/iPadOS, after which they migrate to macOS.

Apple treats Macs differently, due to their legacy and how people still use them. You can run any software you want, access the Unix innards underlying macOS, and turn off security settings cannot be disabled on an iPhone or iPad. Nevertheless, Apple has managed to fold in better protections continuously for Mac users. For instance, a few years ago, Apple reworked how system files were stored, putting them all onto an unmodified, secured volume for better integrity and protection.

This book looks into security features and options and ways to keep your data private for an iPhone, iPad, or Mac. However, given the openness of macOS and its greater configuration, a larger portion of the book is devoted to it. You'll find the lion's share of Mac-specific advice in Fortify Your Mac, and most iPhone/iPad-focused coverage in Protect Your iPhone & iPad.

One strong intent of this book is to help you understand many improvements Apple has made to protect you against physical attacks. Those are *digital* break-ins where someone sits down *physically* at your Mac or has your iPhone or iPad in their hands. People might plug in a hardware cracking device (like one that would enter a zillion iPhone passcode combinations or subvert the firmware on your Thunderbolt controller), plug an external drive into a Mac or attempt to mount the Mac as a drive on another Mac, or try to guess your passcode or password to gain entry.

Apple's Security Enclave for iPhones, iPads, and Macs and the security levels you can set in macOS recovery mode dramatically improve physical resistance. These measures have special importance if your device is lost or stolen in deterring or preventing access. Apple's Stolen Device Protection for iPhone provides an additional level of resilience against theft when someone obtains your passcode.

This book helps you set up your iPhone, iPad, and Mac to be resilient against these attacks. I also dig into what you can do in case you can't log in to your Mac or unlock your iPhone or iPad, or if any of the those devices are lost or stolen.

Due to significant changes in the latest operating system interface update, coalescing into the Liquid Glass approach, this latest version no longer looks backward. It mostly covers macOS 26 Tahoe, iOS 26, and iPadOS 26.

Note: This update encompasses all M-series Apple silicon Macs released starting in 2020. This book does not focus on Intel-based Macs, as Apple released the last new model with an Intel chip in 2019 and only a few late models are supported by Tahoe.

Quick Start to Securing Your Apple Devices

Security is a multi-pronged process that combines understanding risk, checking status, acting appropriately, and deploying changes and potentially new software. Start by reading two early chapters, after which you can read in any order to learn what to do next and why.

Get grounded in security:

- Understand what security is and how it applies to you; see Start with Security Basics.
- Get started with simple changes and new behaviors; see Set Up Basic Security.

Control access to Mac services and files:

- Discover the role Gatekeeper plays in restricting which apps run, and working within and bypassing those limits; see Apple Protects with Gatekeeper.
- Protect your Mac from attacks by other users or those with access to it; see Configure macOS Accounts Securely and Keep Data Safe from Other Local Users.
- Learn to set up network access without exposing your Mac unnecessarily; see Allow Network Access to Services.
- Block malware and unwanted app intrusion; see Keep Malware off Your Mac and Deter Invasion via Sandboxing.

Configure iPhone and iPad protections:

- Make it harder for thieves or assailants to hijack your devices—and its associated Apple Account; see Manage Stolen Device Protection and Avoid Physical Passcode Theft.

Lock down your devices and your data:

- Avoid losing access to your devices through repeated failed passwords; see Password Lockout Protections.
- Make sure you can recover your Apple Account or macOS account after a hijack or security lock by Apple; see Regain Access.
- Control how cloud services allow file sharing; see Share Carefully via Cloud Services.
- Decide how to use FileVault; see FileVault Protection (Mac).
- Configure disk and boot protection to deter risk from physical access to your Mac; see System File Protections (Mac) and Startup Protections (Mac).

Start with Security Basics

Security has a broad meaning in everyday life, but a more specific one when it comes to data, networks, computers, and mobile devices.

In this chapter, I want to introduce you to what you have at risk and how to set your goals in protecting your Apple hardware as part of the philosophy that you'll find throughout this book.

Understand What Security Means

As a general rule, we talk about *security* when we mean a way to reduce the likelihood of harm. You go through a *security* checkpoint at the airport. You have a home *security* system. A lecture is cancelled due to *security* concerns. An ad for a bike lock claims it offers high *security*.

With computing and networking, however, security is more specific: it's the measures you take to prevent harm to you by the extraction, interception, loss, or corruption of your *data*.

Note: You may also see the term *exfiltration*, which sounds highly technical, but means just the extraction of data from a device, often over a network to a malicious or unwanted recipient.

It's rare that a violation of your device's security would result in *physical harm* to you or anyone else—unless someone attacks you while also stealing your equipment. That's quite rare in a home or office, but it can happen when out and about, where an assault or threat of it could lead you to reveal your iPhone passcode or other passwords.

Note: While it's also rare to be attacked, or even drugged, to get your passcode, it does happen often enough that Apple added a new protection. See Manage Stolen Device Protection.

But even without a physical assault or fear of it, you can suffer emotional harm from the sense of invasion or damage that results from an invasion, particularly if someone violates your security to steal personal information that is then disseminated or used against you.

You can also certainly incur financial damage (theft of identity or money), waste your time (canceling credit cards, changing passwords), find yourself spending hours coping with the aftermath (removing malware, restoring deleted files), and so on. If your Mac became part of a botnet, you could also harm *other people's* devices. As a result, your ISP might temporarily cut off your internet service to block attacks coming originating from inside its network.

Apple's security options through the mid-2010s focused mostly on resisting attacks carried out over a network and exploits that relied on software that was downloaded and installed with or without your permission. In the new era stretching back several years now, Apple has shifted increasingly to giving you tools and automatically protecting your data when someone can take physical control of your device.

The company also puts a lot of attention on blocking exploits and malware in macOS, which, because it allows any software to be installed, remains more vulnerable; the network as a vector for compromising a Mac is nearly entirely ignored. It's different with iOS and iPadOS, as the key vector for attack there seems to be phishing text messages and attachments, which has led Apple to a constant cycle of hardening Messages and related components.

Protecting against physical attacks requires your device to resist intrusion. That intrusion might be someone merely sitting down in front of a Mac for a few minutes and extracting the contents of your drive without leaving a trace, popularized by hackers in movies. But it more frequently includes deterring a thief who has purloined your iPhone, iPad, or Mac—whether for a period of time or forever—from successfully cracking it at their leisure

Set Up Basic Security

Time to start improving your security! This chapter contains steps so fundamental to your security that you'd be doing yourself a huge disservice to avoid them. Just as you need to check that the appliance is plugged in before you call customer service, the steps in this chapter constitute a sort of minimum threshold for security awareness.

This chapter covers keeping Apple's operating systems and third-party software up to date, setting up biometric authentication with Touch ID and Face ID, and protecting yourself against peripherals and other hardware plugged into your devices.

Keep Your Software Up to Date

It's a fact of life: software has bugs. And some of those bugs result in security vulnerabilities. Fortunately, most major software vendors, including Apple, have teams of programmers working constantly to identify and fix security-related bugs.

I can't tell you how many times I've read breathless news reports about some newly discovered and seemingly disastrous Apple security issue, only to see a software update from Apple fix it a few days later before any damage occurs. This is Apple's normal pattern, and it's why you should never lose sleep about the security crisis *du jour*.

However, Apple security updates don't help unless you install them! If you have automatic software updates turned off and ignore alerts or badges, you could be needlessly putting your devices and your data at risk from problems that were solved months or years ago.

Software updates fall into several categories, *all* of which can fix security issues:

- Major upgrades, such as from macOS 15 Sequoia to macOS 26 Tahoe or iOS 18 to iOS 26

- Minor updates, which can be small increments for big fixes (26.1.0 to 26.1.1), or larger ones when they include feature changes but not a full OS upgrade (such as 26.0.1 to 26.1)

Apple Resets the Number Wheel

Starting with fall 2025 operating system releases, Apple reset their numbering system to the last two digits of the following year, starting with 26. So 2025 releases are iOS 26, iPadOS 26, macOS 26 Tahoe, tvOS 26, and watchOS 26.

- Standalone security updates that fix specific pieces of system software, usually stuff deep beneath the surface (most common with a Mac)
- Updates to individual Apple apps (Safari, Music, Books, QuickTime Player, etc.)
- Updates to third-party apps

Which of these should you keep up with? Ideally, all of them, but at a bare minimum, install the standalone security updates. After ensuring you haven't heard of any problems other people have had, install minor updates. Major updates require more planning and include quite a lot beyond security fixes.

Tip: To learn about all Apple software updates with security implications, see the Apple security releases page. Click a specific update to read the security details.

Fortify Your Mac

Let's narrow the focus from all of Apple operating systems for a moment and look at all the ways in which you can mediate, filter, and control how your potentially very open Mac handles its security and your private data.

In this chapter, I cover a broad range of Mac-specific security and privacy features. I start with basic settings and how to create new accounts in macOS. I then move on to Gatekeeper, Apple's app-restricting technology designed to deter malicious software, and more general advice on avoiding malware.

From there, I take you through safe networking setup, protecting data on one macOS account from other accounts on the same Mac, and understanding Apple's sandboxing approach, which lets you limit how each apps accesses other data on your Mac.

Manage Security and Privacy Settings

macOS has many privacy and security settings that can be turned off or tuned, reflecting in part how you interact with a computer versus a mobile device. Let's start with System Settings > Privacy & Security (**Figure 8**), which collects several controls and options. I also mention settings in Users & Groups, and Lock Screen, and in the Keychain Access utility, that deserve a quick look.

Note: Find out more about macOS FileVault in FileVault Protection (Mac).

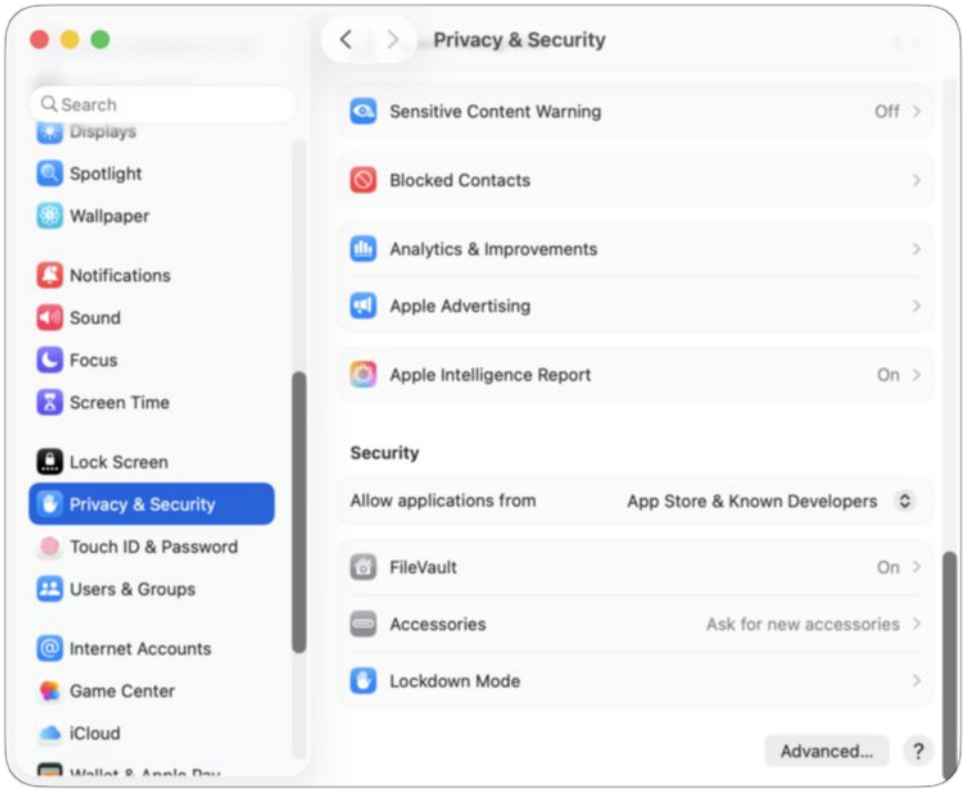

Figure 8: Set some of the most important security options in Privacy & Security in Tahoe.

Unlock the Pane or Setting

Apple requires you prove your identity when accessing more sensitive elements of System Settings. First, click a setting, like changing "Allow applications from" to App Store. Now:

- **Touch ID:** If you have Touch ID, you're prompted for biometric authentication. You can also click Use Password to enter the account password and then click Unlock.
- **No Touch ID:** You're prompted to type in the administrator password. Enter it and click Unlock.

Some settings, like Users & Groups, prompt for your administrator password even with Touch ID installed.

With an Apple Watch, you can also unlock many settings by using a side button double-press. Go to System Settings > Touch ID & Password and enable your Apple Watch under "Use Apple Watch to unlock your applications and your Mac."

That option also lets your Apple Watch unlock your Mac's screen, as I describe a few pages ahead.

Protect Your iPhone & iPad

With macOS given its due in the previous chapter, this one is devoted to iOS and iPadOS protections for your iPhone and iPad—and how to craft your security profile for even better data and personal security.

I start with a feature introduced for the iPhone only in iOS 17, Stolen Device Protection, designed to help you resist physical theft combined with passcode extraction. To further that end, I then provide more general information about how to avoid physical passcode theft, though only some aspects are truly within your control.

Finally, I discuss specifics for managing your passcode and setting up an iPhone or iPad to force its use on demand.

Manage Stolen Device Protection

Apple introduced a hidden flaw when they made it possible to use your iPhone or iPad to reset the password for your Apple Account. There was a perfectly good reason to make this linkage: if you could access the password-changing part of the interface, that meant you possessed your device, could unlock it via your face, fingerprint, or passcode, and had the passcode for further changes.

If Apple hadn't let people reset their Apple Account password with their device, they would have potentially hundreds of thousands of support calls a year dealing with this issue. Instead, resetting is a relatively trivial matter—easy to find instructions online and easy to help someone with if it requires an Apple Support call or text.

However, as you can read about below, in Avoid Physical Passcode Theft, it's possible through subterfuge or violence to obtain both an iPhone and its passcode, at which point someone could hijack your Apple Account and leverage access to your phone and that account to take over your life.

Stolen Device Protection takes the fangs out of this viper. It has a number of tradeoffs, but it may be worthwhile for additional peace of mind for some people. Here's what to consider:

- It is not enabled by default. You have to choose whether or not it's useful to your circumstances, and then opt in.
- It's available only on iPhone, with Apple ostensibly reasoning it's the most at-risk device for theft coupled with passcode acquisition.
- While enabled, your iPhone passcode cannot be used for a host of actions related to passwords, payments, tracking, and erasure. You must use Face ID or Touch ID.
- Apple imposes a new one-hour delay between when you want to make certain kinds of Apple Account, biometric, passcode, or tracking changes and when you are allowed to make them.

> ***Warning!*** Starting in iOS 18, if you turn off or restart your iPhone, the timer restarts, counting down again from a full hour. That new hour is counted from when your device finishes its restart cycle or from the next time you power it up.

That sounds a bit annoying, no? Well, here's the kicker: when enabled, the biometric requirement for some features and one-hour delay for others apply by default only when you are in an "unfamiliar" location. That's right: Apple uses secure device-based stored information—to which they don't have access—to determine whether you're at a place you regularly linger at, like home, work, or a neighborhood pub (**Figure 43**). If you aren't then the extra protections enable automatically.

That means when you're at a familiar location, you won't notice at all that Stolen Device Protection is on. If you return while using your device from an unknown to known location, the restrictions drop, too. You can opt to disable this "familiar location" feature, too, if you want the same level of deterrence everywhere.

Control Device Data Integrity

Apple builds in a huge array of tools that help if your device is physically compromised, as when someone gains access to your iPhone or computer without your permission, someone takes your device away without your knowledge or steals it in order to try to break into it, or when someone extracts hardware (like a drive) from your Mac.

Apple created the chip-based Secure Enclave technology for iPhones and iPads, then expanded it for Macs starting with Intel models. It's integral part of M-series Macs. Secure Enclave was a big improvement for device security and data integrity.

But Apple has layered much more underneath and around it. In this chapter, I start by explaining how the Secure Enclave works, and then proceed to talk about Mac-specific issues: disk encryption and encrypting disks, protecting your startup drive, and working with Apple's security safeguards.

I also dig into the way Apple limits password attempts, and your options for making sure deleted files on a Mac can't be recovered by someone else later. I conclude with a quick look at how Apple Pay can be disabled on a Mac with a Secure Enclave and Touch ID when you switch among users or multiple startup volumes.

Note: The first two sections in this chapter apply to all platforms; the remainder are Mac-only issues.

The Secure Enclave

Apple created the Secure Enclave processor, first for the iPhone, as a way to provide a tamper-resistant one-way vault to handle encryption secrets, biometric information, and many kinds of private data. The

design of the Secure Enclave prevents Apple from accessing information inside it, so the chip that contains it can't be removed or manipulated without almost always destroying its contents.

A Piece of a Bigger Piece

Technically, the Secure Enclave is a component of a system on a chip (SoC), which is a single piece of silicon that integrates all the components normally in separate chips—like a CPU, memory, and various input/output chips.

The Secure Enclave processor is part of all M-series Apple silicon Macs. It's also found in Intel Macs with the T1 Chip (for the Touch Bar) or T2 Security Chip; you can find a complete list of starting models in an Apple support note. All Macs that can run Sonoma or later have a Secure Enclave. You can install macOS 26 Tahoe on all M-series Macs, but only the last series of Intel models support it. (Most Macs with a Secure Enclave can run macOS 14 Sonoma or later, but fewer work with Tahoe.)

All iPhones from the iPhone 5s model forward have it, as well as all iPad models across all variations introduced since the iPad Air in 2013.

Note: Not surprisingly, all of Apple's other devices with its A-series mobile chips also have a Secure Enclave: the Apple TV (HD and later), Apple Watch (all models), and HomePod (all models).

The Secure Enclave is used for a number of different purposes, some of which are directly relevant to this chapter:

- **Touch ID/Face ID:** Fingerprints are enrolled and stored securely within, and logins send patterns to the Secure Enclave to match.

Note: The Magic Keyboard with Touch ID enables fingerprint recognition on M-series Macs by pairing directly with the Secure Enclave in a proprietary secure wireless process.

- **SSD encryption:** All iPhones and iPads with a Secure Enclave encrypt all data stored on their invisible "startup volume." All Macs

Keep Personal Data Private

As we've seen, security and privacy have a complex relationship, but improving your security can often increase your privacy—and in fact, keeping your data private is one of the most important reasons to take security measures. Some of the steps that lead to greater privacy don't involve security in the strictest sense, but they're no less important just because they fall on one side of that conceptual line. This chapter explores a grab bag that contains five of those topics.

I start by looking at features in iOS/iPadOS and macOS for sharing files via cloud services, mostly with iCloud, but also including some third-party cloud services.

I take what appears to be a slight detour—but isn't—into Advanced Data Protection for iCloud that provides end-to-end encryption for most kinds of data you sync among devices. It's a new layer of protection for data stored on your devices.

After this, passwords are the subject: Apple stores passwords across their operating system in different ways, and you should know where they are and how they're protected.

Finally, I address Lockdown Mode, an extreme protective measure Apple intends for users at greatest risk, available for all their operating systems. Are you one? Does it help? Read on.

Share Carefully via Cloud Services

Because of the fraught nature of putting your devices or services on them directly in the path of the entire internet, it's almost always the case that you can share files more easily, with more control, and more securely using a cloud-based sharing service, with a lot of provisos that I describe along with each service.

Each of these services *partitions* access, so you know precisely what you are letting someone view or download, and whether they can

modify, delete, or upload files. You can set a time limit that a link will work, and usually restrict whether something can be downloaded or just viewed online. You may also be able to tell when they access or view files and see exactly what changes they make, if they have permission to modify files.

All the major tech companies offer them, and you may already have free access to substantial storage, or already be paying for a subscription plan or higher level of storage for other purposes.

All of these services encrypt data at rest and use encrypted transport (HTTPS, primarily) for uploads, downloads, and link creation. However, if someone is able to access your account, they can view, delete, modify, download, and add files without any restriction.

If you want to share files in a truly secure, end-to-end manner, however, the gold standard is end-to-end encryption (often abbreviated E2EE). With E2EE, the ecosystem you use generates and retains keys only at endpoints, on devices under your control. (Sometimes you're involved in generating them, but usually the key creation and management is silently handled by the software.)

Data accessible by logging in to iCloud.com never included E2EE before December 2022. Then Apple added an option for iCloud that everyone who can should take advantage of: Advanced Data Protection (ADP). ADP requires at least macOS 13.1 Ventura, iOS 16.2, or iPadOS 16.2. With ADP, iCloud Drive and other items synced, shared, and available via iCloud.com are now protected by E2EE for you and with people with whom you share—so long as they also ADP enabled. See Enable Advanced Data Protection for more on ADP.

If you or your shared partners don't have ADP enabled or can't turn it on, you can layer E2EE on top of standard secure cloud services, because data that's encrypted before transfer and stored in these locations remains encrypted, and is only decrypted by end points that have the keys.

That is, if you have an encrypted disk image and upload it, that integral encryption isn't stripped off. If someone downloads the disk image,

Regain Access

One of the most unsettling things that can happen to your device and your data is when you are locked out from your computer. It's rare, and you can prepare against the possibility so that your recovery is quick—or at least feasible, if not fast.

Prepare for a Future Lockout

An ounce of prevention saves a metric kiloton of care when it comes to accounts and access. If you follow the following advice ahead of time, you can avoid serious downtime and loss of data.

Keep Fresh Backups

I've said this repeatedly throughout this book, but backups are the strongest protection you can have against theft, destruction, and loss, including "loss of access."

If you have daily backups of you Mac and attached drives onsite (via Time Machine or third-party software), copies of your startup volume and external drives offsite, active continuous or daily cloud-hosted backups, or use a sync service to ensure multiple copies and a version history of your active documents, losing access to your Mac still has a sting, but you likely will lose very little data, if any.

Note: You could be like me and do all four. But that's me.

In some cases, you might be locked out of your current Mac, such as with a FileVault failure or the loss of a Recovery Key. In those cases, you can erase the computer and restore from a full backup, putting you right back in business. Or you may be able to use an external drive or synced files to get back to work on another machine—perhaps a borrowed one—while you plot unlocking the Mac you can't get to.

Warning! Macs that support Activation Lock and have it enabled by turning on Find My Mac require that you can log in to your Apple Account to erase the computer. I explain this is more detail just below, in Reset Password via Activation Lock.

With an iPhone or iPad, your biggest job is ensuring you have enough storage in your iCloud+ plan to allow iCloud backups. You can also use a Mac for device backups, but that dramatically increases the odds you'll be out of date and missing data. With automatic iCloud updates enabled and using iCloud Photos, it's unlikely you would lose any data—at worst, very little.

Passwords

You should have a go-to, secure place for all passwords, passkeys, and other login and encryption keys you may need in the event of a disaster, including:

- Passwords for one or more administrator accounts on your Mac
- Passcodes for any iPhones or iPads
- The Recovery Key for macOS's FileVault; see Manage FileVault under Tahoe
- The account name and password or passkey (or hardware security keys) for your Apple Account (or Accounts)
- The password for your password manager (which may be the sole item you memorize, and you may also provide a copy to a lawyer, sibling, or trusted party to hold securely)

This secure password repository should preferably be available from a device or location that isn't tied to where you keep your hardware.

Check Trusted Security Elements

With two-factor authentication (2FA) enabled on your Apple Account, you might be locked out permanently if you lose access to trusted devices, and trusted phone numbers for SMS and automated voice

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.
- Access the book in both PDF and EPUB formats. (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.

More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on Macs and other Apple products.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the Apple Books 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 two formats, PDF and EPUB, which are viewable on any computer, smartphone, tablet, or e-reader. All are DRM-free.

About the Author

Take Control Books Executive Editor Glenn Fleishman never stops writing about technology and its implications. He's in his third decade of writing for publications as varied as *American History*, *Fast Company*, the *Economist*, Increment, the *New York Times*, *Macworld*, and TidBITS, and many others. In 2012, he was a two-game champion on Jeopardy!

You can find Glenn on Mastodon (@glennf@zeppelin.flights) and Bluesky (@glennf.com). Reach him by email at glenn@glennf.com.

Shameless Plug

I don't write just ebooks—I also produce ones of actual physical matter. My latest two are *How Comics Are Made: A Visual History from the Drawing Board to the Printed Page*, about the production and reproduction of newspaper comics; and *Six Centuries of Type & Printing*, tracing the evolution of type and printing technology across 600 years.

About the Publisher

alt concepts, 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 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 Saskatoon, Saskatchewan, Canada, with their two children and their cat.

Credits

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

Copyright and Fine Print

Take Control of Securing Your Apple Devices
ISBN: 978-1-990783-60-9

alt concepts, 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

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 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 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.