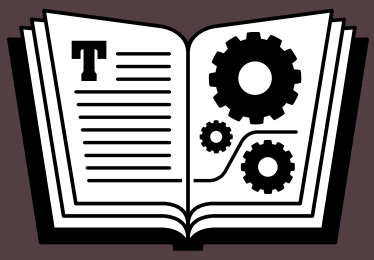

TAKE CONTROL OF

SECURITY FOR MAC USERS

by JOE KISSELL

$15

Table of Contents

Read Me First

Welcome to *Take Control of Security for Mac Users,* version 1.0, published in May 2015 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Geoff Duncan.

This book helps you prevent—or recover from—unwanted access to your Mac and its data. It explains and helps you implement measures that keep out intruders, hackers, thieves, and malicious software; take preventive action to protect your data; and choose the appropriate security settings and software for your particular risk level.

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.

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, links to author interviews, and update plans for the ebook.

If you bought this ebook from the Take Control Web site, 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, read Tonya Engst's free *Read Me First: A Take Control Crash Course*, available on the Web or as a standalone ebook in PDF, EPUB, and the Kindle's Mobipocket format.

Introduction

In survey after survey after survey, security issues like credit card fraud, identity theft, and computer hacking rank among Americans' top worries. Burglary is a bit lower on the list, while threats to personal safety are lower still, and concerns like global warming barely register (statistically speaking). Although poll results vary in other parts of the world, it's still abundantly clear that the fear of having one's devices and data violated is widespread and on the rise.

You might imagine, then, that books about computer security would fly off the shelves, but they don't. (I'm speaking from experience here. I spent most of 2009 writing the massive *Mac Security Bible*, and even though it got great reviews, very few people bought it.)

One big reason for that disconnect is that *computer security* sounds like a scary, complicated technical topic that ordinary people wouldn't be able to grasp. Yes, you're afraid of being hacked—and sure, you want better security in order to prevent that. But you're not a geek, and your eyes glaze over at the very mention of terms like SSL, firewalls, and two-factor authentication. No matter how scary the threat of computer hacking may be, to some people, the prospect of having to *learn about* computer security is scarier!

But authors like me also bear part of the blame. Who was I kidding to think that a 900-page brick on Mac security would seem accessible to the typical Mac user? *Of course* people are going to be put off when it looks like they'll have to invest weeks of study into understanding and solving the problem. I understand. I'm sorry. I repent.

The book you're now reading takes a much different approach.

For starters, it's *much* shorter. As in, about 1/6 the length of *Mac Security Bible*. You can probably read the whole thing in an afternoon—but feel free to browse just the topics you care about.

Next, I've left out many of the gory details that only developers, system administrators, and other propeller-heads would care about. I tell you

enough to understand the basics of Mac security problems and solutions so that you can make smart decisions about what steps to take. But I try not to overwhelm you with tech-speak.

Most importantly, my intention is to strike a more positive and reassuring tone. I don't want you to be as scared of the cure as you are of the disease! On the contrary, my goal is to put your mind at ease. Because really, you don't have to be afraid of bad guys hacking your Mac. Once you understand what the threats are and the (mostly quite simple) ways you can counter them, you'll be able to sleep better at night knowing that your Mac's security is under control. Even if you should fall victim to a security breach, this book will teach you how to recover quickly and gracefully—no panic required.

And, because this is a Take Control ebook, we're able to update it if and when the facts change—it isn't doomed to be obsolete before it's a month old.

This book is for Mac users—and especially those running OS X 10.10 Yosemite. Most of what's here also applies to 10.9 Mavericks, but the older your version of OS X, the less relevant this book will be. I don't go out of my way to spell out the differences from one version of OS X to the next, because one of the most important steps you can take to increase your security is to *keep your software up to date*. If you're still running, say, 10.6.8 Snow Leopard, you can't take advantage of the many security improvements Apple built into newer versions of OS X, and the best advice I can give you is to upgrade if possible.

Since it's an integral part of the Apple ecosystem, I'll occasionally mention iOS, too, but mobile security is another whole ball of wax.

You'll notice that I emphasize network security—that is, helping you prevent attacks and intrusions that originate on the Internet. That's not the only type of Mac security, of course, but it so happens that most of the threats you're likely to encounter involve the Internet in some way. Keeping your Mac's network interactions secure is much more than half the battle. We'll also discuss physical security, protecting your data from other people you permit to use your Mac (not to

mention thieves and snoops), keeping rogue apps from causing mischief, and everyday techniques to keep your data safe.

Of course, your security involves more than your Mac. I can't prevent someone from stealing your wallet, hacking the payment terminals at your local department store, digging through your trash to find personal information, or breaking the lock on your back door. But I can help you achieve that all-important balance between security and convenience when it comes to your Mac and all the data it contains, and that's an excellent start to living a more secure life.

One final note before we move on: I've written Take Control books on other topics that touch upon security. Although there's inevitably some overlap, each book addresses a different core issue. I refer you to these other books where applicable for more detail on specific topics:

- *Take Control of Your Online Privacy*
- *Take Control of Your Passwords*
- *Take Control of 1Password*
- *Take Control of FileVault*
- *Take Control of Backing Up Your Mac*
- *Take Control of CrashPlan Backups*
- *Take Control of iCloud*

Mac Security Quick Start

There are many different aspects to Mac security, which are often intertwingled in confusing ways. In general, I've tried to group similar concepts together and put the most important (and easy-to-implement) material earlier in the book. Here's what you'll find.

Hit the Ground Running

Everyone should read Learn Security Basics, in which I take a broad look at what security means—in general, and to you specifically. Yes, you! I've been watching you read this, which I could do because I just hacked into your Mac. *Kidding! Totally kidding!* But if you had a moment of doubt there, you'll appreciate the discussion of risk profiles. This book often makes recommendations based on what your risk level is—1, 2, 3, or 4—so you need to know your level to get the most out of this book. Plus, having a clearer idea of your risk level will help you make better security decisions and avoid unwarranted paranoia.

Next come three chapters—again, recommended for every reader—that deal with the low-hanging fruit of Mac security:

- Perform Quick Security Fixes discusses a few things you need to know and do *right now*, all of which are pretty easy but can dramatically improve your security. This includes updating your software and making a few important tweaks to OS X's security settings.
- In Beef Up Your System Settings, I continue with (to strain the metaphor) some higher-hanging fruit that may require pruners or a stepladder. I talk about how OS X uses sandboxing to keep apps from doing bad things, and how the settings related to this feature affect your security. I also make suggestions for improving your Users & Groups settings and discuss implications of sharing files, screens, and other resources via the Sharing pane of System Preferences.

- Improve Your Passwords talks about how crucial good passwords are to nearly every other aspect of security and helps you improve passwords that are too weak.

Manage the Ins and Outs

Although network security is a recurring theme throughout the book, the next group of chapters focuses on network-specific topics:

- Improve Your Network Security covers your network connection as a whole (Wi-Fi or otherwise), showing you how to protect various segments of the path data travels between your Mac and other computers—and showing what could happen if you don't.
- In Fortify Your Mac's Defenses, I talk about several categories of software that monitor and filter data as it comes into or leaves your Mac, which is important regardless of how secure your network connection might be. (For example, you could have a secure connection to a compromised computer that tries to send you malware.) I also revisits the age-old question of whether you as a Mac user need anti-malware software—and if so, what the best options are.
- Moving on to more specific tasks, we come to Surf the Web Safely. The Web is a conduit for all sorts of malicious behavior, and in this chapter I tell you what to be on the lookout for—and how to stay out of trouble. This may include altering some browser preferences, installing plug-ins, and taking greater care in which sites you visit. That chapter also helps you safely use passwords and credit cards on the Web, while steering clear of phishing schemes designed to trick you into giving away private information.
- For iCloud users—which, let's face it, is pretty much everyone with a Mac these days—Manage iCloud Security lays out the good and the bad. You might be surprised to learn that some aspects of iCloud are much more secure than generally believed. On the other hand, you could be casually using iCloud features that—without special care—could be fabulously unsafe, exposing personal data (like *those* sorts of photos) to people who should never see them.

Tie Up Loose Ends

The final three chapters cover essential topics that don't fall under either "basics" or "network security."

- Read Prevent Data Loss and Theft to learn about the crucial importance of backups (you *knew* I'd bring up backups sooner or later, right?) as a key to preventing—or recovering from—data loss. However, you also want to prevent someone from gaining unauthorized access to your Mac's data even if you don't lose access yourself—in other words, data theft. I discuss techniques to prevent data theft, including the use of FileVault or other encryption tools and secure deletion.
- You can think of Keep Personal Data Private as the Reader's Digest condensed version of *Take Control of Your Online Privacy*. I hit the highlights and review the key steps you can take to keep your personal information out of the hands of others—whether they're other local users or ne'er-do-wells across the Internet.
- The final chapter is the one I hope you never have to read! In Recover from a Disaster, I reiterate my "Don't Panic" advice and walk you through the steps to take if misfortune strikes. Did you lose data? Here's how to get it back. Did malware find its way onto your Mac? Here's how to get rid of it. Did you suffer a phishing attack, network intrusion, or even—heaven forbid—identity theft? Here are the steps to take.

Tip: At the risk of stating the obvious, you'll be *way* ahead of the game if you've prepared for disaster with measures like strong passwords and great backups, but I tell you what you should do either way.

Learn Security Basics

In the coming chapters, I'll tell you all about security preferences, software, online services, and practices that can help keep your Mac and its data safe. But first, to set the stage (and your expectations), I want to explain just what I mean by *security*—that word may not mean what you think it means. I also help you evaluate your risk level, shed light on some oft-overlooked security principles, and suggest that you can be responsible with your Mac's security without becoming paranoid.

What Does Security Mean?

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*. These sorts of everyday uses of the word "security" all have subtly different senses, but what they have in common is reducing the likelihood of harm or danger.

Moving into the digital world—and more specifically your Mac—security takes on yet another shade of meaning. In most cases, a violation of your Mac's security won't result in *physical* harm to a human being. It may, however, cause you emotional or financial harm (theft of identity or money), waste your time (canceling credit cards, changing passwords), make more work for you (removing malware, restoring deleted files), and so on. Those are the sorts of harm better Mac security can help you avoid.

Closely related to the concept of security are those of *privacy* and *anonymity*. Here's how to keep the three terms straight:

- **Security** is freedom from danger or harm.
- **Privacy** is freedom from observation or attention.
- **Anonymity** is freedom from identification or recognition.

You can have security without privacy (imagine living in a house made of bulletproof glass). You can also have privacy without security (think of a changing room at a clothing store). And you can have both privacy and security without anonymity (think of a royal family ensconced in a castle).

But when it comes to your digital life, these concepts—especially security and privacy—go together more often than not. Many of the harms or dangers that might befall you if your security is insufficient involve personal data being exposed, so one of the biggest reasons to have better security is to maintain your privacy. Or, to put it the other way around, many of the things you can do to protect your privacy are, in fact, security measures. When you Use Encrypted Wi-Fi or Use a Firewall, you're protecting yourself against several kinds of harm, including harm that could be caused by the loss of privacy.

Even though there's a partial overlap between security and privacy, the two topics are distinct. Improving your Mac's security can reduce the chance of harms beyond those that involve privacy, such as:

- Loss of data
- Degraded performance
- Malware that sends spam from your Mac
- Loss of control over your Mac

Conversely, a number of the steps I recommend to preserve your privacy don't involve extra security as such. I'm thinking of things like keeping sensitive information from being exposed to the Internet, modifying your social media behavior, choosing communication methods based on what you have to say and to whom, and in general *not doing stupid things online*.

In short, better security can provide more privacy, but it does much more than that—and security is only one means to protect your privacy. I recommend paying careful attention to both angles.

Perform Quick Security Fixes

Time to get to work improving your security! Let's begin with a few things everyone should do (with small variations depending on your risk level). 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.

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 widespread 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 OS X itself, such as 10.10 Yosemite
- Minor updates to OS X, such as 10.10.1

- Stand-alone security updates for OS X
- Updates to specific Apple apps (Safari, iTunes, QuickTime, etc.)
- Updates to third-party apps

Which of these should you keep up with? Ideally, all of them—but at a bare minimum, be sure to install the stand-alone security updates. The next-highest priority would be minor OS X updates.

> **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.

In most cases, Apple releases security updates, for the current version of OS X and the previous two—so an update in early 2015 would apply to Yosemite, Mavericks, and Mountain Lion. If you aren't at least on the third-most-recent version of OS X, you risk being vulnerable to known security problems that Apple won't ever fix.

Meanwhile, each major new version of OS X contains entirely new security features, independent of bug fixes. Yosemite offers certain intrinsic protections that Mavericks did not, and Mavericks has security features that Mountain Lion lacks. So if you really want all the latest security goodness, you should (if your hardware supports it) upgrade to the latest version of OS X *and* install all the pertinent OS X, security, and app updates.

> **Note:** Often the initial releases of new OS X versions (10.9.0, 10.10.0) have significant bugs that Apple fixes quickly. So it's fine to wait a few weeks on major upgrades, by which time (if there's not already a 10.x.1 version) enough others will have tried out the new release that you can judge how stable it may be for you.

All Apple software updates for OS X are now delivered through the App Store app, which also handles a good bit of third-party software. You can use that app to manually install any available update, and you can configure its preferences to automatically download and/or install new updates as they appear.

Beef Up Your System Settings

In the previous chapter we looked at some of the easiest changes you can make to improve your Mac's security, several of which involved simple changes to settings. In this chapter we continue with some settings that require a bit more explanation and thought. That includes a discussion of OS X's Gatekeeper and sandboxing security features, some basics for using user accounts more securely, and a couple of quick suggestions about sharing files, your screen, and other resources. Except as noted, this chapter applies to people at every risk level.

Manage App Sources

Since Apple released Mountain Lion in 2012, OS X has had an important security feature called Gatekeeper. (Apple later added Gatekeeper to OS X 10.7.5 Lion, too.) Even though you won't *see* the word "Gatekeeper" anywhere in OS X (Apple mentions it in marketing materials, on the OS X Security page, and in developer documentation), Gatekeeper affects how you install and use software.

Gatekeeper examines downloaded apps either when they're installed (if they use an installer) or when they're run for the first time. If the app doesn't meet your criteria, Gatekeeper blocks the app from running. The point is to prevent malicious software from causing damage or stealing data. Gatekeeper can also protect you from apps that have been modified without your knowledge. In both cases, Gatekeeper depends on a process called *signing* an app.

Understand App Signing

Each developer who has joined Apple's $99-per-year Mac Developer Program gets a special digital certificate that serves as a unique identifier. In the process of building an app, the developer can use

that certificate to *sign* the app. A signed app doesn't look any different from an unsigned app, but it contains extra data that enables OS X to determine:

- **Integrity:** Whether the app has been changed since it was built
- **Identity:** Which developer created (and signed) an app
- **Access:** Which system resources the app may access

Each of these attributes helps to protect your security.

Let's start with integrity. If an attacker were to modify an app after it was signed—for example, inserting malicious code while it sat on the developer's Web server or even after you started using it—Gatekeeper would notice the change and prevent the app from running.

> **Note:** Gatekeeper *always* prevents signed apps that have been altered from running, even if they ran fine before, or if your settings specify that unsigned apps may run (see Choose an App Security Setting, next).

Next, suppose someone signed up for the Mac Developer Program and started delivering malicious software, signed with their certificate. The identity feature kicks in—once Apple discovers that the developer is distributing dangerous software, Apple can revoke that certificate, telling Gatekeeper not to let any software signed with that certificate launch. (Your Mac checks for revocations once a day. An Internet connection is required.)

The third aspect, access, involves system resources such as Keychain. If you grant an app permission to store information in Keychain or access it afterward, you don't want to have to keep doing so every time you update the app. But if you install a new version of an app that was signed with the same certificate, Gatekeeper considers it the "same" app for the purpose of allowing access to system resources—you won't be prompted for Keychain access again. Conversely, if someone altered the app or gave you an unsigned and therefore unauthorized version, it wouldn't be able to access your Keychain without your permission.

Improve Your Passwords

Whether you're talking about your Mac's user account, your Wi-Fi router, any of the zillions of Web sites where you might have an account, or countless other services, passwords are nearly always a factor in digital security. They are also nearly always the weakest link.

If the only thing standing between a random visitor and your data is your password, that password had better be pretty darn strong. Unfortunately, most people use lousy passwords that are easily guessed or broken, for the simple reason that they're convenient to remember and type. And that's a real pity—your Mac (including built-in software like Safari and Mail) supports excellent, heavy-duty security methods, but if you pick a terrible password, it's like using a fantastic lock but then hiding your key under the doormat.

So, for the various ways in which your Mac uses passwords, as well as for the devices and services to which you connect with your Mac, one of the most crucial steps you can take to improve your security is to improve your passwords.

Note: If you want to learn much more about password security, you can read my book on that subject: *Take Control of Your Passwords*. It goes into far more detail than this chapter and helps you build a complete strategy for dealing with all your passwords—including complicated special cases.

Learn about Password Security

What's your password?

Sorry, that was a trick question. If you can answer it, you may have a problem.

Wait, what? Ah yes, I misspoke—you more likely have *two* problems!

The first problem is that you shouldn't have just one password, but many; if you do have only one, you're playing with fire. The second problem is that, of the many passwords you (should) have, *nearly* all of them should be so long and complex that you couldn't possibly remember them without looking them up. If you can remember them, there's a good chance they're not strong enough.

If you find any of that information surprising or disturbing, read on for an explanation of both the problem and the solution.

When you're asked to create a new password, perhaps your first impulse is to use the same password you use everywhere else, because it's easiest to remember a single password. And what is that one password? An astonishing number of people use memorable and easy-to-type sequences like `password`, `baseball`, `qwertyui`, the name of a child or pet, or something snarky such as `stopasking`. What if they're required to include a capital letter and a number? Why, they'll choose `Password1` or `Baseball2`, of course! This is a dangerous habit.

If I found your Mac unattended and decided to break in to one of your accounts, I might start by trying some of the most commonly used passwords—it's easy to find lists of them online—and if I happened to know anything about you, I might also try words, names, and dates I know you'd remember.

But that's not how most password attacks work. Sophisticated attackers can use freely available software to crack passwords using a variety of methods, including automatically checking lists of common passwords, trying patterns of all sorts, or even systematically checking every possible combination of characters (up to a point)—all very quickly and effortlessly. Your passwords need to be more sophisticated to resist cracking attempts long enough that the attacker will give up. (How do you come up with passwords like that? We'll get to that in a moment—see Create Strong Passwords.)

Note: An easier way to get your password than guessing or using cracking software is to trick you into supplying it yourself—for example, with email messages that lure you to fake Web sites. We'll return to that topic in Avoid Phishing Attempts.

Improve Your Network Security

Macs usually connect to the outside world using Wi-Fi or Ethernet. ("Outside world" might mean another Mac across the room or a server on the other side of the planet.) In fact, most of us have become so dependent on network access that we find it hard to get any work done if that all-important Internet connection goes down.

That dependence on interacting with other devices is both a strength and a weakness. It gives us access to massive power and instantaneous global communication—but it also gives the bad guys an attractive target. This chapter discusses the reasons for protecting your network connection and how to go about doing so.

What You're Trying to Protect Against

Broadly speaking, the point of network security—or at least, the particular subset of network security I cover in this chapter—is to protect data as it flows to and from your Mac over both local networks and the Internet. (In Fortify Your Mac's Defenses, I talk about another aspect of network security—protecting your Mac itself from intrusions and damaged caused by network-based attacks.) But what sort of threats might your network communication face, and from whom?

In a word, you're trying to protect your data against *eavesdropping*. If someone is able to see the data that enters and leaves your Mac, then anything you send or receive over a network—email, Web searches, photos, passwords, chats, files, and so on—is no longer private. But it's not just a privacy issue; someone who intercepted just the right kind of information could use it to break into your Mac, install malware, steal your identity, or do other sorts of damage. In this case, privacy and security are two sides of the same coin.

Eavesdropping sounds passive—like someone listening in on a phone call because the line was tapped—but in skilled hands it can be used actively for more sophisticated wrongdoing. One example is a *man-in-the-middle attack*. In a simple case, imagine that someone tricked your Mac into connecting to a bogus instant messaging server. You continue to send and receive instant messages as though nothing happened, but all incoming and outgoing text is actually funneled through the attacker's rogue server. That means any message could be altered (or even deleted) on its way from sender to recipient—and neither party would know the difference!

> **Note:** We'll address email security later. Encrypt Your Email explains a way to avoid man-in-the-middle attacks on email communication.

Why would someone eavesdrop on *your* network activity? Unless you're at Risk Level 4—that is, you're being targeted individually—most likely no one cares about your data specifically. It's not personal! Rather, there are software "robots" (and occasionally real people) that constantly probe any network connection they can find for vulnerabilities and slurp up any useful bits of information, to be used for everything from petty scams to identity theft. (A hacker may also sell that data rather than using it directly.)

Although, in principle, nearly the entire Internet is vulnerable to this sort of monitoring, the least secure link in the chain is almost always your Wi-Fi connection—especially if you're using an open, public network. Someone sitting nearby at a coffee shop or library—or even across the street, in a car, or in a different building—can use freely available software to "sniff" the Wi-Fi signal, and monitor all the Wi-Fi sessions nearby. It's not hard. I've done it myself (for research purposes only, mind you), following directions I found on the Web, and I was shocked and appalled at what information I found floating freely through the air around me.

Fortify Your Mac's Defenses

In the previous chapter, I talked about ways to ensure that the data you send and receive with your Mac isn't intercepted, monitored, or hijacked in transit. But regardless of how secure your Mac's connection with another computer may be, that computer could try to send your Mac dangerous software, or someone could attempt to break into your Mac remotely. Conversely, you could have software on your Mac that attempts to make connections to distant servers without your knowledge and send them information you'd rather keep private. This chapter discusses ways of keeping your Mac and its data safe from outside attacks, some of which could appear in the form of malicious software, or *malware*.

Use Anti-malware Software (or Don't)

"I thought Macs didn't get viruses." I can't tell you how many times I've heard statements like that, and how dizzy I've gotten from all the eye-rolling I did as a result. There's a kernel of truth in that claim, but it's far from the universal principle people often imagine it to be.

Let's talk about the true-ish part first.

Malware that can run on Windows outnumbers Mac malware by a factor of at least 1,000. I've seen estimates ranging from a bit over 100,000 to many millions of Windows malware variants, but even the most generous estimate puts the number of Mac malware programs in the mere hundreds. Furthermore, of these however-many Mac malware programs, the vast majority are either outdated and thus unable run on current Macs, are only proofs of concept that have never been seen "in the wild," or are effectively blocked by OS X's built-in security measures. So, in terms of sheer numbers, the odds favor Mac users.

But let's be clear: there's nothing inherent to the design of OS X that makes it intrinsically immune to malware. Security holes have indeed been uncovered and exploited by malware, and that will continue to happen. Although the bad guys generally like to focus on the largest targets, the statistical accident that there are more PCs out there doesn't count as protection. And sure enough, in the last few years there have been some dangerous and fairly widespread infestations of Mac malware.

You'll notice, by the way, that I keep saying "malware" and not "viruses." That's because another true-ish aspect of the "Macs don't get viruses" claim is that a *virus* is a very specific kind of malware that can replicate itself and become part of a file or another app, and I could probably count on one hand the number of actual Mac viruses that have ever been in the wild. Other kinds of Mac malware, particularly Trojan horses (malicious software disguised as something useful), are much more common. Although lots of people use the term "virus" loosely to mean any sort of malicious software, I prefer to call a spade a spade.

About Ransomware

One especially vicious type of malware is called *ransomware*. You download and run an infected app, and it immediately starts encrypting everything on your disk. Then it displays a ransom note: send hundreds of dollars (in difficult-to-trace Bitcoin or other virtual currency) to a certain address by the specified date and we'll give you the key to decrypt it. Fail to comply, and we'll erase your disk forever! (A less-severe variant simply tries to lock you out of using your Web browser.)

Ransomware for OS X is rare, but it does exist. You can guard against it in the same way you guard against any other malware. But if you have a full, offsite backup of your Mac's disk (see Prevent Data Loss with Backups), you have an ace in the hole—it doesn't *matter* if your whole disk is erased, because you can restore it without paying a penny. That's just one of many reasons I consider excellent backups to be one of the most important security measures you can take.

Surf the Web Safely

The Web is perhaps your Mac's most obvious gateway to the outside world, and as a result, it's one of the best places to find people and software that present threats to your security. Even though you've secured your Wi-Fi connection, selected good security settings, and chosen strong passwords, a brief visit to a malicious Web site can cause all sorts of harm to your Mac.

In this chapter, I review several keys to safer Web browsing, including using SSL/TLS when possible, making sure your browser uses appropriate settings, and using a combination of common sense and technology to avoid phishing attempts and Web-borne malware. Everything here is applicable to users at all risk levels, although those at higher levels may want to choose more restrictive options, where they exist.

I focus mostly on Safari and Google Chrome, the two most popular Mac Web browsers, but my advice applies to nearly every browser, and you can likely find settings and extensions comparable to the ones I discuss here even if you use Firefox, iCab, Opera, or another browser.

Understand SSL/TLS and Web Browsing

If you can ensure that the connection between your browser and a Web server is securely encrypted, you can also be confident that no one in between can read what you send or receive—that's especially important when using the Web for email, online shopping, and other private communication.

The standard way for a Web site to encrypt its connection is to use *HTTPS*, a secure version of the HTTP protocol. HTTPS relies on a technology called TLS (Transport Layer Security), which is the latest generation of an earlier standard called SSL (Secure Sockets Layer). Because most people are still more familiar with the term SSL, I'll refer to the technology as SSL/TLS. You do not need to know the details

about how this works or even remember those initials. But the result of all this technology is that your communication with the site is encrypted in both directions, and in addition, your browser can independently verify that the site is authentic. All this happens automatically, behind the scenes.

You'll know a site uses HTTPS if the URL starts with `https:` (although many browsers now hide this portion of the URL) or if you see a lock icon (often in green, perhaps with the company's name, right next to the URL in your browser's address bar). You can then click the lock icon to view details about the certificate and confirm its identity.

> **Note:** Ignore any lock icon on the Web page itself—it be there to trick you into thinking a page is secure when it isn't.

Increasingly, sites that transmit or receive personal data—even just a username and password—use HTTPS by default, which is an excellent idea. In fact, I'd go so far as to say you should assume any password or other personal data entered on a site that *doesn't* use HTTPS could be intercepted. Some sites use HTTPS only optionally; you might look for a preference you can enable, which will automatically redirect you to the secure site even if you enter a URL starting with `http:`.

The Electronic Frontier Foundation (EFF) offers a free browser extension for Chrome, Firefox, and Opera called HTTPSEverywhere (sorry, no Safari version available). This extension has a regularly updated list of sites that offer HTTPS connections and instructs your browser to use HTTPS for those sites, even if you visit the site with a non-HTTPS link or URL. It can't encrypt sites without HTTPS support, but it can prevent you from accidentally visiting an insecure version of a site.

Alas, HTTPS, for all its virtues, is not foolproof. I've read of various hacks and exploits that could enable an attacker to intercept and decrypt an encrypted Web session. However, the real-world risk of encountering such a problem is quite low, and Web browser developers generally fix security problems like these in short order. So, as always, your best defense is to make sure you keep your operating system and browsers (including any security updates) current.

Manage iCloud Security

Because so many aspects of OS X depend on Apple's free iCloud service for key functionality, I wanted to devote a brief chapter exclusively to iCloud security. Of course, iCloud works on mobile devices, Windows PCs, and even Apple TVs—not just on your Mac—but the more you know about iCloud security, the better you'll be able to protect your Mac and its data from unwanted access.

Note: Portions of this chapter first appeared in my book *Take Control of iCloud*, which goes into considerably more detail about all iCloud features, including their privacy implications.

Understand Apple's Security Policies

Apple's privacy policy is written in refreshingly straightforward, legalese-free, non-technical English. That page, and the pages it links to with details on built-in privacy, managing your privacy, and government information requests, are well worth reading. They paint a picture of a company that is committed to doing everything it's legally allowed to do to protect your privacy.

I believe what Apple says there—that is, I think the company's corporate heart is in the right place. That's not to say I trust Apple, or any company, 100 percent, because companies are composed of people, and sometimes people make mistakes or do bad things that are not at all in keeping with their employers' policies. But it is certainly in Apple's business interest to do what it claims to do with regard to privacy.

Turning more specifically to iCloud, Apple has an entire page detailing the extent to which the company encrypts your iCloud data and what other privacy and security measures are in place; see iCloud security and privacy overview. Again, it's well worth reading.

The good news is that every type of data iCloud handles is encrypted while in transit, and *almost* every type of data is also encrypted while it's stored on Apple's servers. That's fantastic, and it means that most of your iCloud data is safe from random hackers.

Interestingly, although the page specifies that Apple does *not* have the capability of decrypting your iCloud Keychain data, it doesn't make the same claim about anything else—it only states that Apple never provides encryption keys to third parties. That means an Apple employee could, in principle, access any of your iCloud data other than iCloud Keychain. That includes your email and notes (which aren't encrypted on the server anyway). It follows that Apple could provide your unencrypted email to law enforcement or government agencies if required to do so by law.

If you take Apple's policies at face value, you should assume that the company is motivated to protect your data. However, "Apple wants to protect your data" and "your data is perfectly safe" are two different things. There are always weak spots.

One of those weak spots is your password. (Of course, you should make your iCloud password nice and strong—see Improve Your Passwords, and in particular, iCloud Password.) Anyone who can figure out your password can log in as you and get at any of your data! And that's why Apple offers an optional (but highly recommended) method to increase your security.

Use Two-step Verification

Even the longest, strongest, most random password provides no security if someone else finds out what it is. Perhaps someone watches over your shoulder as you type your password at your local coffee shop. Or maybe a spam email message persuades you to enter your password on a phishing site that looks almost exactly like the Apple site. Or an as-yet-undiscovered security bug or exploit exposes your password to an attacker.

Prevent Data Loss and Theft

Most of the topics in this book address ways of protecting your data in one fashion or another. For example, you want to keep people from breaking into your accounts, from sniffing your Wi-Fi signals, and from using malware to collect private information. But I haven't yet addressed two key pieces of data security—preventing loss and theft of your data *while it's stored on your Mac*.

Perhaps I should explain what I mean by "loss" and "theft" here:

- *Data loss* is when you no longer have access to your own data. For example, a file you need (or a portion of a file) disappears from your disk, or is overwritten or damaged in such a way that you can no longer read it. The data is just gone—it doesn't exist anymore.
- *Data theft* is when someone else gets access to your data illicitly. A curious thing about data theft is that—unlike with theft of physical objects—you usually still have your data after it's been stolen! But the point is, it's no longer under your exclusive control.

The way to prevent data loss is to have excellent backups. That way, no matter what catastrophe might wipe out data on your disk, it isn't truly lost—you have a copy that you can restore easily. Backups are one of the most crucial security measures you can take—they're a form of insurance. Just as you insure your home and your car so that, if they *were* to suffer theft or damage, you can put them right again, you insure your data with good backups.

Data theft can occur in many ways, as we've seen throughout this book, but what I'm thinking of here is data theft that results from losing physical control of your Mac. That is, someone steals your Mac, or uses it when you aren't around, or picks it up from the train where you accidentally left it. Given access to your Mac, all your data is there for the taking. And the way to prevent that is with encryption.

Prevent Data Loss with Backups

You can back up your Mac's data in numerous ways, using any of about 100 different backup apps. Each method and storage medium has its pros and cons, and everyone has different backup needs and preferences. Nevertheless, for most people, most of the time, I can summarize my backup recommendations in three steps: versioned backups, bootable duplicates, and offsite storage.

> **Note:** I can only scratch the surface of backup options and strategies here. For the full treatment, read *Take Control of Backing Up Your Mac*.

Each of these elements solves a different type of problem, and only with all three together do I consider my data reasonably safe from loss. I recommend all three types of backup for anyone at Risk Level 2 or above. People at Risk Level 1 should still have backups, but if you have next to no personal files on your Mac, picking just one form of backup is a reasonable approach.

Versioned Backups

A *versioned backup* is one in which the backup app stores multiple versions of each file. When it runs the first time, it copies all the files you specify. Later, when the backup runs again, it copies only the files that are new or changed since the previous run, but it doesn't delete the earlier files from your backup—even if they've been deleted from your Mac's disk. Although Mac backup apps refer to this capability by a variety of names and implement it in many different ways, the key characteristic you're looking for is the capability to recover your disk (or a particular file) to its state from a week or a month ago—even though your Mac has been backed up numerous times since then.

Here's the basic problem versioned backups solve:

- You have a Very Important File.
- Something bad happens to that file. Maybe you delete it accidentally. Or you mistakenly delete a portion of the file before

Recover from a Disaster

I wish I could tell you that merely following all the steps in this book will guarantee you'll never have a security-related problem with your Mac. But no one could make such a guarantee—not even if you used every single Risk Level 4 option I describe here. The combination of software bugs, human error, and clever attackers could take down the best of us.

The question is what to do next. If you've lost data, or you've discovered malware on your Mac, or someone has stolen your personal information and applied for credit in your name, you need to take action to fix the problem as soon as possible. Regardless of the type of disaster, your first step is:

1. Don't panic.

(Repeat this step as needed until you're no longer panicking.)

Then you can methodically undo or repair the damage. Although the exact procedure will depend on your situation, this chapter contains some suggested general steps to get you started.

Recover from Data Loss

You have terrific backups. In fact, you have three kinds—versioned backups, a bootable duplicate, and an offsite copy of your backups. I know this because you read Prevent Data Loss with Backups, and I'm confident you followed those instructions immediately. Since you have backups, recovering from data loss should be easy. (If you *don't* have adequate backups, you're going to have a much harder time, but I'll return to that topic in Recover Deleted or Damaged Data.)

Restore Data from a Backup

Whether you've lost a single file or the contents of an entire disk, backups can save your bacon. In general, you have two options—restore individual files or folders, or restore your entire disk.

Restore Individual Files or Folders

If you know exactly which file(s) were affected (lost or damaged)—and the number of such files is small (a single file or folder, or a handful of files all stored in one place)—your fastest path to recovery is to use either your versioned backup or an online backup (whichever one was updated more recently). For example, suppose you use both Time Machine and CrashPlan. Time Machine runs once an hour, but CrashPlan runs continuously (subject to your preferences), so the odds are that CrashPlan will have the more recent version of the file(s). On the other hand, if the files are quite large, you'll be able to restore a local backup much more quickly than a backup stored in the cloud. Refer to your backup software's documentation for restoration instructions.

Restore an Entire Disk

If your Mac is lost or stolen, if its hard drive or SSD suffers a hardware failure, if the damage to your disk's data is extensive and widespread, or if you have malware that you're unable to remove (see the next topic, Recover from Malware), you'll need to restore *everything* on your disk. You can use any of three main approaches:

- Restore the disk from your bootable duplicate. Then, if necessary, use your versioned backup or an online backup to restore just those files that had changed since you made your duplicate. See Restore a duplicate.
- Using Recovery Mode, restore your entire disk from Time Machine. This process is more time-consuming than restoring from a duplicate (it could take anywhere from several hours to overnight), and you won't be able to use your Mac for anything else during the restoration process. If you excluded any files or folders from Time Machine, they weren't backed up and therefore can't be restored—you may need to fetch them from another backup later on. See Restore a Time Machine backup.

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 postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.

If you bought this ebook from the Take Control Web site, 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 Web site, contact us.

About the Author

Joe Kissell is the author of numerous books about technology, including *Take Control of iCloud* and *Take Control of Your Online Privacy*. He is a contributing editor to TidBITS, and a senior contributor to Macworld.

He is also the winner of a 2009 Neal award for Best How-to Article, and has appeared on the MacTech 25 list (the 25 people voted most influential in the Macintosh community) since 2007. Joe has worked in the Mac software industry since the early 1990s, including positions managing software development for Nisus Software and Kensington Technology Group.

When not writing, Joe likes to travel, walk, cook, eat, and practice t'ai chi. He lives in San Diego with his wife, Morgen Jahnke; their sons, Soren and Devin; and their cat, Zora. To contact Joe about this book, send him email and *please* include `Take Control of Security for Mac Users` in the subject line of your message so that his spam filters won't intercept it.

Shameless Plug

On my site Joe On Tech, I write about how people can improve their relationship with technology. I'd be delighted if you stopped by for a visit! You can also sign up for joeMail, my free, low-volume, no-spam mailing list, or follow me on Twitter (@joekissell). To learn more about me personally, visit JoeKissell.com.

About the Publisher

TidBITS Publishing Inc., publisher of the Take Control ebook series, was incorporated in 2007 by co-founders Adam and Tonya Engst. Adam and Tonya have been creating Apple-related content since they started the online newsletter TidBITS in 1990. In TidBITS, you can find the latest Apple news, plus read reviews, opinions, and more.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Geoff Duncan
- Production Assistants: Michael E. Cohen, Oliver Habicht
- 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 and OS X, but we also publish titles that cover iOS, 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. 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 Security for Mac Users
ISBN: 978-1-61542-449-8

TidBITS Publishing Inc. 50 Hickory Road Ithaca, NY 14850 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, he or she 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 TidBITS Publishing 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 TidBITS Publishing 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.