EBOOK EXTRAS: v1.2
Downloads, Updates, Feedback

TAKE CONTROL OF

SECURING YOUR MAC

by GLENN FLEISHMAN

$14.99

Table of Contents

Read Me First

Welcome to *Take Control of Securing Your Mac,* version 1.2, published in October 2021 by alt concepts inc. 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 using macOS on its own and connected to the internet, and offers detailed strategies and directions on securing it against outside intrusion, including deterring malware 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.

About a Previous, Related Title

Take Control of Securing Your Mac is the spiritual successor to Joe Kissell's book *Take Control of Security for Mac Users*, last updated in 2015 and discontinued in early 2017. As Apple has changed and added options for security, encryption, and privacy, it felt like this subject was a missing piece in our lineup.

This new book adapts parts of the previous work, but it's full of fresh information and has been overhauled to reflect the choices and risks present in 2021.

Tip: This book is also a counterpoint to my separate title, *Take Control of iOS & iPadOS Privacy and Networking*, which covers remarkably little of the same material due to the different nature of how each platform handles privacy and offers security choices. (The big overlap is in Safari across all platforms.)

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.

What's New in Version 1.2

This version of the book updates details throughout for changes that appeared in macOS 12 Monterey's public releases through early October 2021. This book will be updated with any changes required when Apple ships Monterey's production release.

Many of the changes were superficial, but more significant ones that require rethinking how you set up and use macOS include:

- **Touch ID:** With the addition of Touch ID as an option for M1 Macs through the Magic Keyboard with Touch ID, I've added a recommendation to enable Touch ID and provided more details in one place about how it works to the chapter Set Up Basic Security: Enable Touch ID.
- **Changes and expansions to Gatekeeper:** Apple has made some subtle changes to its Gatekeeper software-installation guardian relating to opening virus-free apps from known developers that aren't in the App Store. I also expanded slightly on some of the

and added more screenshots to them. See Apple Protects with Gatekeeper and Override Gatekeeper.

- **iCloud Private Relay:** Apple now offers an anonymity-protecting relay service for Safari browsing that's included with iCloud+, their new name for the upgraded paid tiers of iCloud service. Because this helps protect both your privacy *and* aids in security, I cover it in Protect Anonymity via a Private Relay.
- **Verification codes and password changes:** Safari 15 for macOS and Monterey both introduce changes in how you interact with passwords for websites in macOS. This is covered in Where Do Your Passwords Reside? and 2FA Codes via SMS, Voice, and Authentication Apps.
- **Monterey Passwords preference pane:** Apple added a Passwords pane to System Preferences, providing access to the password manager that was formerly found solely inside Safari's preferences. This is noted as appropriate.
- **Find My:** This book originally included a small section on using Apple's Find My ecosystem to recover lost and stolen items. However, the subject has become so large and complex—and isn't actually about the kind of security discussed in this book—I took the portion in *Take Control of iOS and iPadOS Privacy and Security* and this book, we released it as its own, expanded multi-platform title: *Take Control of Find My and AirTags*.

Introduction

A Mac is not impregnable. Any operating system has flaws and weaknesses 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 raised the level of 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.

Macs have nearly always been better than Windows at deterring remote attacks, and modern malware recognizes that degree of immunity. Instead of trying to hammer away at your Mac over the internet, the focus now is on fooling you into making a bad choice disguised as a good one to subvert your computer. Ne'er-do-wells try to convince you to visit a website, download a malicious program, and launch it, and then bypass additional protections. That's a high bar to cross. Yet Apple keeps raising it by making it harder for you to install unwanted and misleading software and largely preventing such apps from launching at all.

In this book, I show you all these protections, along with how to configure them to offer resilience without making your computer experience less pleasant. You also learn how to add additional software that can increase your security and privacy.

While making these improvements over the last decade, Apple has simultaneously strengthened protections against physical attacks. Those are *digital* break-ins where someone sits down *physically* at your Mac. An unwanted party might attach an external drive, connect your Mac to another Mac, plug in a hardware cracking device (like one that would try to subvert the firmware on your disk controller or Thunderbolt controller), or simply tap away at the keyboard to gain

entry. Apple's upgraded protections—including the Secure Enclave and security levels you can set in recovery mode—dramatically improve physical resistance. These measures have special importance if your computer is lost or stolen, which affords someone as much time as they want to try to gain entry.

In the last few years, Apple has also hardened the core part of macOS—all its system files, background processes, and preinstalled programs. With Mojave, Catalina, and Big Sur, Apple pushed out rugged improvements that keep system files from being modified or overwritten—even someone who has a system administrator account can't modify these files while macOS is running. Making changes to a Mac's copy of macOS through other means—such as mounting it as a drive—will be detected at its next startup. Recent Mac hardware has layers upon layers to prevent a modified system from running at all. (Monterey just stayed the course! No major system revisions.)

This book helps you set up your Mac to be resilient against physical attacks. I also dig into what you can do in case you can't log in to your Mac, or if it's lost or stolen.

Which Models and OS Releases This Book Covers

Because of Apple's continuously improving Mac software and hardware security, this book is largely limited to macOS 10.15 Catalina, 11 Big Sur, and 12 Monterey (public beta, October 2021). That encompasses several years' worth of Mac models:

- Macs that can run Catalina, dating back to 2012; see this list
- The short-lived 2015 and 2016 12-inch MacBook with USB-C
- 2016 MacBook Pros with Thunderbolt 3 and the T1 security chip
- 2017 and later Macs with Thunderbolt 3 and the T2 security chip (includes a Secure Enclave)
- M-series Apple silicon Macs released starting in 2020

Note: Looking for more help in deciding to buy, migrate to, configure, and secure an M-series Mac? Check out my book dedicated to all M-series specifics, *Take Control of Your M-Series Mac*.

Quick Start to Securing Your Mac

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.

Open up access to services and files:

- Learn to set up network access without exposing your Mac unnecessarily; see Allow Network Access to Services.
- Make use of cloud services for sharing; see Share Carefully via Cloud Services.

Lock down your Mac and your data:

- Protect your Mac from outside attack and snooping; see Fortify Yourself and Your Mac.
- Configure disk and boot protection to deter risk from physical access to your Mac; see Learn macOS Startup and Disk Protections.
- Avoid exposing your data; see Keep Personal Data Private.
- Prepare for and recover from lost access; see Regain Access.

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 Mac 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 Mac's security would result in *physical harm* to you or anyone else—unless someone breaks in and attacks you while also stealing your Mac.

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 becomes part of a botnet, you could also harm *other people's* devices. You might, as a result, also have your internet service cut off temporarily by your ISP in an attempt to block attacks coming from inside its network.

Previously, Apple's security options focused mostly on resisting network-based attacks or local ones from software that was downloaded and installed with or without your permission. But Apple has stepped up tremendously over the last few years in a new area: protecting your data when someone can take physical control of your Mac.

That includes someone merely sitting down in front of your machine for a few minutes and extracting the contents of your drive without leaving a trace, popularized by hackers in movies; or someone purloining your computer temporarily or indefinitely to try to crack into it at their leisure or with specialized equipment. It could be as simple as them rebooting a Mac from a USB drive, installing malware, and restarting—or as fiendish as a little hardware tap.

As a result, you now should think both about the *digital* sense of security and the *physical* sense:

- The digital part involves protecting your passwords, guarding against remote attacks over the internet, and halting the delivery, installation, and deployment of malware.
- The physical part involves configuring and understanding Apple's features that deter hands-on attacks, up to and including someone removing a motherboard or an SSD or hard disk drive.

Note: There's a limited case in which adding security might give someone a way to lock you out of your computer remotely! I discuss how that attack works and how to prevent it in a separate book: *Take Control of Find My and AirTags*.

Improving your Mac's security reduces the chance of certain harms:

- Loss of data

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 chapters covers keeping macOS and third-party software up to date, configuring security and privacy settings in macOS (particularly regarding locking your Mac when you're not in front of it),

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 Mac 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 Mac security crisis *du jour*.

However, Apple security updates don't help unless you install them! If you have automatic software updates turned off and never bother to check for updates, you could be needlessly putting your Mac 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 to macOS, such as from Big Sur to Monterey

- Minor updates to macOS, which can be small increments for big fixes (12.0.0 to 12.0.1), or larger ones when they include feature changes but not a full OS upgrade (such as 12.0.1 to 12.1)

Apple Resets the Number Wheel

Apple reset how they number major and minor updates with Big Sur. Back in 2001, Mac OS X (pronounced "ten") launched with version 10.0. Apple incremented 10.0 to 10.1, 10.2, and all the way through 10.15 Catalina, before turning over to 11 with Big Sur and then 12 with Monterey. (What will lucky 13 be?)

- Standalone security updates for macOS that fix specific pieces of system software, usually stuff deep beneath the surface
- 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 macOS 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 updates page. Click a specific update to read the security details.

Fortify Yourself and Your Mac

It's time to step up the security game with a bit more information and more choices to make in ways that keep marauders out (with one loophole), and that let you protect data entering and leaving your Mac. This will include using, purchasing, or subscribing to third-party software, something I suggest sparingly, but that is critical in this case.

In this chapter, I dig into Gatekeeper, Apple's built-in software integrity system hinted out back in Control Which Apps Launch, and now spread out so you can better understand it—and now how to override it.

I also dive into anti-malware software, and why a modern Mac user who may have skipped it for decades, should consider it in 2021 and beyond. Finally, I look at Apple's new anonymized relay service for Safari browsing that's part of iCloud+, and help you understand whether a virtual private network (VPN) offers the kind of umbrella protection you want for all internet usage outside of the home or office.

Apple Protects with Gatekeeper

Apple hides one of its most powerful features behind two radio buttons in System Preferences > Security & Privacy > General. Earlier, in Control Which Apps Launch, I introduced those buttons. But now it's time to dig into understand what Apple manages behind the scenes to protect you against malicious software.

The point of knowing more is twofold: First, to recognize when something's gone wrong. Second, to bypass protections in the limited cases in which you need to.

Manage App Sources

Apple has offered an important security feature called Gatekeeper in its operating system releases available in releases dating back to Mac OS X 10.7.5 Lion. I alluded to it earlier in Control Which Apps Launch. Gatekeeper affects how you install and use software.

Gatekeeper examines downloaded apps when they are first launched, including custom installers from a developer. (Apple has a generic installer that most apps rely on.)

If you have set your app launch preference to App Store only, macOS tells you that you can't open a given app (**Figure 10**).

Figure 10: The app is fine, but your preferences say "no."

However, there's a workaround if you want to be able to open some of these apps. If you go to System Preferences > Security & Privacy, the General tab will show a message: "'*App Name*' was blocked from use because it is not from an identified developer." That much we know. But there's also an Open Anyway button to the right of this message. With the preference pane unlocked, you can click that, and it launches the app with a new dialog that asks you to confirm you really, really want to open it (**Figure 11**).

Share Resources Securely

No Mac is an island. From almost the company's first days, Apple has given the Mac the ability to talk with other devices—and share things with them. macOS can share files, folders, and volumes, as well as share a variety of services, like internet access and even content from Apple cached to a local network server.

What's critical is that you make choices to share only the things you want to, and that you don't open up access in a way that reduces your security and exposes your data or system to exfiltration or attack.

An extremely popular additional way to share for the last several years is via cloud-based services that let you upload or sync files, and then access them yourself or share them to others, often with granular access controls. I look into some of the best-known of these—including Apple's iCloud Drive—to compare features and security options.

Allow Network Access to Services

If you open System Preferences > Sharing preference, you'll notice several different resources your Mac can share with other devices on your local network—and, in some cases, beyond it (**Figure 19**).

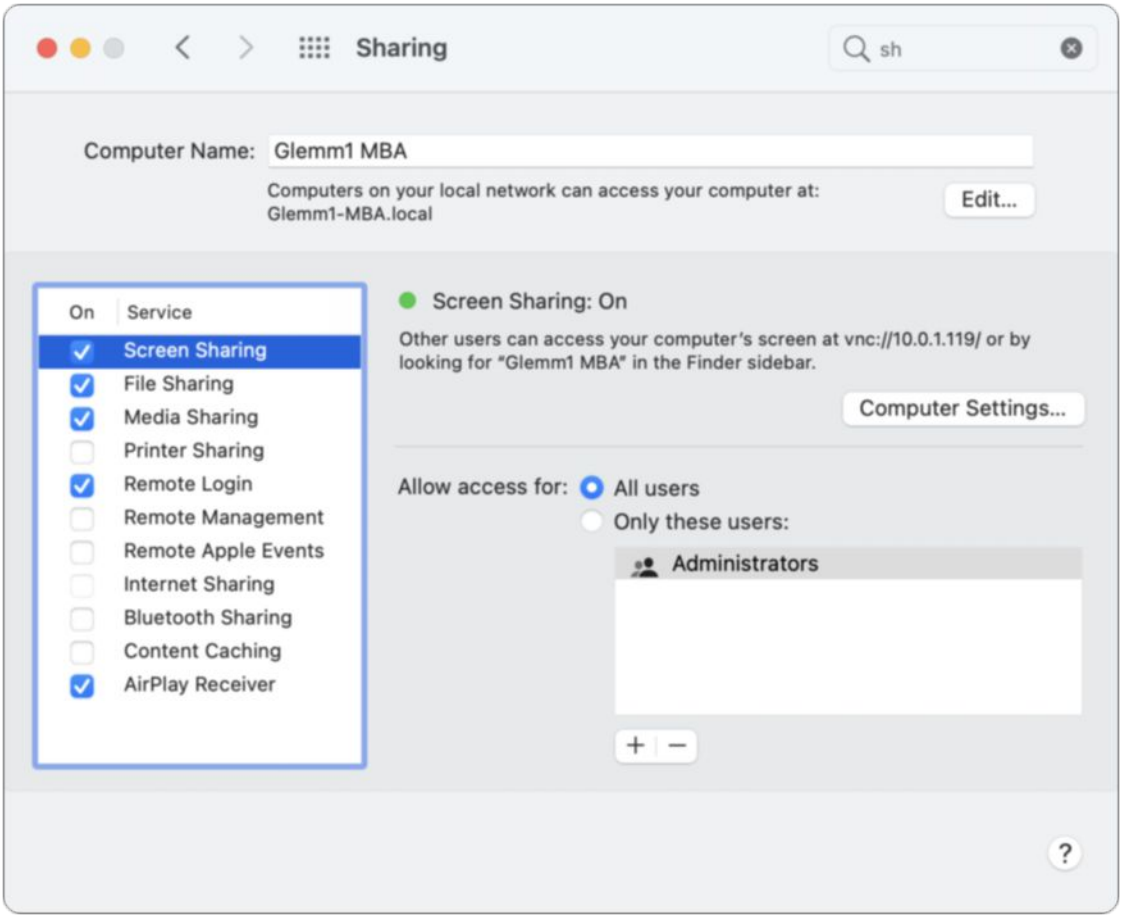

Figure 19: The Sharing pane of System Preferences.

You can share your screen, files, printers, and internet connection, for example, and you can also enable various types of remote access to your Mac.

Tip: Monterey added AirPlay Receiver as an option, finally moving the control from the Finder to a more sensible location after many, many years for who may pass files to you—and adding a password option.

All these features can be handy, especially in that they enable multiple Macs in your home or office to talk to each other. You can copy a file from a Mac in the other room, or view what's on the screen of the Mac upstairs when you're downstairs.

However, Apple pairs easy local access with easy *remote* access: if your Mac is reachable from the internet, some services you share locally can be available remotely. Some may require a password, but that could be easily guessable if you haven't been thinking about internet-based attacks. And just having certain services active, like Remote Login,

Learn macOS Startup and Disk Protections

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

Starting a few years ago, Apple embedded the same chip-based Secure Enclave technology into Macs that had already appeared in iPhones and iPads for a few years. That's 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 in a Mac, and then proceed to talk about disk encryption and encrypting disks, and protecting your startup drive and working with Apple's security safeguards.

I also dig into the way Apple limits password attempts when logging into a MacOS account, and your options for making sure deleted files 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.

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.

The Secure Enclave processor is part of all Macs with a T2 Security Chip or based on Apple silicon, which includes just the M1 processor as of February 2021.

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 and various input/output chips. The T2 chip is a coprocessor for Intel Macs that have it, and the M1 Apple silicon is the main Mac circuitry. (A SoC cheaper to produce and works more efficiently, too.)

Mac series that include these chips with their model years are:

- MacBook Pro, 13-inch, 2018 through early 2020 (T2)
- MacBook Pro, 13-inch, late 2020 (M1)
- MacBook Pro 15-inch, 2018 and later (T2)
- MacBook Pro 16-inch, 2019 (T2)
- MacBook Air, 2018 through early 2020 (T2)
- MacBook Air, late 2020 (M1)
- iMac, Retina 5K, 27-inch, 2020 (T2)
- iMac Pro, 2019 (T2)
- iMac, mid-2021 (M1)
- Mac mini, 2018 (T2)
- Mac mini, 2020 (M1)

Note: Apple did offer a T1 chip in the 2016 series of Thunderbolt 3 MacBook Pro models, but it handled only Touch ID and a few unrelated purposes. It didn't provide any disk-based restrictions or other security enhancements.

Keep Personal Data Private

As we've seen, security and privacy have a complex relationship, but improving your Mac's 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 four of those topics.

First, I look at the implications of sharing a Mac with other people who each have an individual login account. To what extent do separate accounts keep each person's data safe, and how do file ownership and permission settings affect your privacy?

Next, I look into *sandboxing*, a technique Apple uses to keep apps' virtual hands to themselves and away from your data without your explicit and specific consent in a few different contexts, as well as blocking unwanted access to your audio and video inputs and protecting certain folders.

Then, I explain how to configure macOS's built-in privacy settings, which allow or prevent apps from determining your location, using accessibility settings to grab keystrokes, and more.

Finally, passwords are the subject: Apple stores passwords across macOS in different ways, and you should know where they are and how they're protected.

Keep Your Data Safe from Other Local Users

If you're the only person who ever uses your Mac, there's nothing to see here—skip ahead to Deter Invasion via Sandboxing. Otherwise, you should know a few things about what sorts of access other people may have to your data.

First, if everyone uses the Mac via a single account—without having to log in and enter a separate username and password—all bets are off. Whatever's available to you is available to everyone else. I'm not a fan of that arrangement. Ideally, every human who uses your Mac should have a unique username and password. (I might make exceptions for kids too young to type their own passwords. See Configure Accounts & Groups Securely for details.)

But let's say each person does have a separate account and password, and each one diligently logs out (or shuts down the Mac) after every session before the next person logs in. Then what?

macOS, as a variety of Unix, relies on the properties of *ownership* and *permissions* for each file. To oversimplify a bit, each file and folder has a designated owner—usually one of the individual account holders or the system itself—and a set of attributes assigned to it that specify who can access it, modify it, delete it, or execute it, in the case of files. (Apple adds a number of Mac-specific attributes on top of that.)

But there are owners and there are *owners*. macOS Standard accounts owners can access files, apps, and folders in all public places, like the system-wide Applications folder, but they can modify and add items only in specific locations: their own home folder (`/Users/username`) and the Shared folder in the main `/Users` directory. No other standard user can view files in any other users' home folders, except the default `Public` folder, which is read-only and has a `Drop Box` item (not Dropbox, the service) that other users can drag items into, but then not see afterwards (write-only). For day-to-day segregation of one person's data from another, this system provides a reasonable barrier.

An administrator can assign additional access to all non-system files and folders by changing ownership to a user, creating a group and providing group read/write access to a folder, or changing permissions to make things readable and modifiable by anyone with an account.

But that reveals the weakness, no? An administrator has "root" access, which is the top-level permission holder in Unix. Anyone with an administrator account and working knowledge of the Unix command line can access everyone else's files by opening the Terminal app

Regain Access

One of the most unsettling things that can happen to your Mac 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—and I guarantee you I will say once more in the next chapter—but backups are the strongest protection you can have against theft, destruction, and loss, including "loss of access."

If you have nightly backup of all your data on site (via Time Machine or third-party software), copies of your startup volume and external drives offsite, active cloud-hosted backups happening all the time, 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 haven't lost any data, or at least very very little data.

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

In a case where you can't get back into your current Mac, such as a FileVault failure or the loss of a Recovery Key, but you can erase the computer and set it up again, restoring from a full backup puts 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.

Note: Big Sur and Monterey make it harder to create a bootable clone of your startup volume, but keeping an up-to-date clone of the Data volume is no problem at all. In that scenario, to update the operating system on your bootable clone, you have to reinstall macOS, or start with a clean Big Sur or Monterey installation and then restore your Data volume to that startup drive.

Passwords

You should have a go-to, secure place for all the passwords and keys you may need in the event of a disaster or lockout. These include:

- Passwords for one or more administrator accounts on your Mac
- The firmware password, if one is set (see Firmware Password (Intel Macs))
- The Recovery Key for FileVault, if enabled and displayed (see Enable and Manage FileVault)
- The Recovery Key for your Apple ID account (an option starting in iOS 14, iPadOS 14, and Big Sur, and discussed below)
- The account name and password for your iCloud account associated with the Mac
- 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 Mac.

Tip: For my part, I rely on 1Password for this, because it offers a central secure store and access from any number of secure end-points, such as with Face ID on my iPhone. I only have to memorize the main vault password for access on trusted devices, and I have a piece of paper printed out and stored for emergency backup access if everything I owned were lost.

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.

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

About the Author

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

Acknowledgments

I appreciate Joe letting me take his 2015 book as the basis of this significantly revised edition. I stand on the shoulders of giants—Joe is a little taller than me, honestly—and, boy, are the giants getting tired. Thanks, Joe!

Shameless Plug

My latest book made of atoms is *Six Centuries of Type & Printing*, a title that traces the technology and advancements in making type, composing it into words and pages, putting ink on it, and pressing it to paper from before Gutenberg's perfection of metal printing types through the digital era in which type transcends the printed page.

The type for the book was composed on a hot-metal Monotype casting system and printed by letterpress in London. The page is a 64-page cloth-bound hardcover book with foil stamping that comes in its own slipcase, bound in Germany. It unfolds nearly 600 years of printing and is a work of art in its own right. You can order a copy directly.

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 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

- 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 Mac
ISBN: 978-1-95-454601-1

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.