TAKE CONTROL OF

YOUR ONLINE PRIVACY

by JOE KISSELL

$10

Take Control of Your Online Privacy (1.1)

Joe Kissell

This book is for sale at http://leanpub.com/tco-your-online-privacy

This version was published on 2014-03-18

* * * * *

* * * * *

ISBN for EPUB version: 9781615424252

ISBN for MOBI version: 9781615424252

Table of Contents

Read Me First

Welcome to *Take Control of Your Online Privacy,* version 1.1, published in March 2014 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Geoff Duncan.

This book explains potential privacy risks in everyday online activities like Web browsing and sending email, and suggests strategies for avoiding common pitfalls and improving online privacy.

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. Also, you can Teach This Book.

Updates and More

You can access extras related to this book 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

Here are a few "rules of the road" that will help you read this book:

- **Links:** All blue text in this ebook is *hot,* meaning you can click (or tap) it, just like a link on the Web. If you click a link that takes you to a different part of the ebook, you can return quickly to where you were if your ebook reader offers a "back" feature. For example, if you use iBooks to read the EPUB version of this ebook, you can click the "Back

to" link at the lower left. Or, if you use Preview on the Mac to read the PDF version of this ebook, you can choose Go > Back or press Command-[.

- **Menus:** Where I describe choosing a command from a menu in the menu bar, I use an abbreviated description. For example, the abbreviated description for the menu command that creates a new folder in the Finder is "File > New Folder."
- **Mobile devices:** In this book I distinguish between conventional (desktop or laptop) computers and *mobile devices*, by which I mean smartphones, tablets, e-readers, and other handheld computer-like devices. The iPhone, iPad, iPod touch, Kindle, and BlackBerry (among many others) would all be considered mobile devices.

What's New in Version 1.1

Version 1.1 of this book, released about eight months after the original publication date, updates the book with the latest privacy-related information and adds numerous details. The most significant changes are as follows:

- Added a note in Hackers about how to search for information on recent privacy breaches.
- Included a tip in Big Brother with links to resources detailing government surveillance revelations.
- Updated Fix the Easy Things to emphasize the importance of keeping one's operating systems up to date with security fixes.
- Replaced numerous graphics (see, for example, Encrypt Your Wi-Fi Connection) with spiffier versions.
- Made several clarifications about speed and reliability in Use a VPN.
- Added a sidebar, SSL Implementation Bugs, covering the serious SSL vulnerability Apple disclosed and fixed in February 2014.
- Updated the sidebar Set-top Boxes and the Like to further discuss the Internet of Things ("smart" connected objects like light bulbs and thermostats).
- Mentioned how a password manager can ensure that you Go to the Right Site.
- Noted the improved Private Browsing option in Safari for iOS 7 in Private Browsing Modes.
- Included information on iCloud Keychain in Protect Passwords and Credit Card Info.
- In Browse Anonymously, added a note distinguishing between anonymity and untraceability, and mentioned a further Tor vulnerability.

- Mentioned cryptocurrencies such as Bitcoin in Shop Online Privately.
- In Understand the Privacy Risks of Real-Time Communication, noted a potential vulnerability in audio and video chats, and added a sidebar, Security in iMessage and Other Apple Services.
- Added “secret-sharing” apps to the list of areas of concern in Use Other Social Media Precautions.
- Renamed “Create a Private Cloud” to Create a Personal Cloud and added information about several other products.

Introduction

"A book about online privacy? That'll be pretty short!" my friend joked. It was his way of saying, "We both know there's no such thing as privacy on the Internet."

He's not far from the truth, but to be fair, the illusion of privacy extends far beyond the world of computers and networks.

If you want complete privacy, go live in a remote cave without any electronics. Don't build a fire, because the smoke could give away your location. Never step outside, because a satellite or a passing drone might snap your picture. And avoid all human contact, because you never know who might be a spy. I hope you packed plenty of food, water, and clothing, too—you won't be getting any more!

In other words, there's essentially no such thing as total privacy, online or otherwise. People have to interact with each other to survive, and every interaction reveals something about each participant.

I don't know about you, but I wouldn't want it any other way. I like having family and friends who know me well, and who can get in touch with me whenever they want (or need) to. I like sharing thoughts and opinions with a wider audience online. And I like the convenience of using my computer, phone, or tablet to communicate, find directions, and make purchases anywhere in the world. All these things involve revealing information about myself, so I wouldn't want *complete* privacy.

And yet, the Internet turns many of our everyday assumptions about privacy upside down. If I'm at home, I can close the curtains and feel reasonably confident that whatever I say or do inside my house won't be seen or heard by anyone else unless I (or a family member) choose to reveal it. Not so with electronic communications. Whether I'm sending email, browsing the Web, or doing a video chat with a friend, the only safe assumption I can make is that strangers *might* be able to see that information—now or in the future.

Once something has traveled over the Internet in any way, it's potentially out there forever—and potentially public. You can delete a file from your computer, but once data has gone into the cloud, there's never a guarantee that all copies of it have been eternally expunged. In fact, it's far more likely that any given piece of data on the Internet will live on indefinitely. Not only that, but data tends to escape even strong restraints—hence the saying "information wants to be free."

To be brutally honest, someone who wants badly enough to learn what you've transmitted or received on the Internet can probably do so, given enough time, effort, and skill. Part of the reason for this book is to explain how your words, personal information, and activities could become known to individual strangers or even the public—and that knowledge may lead you to make different choices about how you use the Internet. But I'm not saying you must give up any hope of basic privacy. On the contrary, common-sense strategies—the Internet equivalent of drawing the curtains and locking your door—can significantly reduce the risk of having your personal information fall into unwelcome hands. And, when you have more sensitive or valuable data to protect, you can take appropriately stronger measures.

Of course, there are often trade-offs—you may lose convenience, valuable social interaction, and even (paradoxically) personal safety if you choose to keep certain information private. For example, the same technology that can reveal your whereabouts to advertisers could also help someone trying to rescue you during a natural disaster or other emergency. Privacy cuts both ways.

That's why I don't recommend attempting to lock down all electronic communication, all the time. You need the curtains open to see the sunlight, and you need the open Internet too.

This book isn't a guide for the paranoid—or for people with outrageously sensitive or scary secrets to protect. It's a book for ordinary people with ordinary privacy needs. You want to go about your business, enjoying the many benefits of modern technology without worrying that someone is snooping on you all the time—whether to sell you something or for more sinister reasons. That's what I plan to help you do, regardless of whether you use a Mac or PC, iOS or Android device, set-top box, cell phone, or any of a thousand other network-enabled gadgets.

I focus more on general principles than on nitpicky settings, particular apps, or elaborate technological rituals. I offer examples and pointers to more information as appropriate, but I don't dwell on minutiae. The lack of detailed, step-by-step instructions may come as a surprise to some readers, so let me spell out my reasons:

- Privacy settings are a matter of choice. There's no single right answer; each person's decisions about what information to keep private and how to do so will be different from the next person's.
- Each app, operating system, and device has its own way of doing things. Spelling out how to configure the privacy settings in every email client, Web browser, telephony app, and other Internet-connected software—on every version of OS X, Windows, iOS, Android, and other operating systems—would take hundreds of dull pages. And all those instructions would go out of date as soon as the next software or hardware update appears!
- I don't want to give you a false sense of security. Although you can certainly take steps to

dramatically increase your privacy, I don't want you to think that some magical combination of software and settings will keep your online activities completely and permanently private. Knowledge and vigilance go a long way, however.

Think of this book as a primer on the things that affect your online privacy. It tells you what's going on, how it pertains to you, and why you might care. More than that, it puts privacy issues in perspective. If you feel overwhelmed by privacy concerns, you can take control of your online privacy by replacing paranoia and guesses with knowledge and smart choices.

Because I live in the United States, many of my examples involve things I know or suspect to be the case here. But even though laws and policies vary from country to country, nearly everything I say here is applicable in some fashion to anyone in the world.

Online Privacy Quick Start

You can think of this book as being divided into general topics (the first four chapters) and specific topics (the rest). I recommend that you read the first four chapters before you do anything else in order to understand your overall privacy risks and the simple, preliminary steps you can take to reduce them. Then feel free to skip to whichever other chapters are of particular interest.

Identify your online privacy needs:

- Think you have nothing to hide? Think again. Read Learn What You Have to Hide.
- Find out who might be trying to invade your privacy. See Learn Who Wants Your Private Data (and Why).

Take preliminary steps:

- Come up with a plan to deal with most common privacy issues in Develop a Privacy Strategy.
- Block the broadest and most likely privacy risks. See Keep Your Internet Connection Private.

Use specific online services privately:

- Surf and shop without compromising your personal information. Read Browse the Web Privately.
- Reduce the chances that email will be read by anyone other than the intended sender and recipient. See Improve Email Privacy.
- Reduce the chances of eavesdropping when using instant messaging and other audio, video, and chat services. Read Talk and Chat Privately.
- Social may be another way to say “public,” but you need not give up all your privacy when using Facebook, Twitter, and other social networking services. See Keep Social Media Sort of Private-ish.
- Cloud backups and syncing could involve privacy risks if you’re not careful. See Keep File Syncing and Backups Private.
- There are many ways to share files online, but some of them may expose data you’d rather keep private. Read Share Files Privately.

Help others with their online privacy:

- If you have children, you have the additional responsibility to take control of their online privacy. See Maintain Privacy for Your Kids.
- Share what you've learned about online privacy with your friends, family, or a large group. See Teach This Book.

Learn What You Have to Hide

I'm sure you're an honest, moral, law-abiding citizen. Good for you! But if you tell me you have nothing to hide, I'm going to laugh in your face. I'm sorry, but "I have nothing to hide" is an absurd statement, no matter who's saying it. Of course you have things to hide! We all have secrets, and that's as it should be. But you may not realize how much you want to keep private and how you might inadvertently give it away online. That's what I want to help you understand in this brief chapter.

Bear in mind that privacy nearly always depends on context. You may want to keep certain information from your employer but not your doctor; you may want to tell your spouse things that you wouldn't tell your kids; you may share information freely with your lawyer that you would prefer not to have repeated in court. In the next chapter, Learn Who Wants Your Private Data (and Why), I further explore that part of the question—private *from whom*? You can't keep all information private from everyone (and you wouldn't want to), but you can take steps to keep some information private from some people.

Things You Might Want to Keep Private

If you'll indulge me for a moment, I'd like to run down a list of some categories of information you probably want to keep private in the sense of controlling who it's shared with online. This is in no way intended as a complete list, but only as a few highlights:

- **Contact information:** You may hand out business cards freely, but are you willing to let any stranger know your name, telephone number, and home address? (Some people don't mind at all, but others find it problematic.) You enter this information nearly every time you make a purchase online, and in many other situations.
- **Vital statistics:** Personal facts such as your date and place of birth, the names and ages of your parents and children, and your marital status are probably well-known among family and close friends. In the wrong hands, that data could help someone hack into your accounts, steal your identity, or even blackmail you. And yet, you've probably revealed much of this information on Facebook.
- **Location:** Unless you take deliberate steps to prevent it, the mere act of turning on a mobile phone or visiting a Web site on your computer can reveal your physical location, sometimes down to your street address. This information may be stored, too, such that your movements and online activity over time can be mapped out—and that, in turn, can often suggest what you have been doing in all those locations, or even with whom you've

been doing it. Do you mind that someone you don't know can tell where you are now, and where you've been in the past?

- **Financial information:** You may file your taxes online, and you may submit online applications for credit or other financial services. That's all fine; tax authorities, banks, and lenders have a legitimate need to know how much money you earn, what your Social Security number is, and so forth. But I'll bet you wouldn't want *everyone* to know that information. Likewise, you can probably log in to your bank accounts online, but it may not be in your best interest for just anyone to see your bank statements. And yet, any information that's transmitted online could conceivably be misused.
- **Medical information:** Everything that your doctor knows about you—your height and weight, past and present illnesses, surgeries, medications, pregnancies, genetic data, and so on—is almost certainly stored in a computer somewhere. If a security breach or human error resulted in any of that information leaking out, or if you shared it injudiciously by email or social networking, might that have any negative consequences?
- **Purchases:** When you buy anything online, the vendor keeps a record. Your bank may know about all your transactions, too, including those made in person with a credit card. And some of your purchases will also be known to online advertisers. All that data is online somewhere—and some pieces of it are more secure than others. Can you think of any purchase you might not want to be made public?
- **Communication history:** Some of us deliberately save every email message we receive or send, but even if you don't, that information (possibly including messages you deleted long ago) is out there—it's on a server somewhere, or on someone else's computer. Ditto for chats, instant messages, Twitter, and most other forms of electronic communication. Most of it is probably innocuous, but if you ever sent a message that you wouldn't want your mother, spouse, or employer to read, you may have a legitimate worry about your online privacy.
- **Browsing behavior:** You're aware, I'm sure, that every Web site you visit, every Web search, every video you watch, and every file you download leaves a trail, which includes information about your location, your computer, and your browser, among other things. Parts of this trail are stored on your own computer or mobile devices as histories, caches, and cookies. Some parts are stored on the servers of search providers, advertisers, and other entities. It's extremely difficult to avoid leaving a trail and virtually impossible to erase all traces of your browsing behavior after the fact.

I can go on, but I hope I've made my point by now. You want your real-life friends and family to know where you are and what your kids are doing; you don't want strangers to know. You want to order things online, but you don't want your spouse to know about the surprise

birthday present you bought. You want your sister to know you're pregnant, but you want to wait before letting your parents or your employer know.

Unfortunately, you can't always control what happens to information about yourself on the Internet. Far too often, for one reason or another, online information about you becomes available to people or organizations that you would prefer didn't know it—and this usually happens without your knowledge.

Personally Identifiable Information

In the foregoing list, I assumed that all the information about yourself that could conceivably "escape" online can be traced back to you personally. Sometimes that's true, but not always.

If you read the privacy policies of the Web sites you visit (an admittedly boring undertaking that I discuss further in What about Privacy Policies?), you'll notice that they normally distinguish between *personally identifiable information* and *anonymous* or *aggregate* information. This difference is worth understanding.

If a message, database entry, or other snippet of information online includes your full name, your email address, your photograph, your driver's license number, or some other detail that uniquely belongs to you, it's personally identifiable—even if the person or company who has that information hasn't actually identified you with it.

On the other hand, some information—your city, area code, operating system, and so on—is the same for many people. An advertiser may find it useful to know that 145 people in Fresno who also own iPhones visited a certain Web page today, but if you were one of them and that's the only information the advertiser has, it won't point to you personally. This sort of aggregate demographic information is valuable to businesses, political campaigns, and other entities even it doesn't identify you personally. But sometimes a combination of seemingly innocuous facts can turn aggregate information into personal identification (see On a Web Server).

IP addresses are an interesting case. Every device that connects to the Internet uses one, although often more than one device shares an IP address (using a process called NAT, or Network Address Translation), and a device's address may change from time to time. When you visit a Web site, it records your IP address. If you happen to be using a device whose IP address isn't shared, that number can potentially be traced back to you personally. But if you visit the same page at, say, a public library or using a device connected to a public Wi-Fi hotspot, the IP address recorded by the Web site would not be personally identifiable.

Privacy vs. Security vs. Anonymity

The words privacy and security are often tossed around as though they're synonymous, and some people also confuse privacy with anonymity. In fact, these three words all mean different things, but the concepts are related, especially when it comes to the Internet. The basics:

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

To picture the difference between privacy and security, think of a bear. If you visit a bear in a zoo, you have no privacy (anyone can see you) but you have near-total security in regard to the bear: it's very unlikely the bear will harm you or anyone else. On the other hand, if you're in a tent in the woods, you might have privacy (no one can see you) but not security (a bear could still harm you in your tent). Either way, you're anonymous from the bear's point of view (he doesn't know you), but once your remains are identified, we'll all know who you were.

Bears tend not to use the Internet, but you might have **privacy** online if no one can see what you type, the contents of your email, which sites you visit, and so on without your permission. If you are safe from malware, hackers, and other potential causes of harm (including data theft), that's **security**. And if you send a message or visit a Web site without anyone being able to tell that it was you in particular who did so, that's **anonymity**.

Computer security can often increase your privacy, just as a lock on your door (security) can prevent someone from opening it and seeing you in your underwear (privacy). But there are situations in which you might have privacy without security, and vice-versa.

Likewise, if I send you a message only the two of us can read, it's private—but not anonymous if we know each other's identity. If I post a comment anonymously on YouTube, it's not private at all, even though no one may know who it's from.

Learn Who Wants Your Private Data (and Why)

We've seen that lots of information you may want to keep private travels over the Internet. That in itself isn't a problem; after all, you *want* to share private information with your family, friends, doctor, and so on. Problems can occur when someone accesses personally identifiable information (see Personally Identifiable Information) without your consent or even, in some cases, your knowledge.

Who exactly might be trying to learn private information about you online? I'm glad you asked; this chapter shows you who wants to know about you and, crucially, *why*. Knowing who you're trying to keep your private data private *from* is a useful first step.

Advertisers

The Web is powered by advertising as much as it's powered by servers and routers. Many Web sites devote far more space and resources to ads than to their actual content. As you know, it's difficult to read the news, watch a video, check your email, or even search for pictures of cute cats without being bombarded by ads.

Web sites sell advertising space because that's the only way most of them can make any money. However irritating or even slimy you may consider online advertising, it is the mechanism that has kept most Web sites and other Internet services free.

The companies that purchase advertising want to get their money's worth, and that happens only if the ads result in sales. So advertisers expend a tremendous amount of effort to ensure the ads each person sees are likely to be interesting and thus lead to purchases. When advertisers make money, they're able to keep buying ads and the sites that display the ads can stay in business.

Years of experimentation have shown that the most effective ads are those that target *individual* needs and preferences (including things you didn't even think you needed!), not those that are merely relevant to a site's content or the perceived needs of a broad demographic group. For example, if an advertiser knows I'm in the market for an air conditioner and shows me an ad for one—even on a completely unrelated site—the chances of making a sale go way up.

How might an advertiser know I'm in the market for an air conditioner if I'm not on the site that sells air conditioners? There are a number of techniques, including tracking cookies (which I discuss in Manage Local Storage of Private Data), but most involve using instructions hidden on a Web page that store data on my device when I visit one site (say, a search at Amazon.com) and then check that same data when I go to another site (say, weather.com) containing an ad from the same provider or advertising network. Although the server may store the details of my visit, the local data enables me to be identified across sites.

As you search the Web, browse various sites, follow links, and use ad-supported apps, advertisers can build up elaborate profiles of your perceived interests and tastes. And, because your IP address (or profile information you've entered into a social networking site like Google+ or Facebook) tells them roughly where you are, they can even display ads for local businesses selling the products you've shown interest in.

Unless you regularly search for things that someone else might regard as suspicious, none of this should be a concern. After all, if I truly do want to buy an air conditioner, I'd rather see an ad for an air conditioner than an ad for weight-loss products or hair color. Targeted ads should, in principle, be more helpful to me than random ads.

But…

Individually targeted advertising isn't always to your benefit. The same bits of data advertisers can piece together to determine your interests and location can be used for things like showing higher prices on furniture to people who live in wealthy neighborhoods—or higher prices on electronics to people using Macs rather than PCs. They could also be used to determine that you are a registered voter in the "wrong" party, resulting in a phone call sending you to the wrong polling place.

In fact, the privacy concerns get even worse. Imagine this scenario, only slightly fictionalized from real life. A retailer tracks your online purchases and, noticing that you're buying larger clothes, folic acid, and unscented lotions, guesses that you might be pregnant. Then, in an effort to be "helpful," they display ads for baby clothes and cribs—or maybe they even send such ads by mail. Now family members, coworkers, or other people who might see those ads *also* suspect that you're pregnant. Oops.

The variations on this theme are endless, but the point is that advertising can never be targeted with perfect precision. An advertiser may think it's showing ads only to you, but your spouse, parents, kids, or anyone else who might use the same accounts or electronic devices can also infer private information about you by seeing on your screens the ads that were targeted at you.

When targeting becomes unfair or misleading, when it gives away personal information to others, or when it benefits only the advertiser and not the consumer, you may feel that your private data has been misused. Unfortunately, there's no master switch you can throw that says, "Sure, you can know who I am and what I search for, but only if you use that information responsibly." If advertising becomes intrusive or creepy rather than helpful, you may want to take steps to prevent any advertiser from collecting your private data, not just objectionable advertisers. As you'll see throughout this book, the number of ways in which you voluntarily give away personal data extends far beyond the Web sites you visit, so this isn't a problem with a perfect solution—but you can certainly reduce the risk.

The Google Problem

Google isn't just a search engine; it's a provider of email, document storage, videos, phone service, and numerous other capabilities. What they all have in common is Google's legendary contextual advertising—that's how Google makes money. And the more of Google's services you use, the more personal data the company has about you that can be used to target ads with ever greater precision. Make no mistake about it: every search, every YouTube video viewed, every email read contributes to Google's personal profile on you, to be used for the express purpose of displaying targeted ads.

You can use other search engines and other email providers, buy a non-Android cell phone, and watch videos on sites other than YouTube. But it's nearly impossible to avoid Google altogether (although some people try). By all accounts, Google works hard to prevent your personal data from falling into *other* companies' hands—after all, that would be giving away the store. But will Google be able to protect your data from everyone, forever? And can you trust Google itself not to be evil with your data?

On the one hand, it's not in Google's best interest to alienate its users. On the other hand, it is a giant corporation whose primary mission is to increase shareholder value, not to protect your privacy. If push came to shove, I'd have to guess Google would choose profit over kindness. And, even the best-intentioned companies sometimes experience security breaches that leak personal data.

I won't say that you shouldn't trust Google. But you should be aware of the massive amount of information most of us give Google for free—and remember that there's always a cost somewhere.

And, even though I'm picking on Google here as the largest provider in its class, you shouldn't think other companies with comparable services (Microsoft, Yahoo, and so on) are fundamentally different. The more data any company has about you, the more power they have—and the greater the risks to your privacy at their hands.

Local Villains

Another category of people who might be out to get the digital goods on you is what I'll call "local villains." Let me give you some examples:

- Ex-spouses or former partners who want to make your life miserable or even find evidence to use against you in court
- Neighbors with whom you have a dispute or disagreement

- Your current employer, who may want to make sure you're not violating company policies or misusing proprietary information
- A prospective employer who's trying to judge your appropriateness for a position
- Stalkers, thieves, and other criminals looking for evidence of when you're home or not, where your kids are, and other information
- Friends and relatives who like to snoop and gossip

As a group, local villains tend to be less technologically sophisticated than advertisers, hackers, and others who seek your personal information. On the other hand, they may be more motivated, and they're far more likely to be focused on you *personally* rather than on a sales demographic you represent. And, let's face it, most of us have tons of personal information online that's readily accessible by the general public—Facebook, Twitter, Flickr, personal blogs, and so on.

Hackers

Some of them do it for fun. Some do it for notoriety. Some do it to make money. But one way or another, thousands of intelligent but misguided people around the world spend every waking hour trying to break into computer systems to steal information and money, to trick you into buying something, or simply to cause mischief.

I shouldn't call them "hackers," because hacking is a noble art and only a small subset of hackers use their powers for evil. But you know what I mean: black hats. People—mostly young men—who write and distribute viruses, keyloggers, Trojan horses, and other malware. People who send spam and use phishing messages to con you into handing over your passwords. People who take over computers by the millions to turn them into botnets. Bad guys.

Hackers rarely target specific individuals—in most cases, it's nothing personal. The two pieces of private information most of these bad guys would be happiest to have are your credit card number (for obvious reasons) and any password that protects financial information (for the same reasons) or provides access to large amounts of your data, such as your email account. Although it's difficult to protect your privacy from a truly determined hacker, you can take steps (as discussed elsewhere in this book) to make their work harder and less rewarding.

Note: If you want to see what the bad guys—hackers and others—have been up to lately, you can search the massive (although incomplete) database of the Privacy Rights Clearinghouse for privacy breaches. It's fascinating and deeply sobering: the list is extremely long and growing fast.

Big Media

The RIAA (Recording Industry Association of America) and MPAA (Motion Picture Association of America)—along with record labels, movie studios, publishers, and other major copyright holders—are keen to know who has been pirating their media. Apart from monitoring BitTorrent traffic and file sharing sites, these firms work closely with ISPs to identify people who illegally share movies, software, and other copyrighted materials. Depending on your location and provider, this could lead to serious consequences including civil lawsuits and termination of your Internet service.

I don't blame copyright holders for protecting their property; I've had my own work pirated and lost money because of it, and it's no fun. (You *did* pay for this book, right? Just checking. If not, I should mention in passing that I can see you right now.)

The problem is, sometimes big media companies make mistakes. They've sued little old grandmothers who don't even own computers and made other egregious blunders. Even if you'd never consider stealing media (I did tell you I'm watching, right?), you might prefer that your file sharing activities be kept private.

Big Money

Banks, credit unions, credit card providers, and other financial institutions may want evidence of your thriftiness or trustworthiness in considering whether to offer you a mortgage or other loan. Insurers may want to see whether you engage in risky behavior or have medical conditions that might influence your rates or disqualify you. When lots of money is at stake, it's only prudent to collect as much information as possible to make a good decision. That's as true for large corporations as it is for you.

You should not be at all surprised if a potential lender or insurer checks out your Facebook page or searches for your name on Google. Your health-food blog and tweets about your jogging regimen might score you a better life-insurance premium; Facebook posts about late-night drinking binges could raise your car insurance rates. You may never learn *why* these things happened, either—companies generally aren't required to reveal how they go about researching you.

Big Data

I've mentioned Google (and will do so again)—it may be the largest non-governmental data collection entity in the world. But it's certainly not the only one. Facebook, Twitter, and other companies with users numbering in the hundreds of millions collect massive amounts of data on users' tastes, preferences, opinions, geographical whereabouts, and other details.

Although this data is mostly used for targeting advertising (see Advertisers), it can also be put to many other uses, from the virtuous (helping you find a parking space) to the creepy (profiling you as a potential criminal).

Big Brother

Unless you've been protecting your privacy by living in a remote cave without electronics or human contact, you're probably aware of the string of revelations starting in mid-2013 about ways in which government agencies, including the NSA (National Security Agency) in the United States and Britain's GCHQ (Government Communications Headquarters), have been secretly collecting phone records, email, recordings of Skype conversations, and other data most of us thought was private—on the authority of secret courts and accompanied by gag orders that prevented those who knew about the data collection from revealing it. In fact, this sort of thing has been going on for a long time, and there's no end in sight. The public might never know the full nature or extent of government data monitoring.

Tip: For detailed and continuously updated discussions of the ongoing revelations about government monitoring, see Timeline of NSA Domestic Spying at the Electronic Frontier Foundation (EFF) or Global surveillance disclosures (2013–present) at Wikipedia.

All this is being done, of course, in the name of preventing terrorism and other crimes. You may or may not believe that. You may trust the government and feel that a reduction of privacy is justified by an increase in security, or you may feel the whole thing is an appalling abuse of power. Whatever your opinions, I believe the following facts are uncontroversial:

- Massive data collection has happened and continues to happen. There are apparently no *technological* barriers preventing the government from monitoring most email, phone calls, and other online data.
- The laws governing data collection may eventually change, but if the U.S. government's current monitoring was performed for years without the public's knowledge that the law permitted it, the same thing can happen again. (And in any case, making something illegal doesn't mean it won't occur.)
- Although we now know something about data collection by the NSA, FBI, and other U.S. law enforcement agencies—and comparable efforts in certain other countries—the full extent of global monitoring is unknown. It's plausible that other governments have the capability to capture at least some of your personal data, even if you access Internet services only in your own country.
- Other than lobbying for changes in laws you may disagree with and voting for people whose privacy positions you trust, there's little that average citizens can do about this sort

of data collection.

Going back to the "I have nothing to hide" argument (see Learn What You Have to Hide), the difficulty with all this from a privacy point of view is that even if you are the most harmless and trustworthy person in the world, something you say or do online could be misconstrued or misrepresented. Just as spam filters incorrectly flag some legitimate messages as junk mail, government computers could incorrectly flag you as a potential threat, and that could have consequences ranging from inconvenient (such as being put on a no-fly list) to devastating (being charged with a crime you didn't commit). Computers have been known to make mistakes—and so have the people using them.

What about Privacy Policies?

Almost every Web site and Internet service has a published privacy policy, and I'd think twice about using a site without one. Privacy policies spell out what data the company collects (particularly personally identifiable information), how it's used, what protections are in place to safeguard it, and so on.

Privacy policies, like software licenses, are typically full of boring, inscrutable legalese. They might be good for curing insomnia, but they're not exactly page-turners. Even so, you might find it interesting and educational to read the privacy policies from a few sites you visit often. As you do, keep the following in mind:

- Although a company may be legally obligated to publish a privacy policy stating how it uses your data, it's not required to have a policy that *protects* your privacy. A privacy policy could state, "We ruthlessly collect every scrap of personally identifiable information we can find about each user and sell it to the highest bidder, with malice aforethought." So, don't mistake the *presence* of a privacy policy for a pledge of privacy.
- Privacy policies sometimes contain cleverly worded loopholes—and policies could be updated without your knowledge to become less protective of your personal information.
- However strict and commendable a privacy policy may be, it is, at best, only a *policy*—not a barrier. A company may say it stores your data in a secret mountain fortress protected by a dragon, but does it have a contingency plan in case a hobbit shows up with a magic ring and a bunch of dwarves? These things happen.
- A privacy policy does not, by itself, have the force of law. If you can prove that a company violated its stated policy, you might be able to win damages in a civil lawsuit. But that can't prevent, undo, or correct a breach of privacy.

I wouldn't want to do business with a company whose privacy policy admitted to practices I disagree with, and I'd rather know about such things up front. But even a fantastic privacy

policy is no guarantee.

Develop a Privacy Strategy

Online privacy is, as you now know, a complex problem with no definitive solutions. But it doesn't have to be overwhelming. In this chapter, I help you think through a high-level strategy you can use to help inform your decisions about specific tasks such as Web browsing, email, and file sharing (all of which I cover later in the book).

I suggest dividing your privacy concerns into three broad categories:

- First, Fix the Easy Things—that is, make simple changes to your software, settings, and habits that will address many of your privacy concerns but will require almost no planning or effort.
- Next, Create Privacy Rules for Yourself. These simple statements focus on a few types of information you always want to take extra care with and a few people you always want to communicate with privately.
- Finally, Cope with Special Cases. Troubling situations may come up occasionally that require extra privacy but for which you don't have an existing system. Think through the possibilities in advance and prepare for them so you don't make a foolish decision on the spur of the moment.

For extra credit, Take the Pledge: promise me, yourself, and the rest of the world that you won't do stupid things online.

Fix the Easy Things

You instinctively take measures to protect your real-world privacy—you draw the curtains at night, use a changing room to try on clothes, and lower your voice when discussing something sensitive in public. Adopting a comparable set of habits for online communication can eliminate some of your most serious privacy risks. Better yet, you can make a number of simple, one-time adjustments to your devices and software that will improve your ongoing privacy without further effort.

I cover many of these "easy things" elsewhere in the book, but I'll list some prominent examples now.

First, here are some one-time changes you might consider:

- **For your Internet connection:** Follow the advice in Keep Your Internet Connection

Private, including using WPA encryption on your Wi-Fi network (see Encrypt Your Wi-Fi Connection), turning on your computer's firewall (see Use a Firewall), and fortifying your DNS settings (see Avoid DNS Mischief).

- **When browsing the Web:** Use your browser's built-in controls or third-party software to confirm that you're not visiting fake or dangerous sites; see Go to the Right Site. Also, configure your Web browsers not to store third-party cookies and other unnecessary private data, or take even stronger measures such as blocking all ads and trackers; see Manage Local Storage of Private Data.
- **For email:** Make sure your email program transmits your password in an encrypted form (see Log In Securely), or better yet, use SSL for incoming and outgoing mail (see Transfer Email Securely).

Next, consider adopting some new customs, such as:

- Always use a VPN to connect to the Internet when you're on an open or unfamiliar network; see Use a VPN.
- Use a password manager not only to store passwords and credit card data securely, but also to reduce the risk of phishing; see Protect Passwords and Credit Card Info.
- Kick the Google (Bing, Yahoo, etc.) habit for searches; see Search Privately.
- If your computer or other device supports multiple user accounts, be sure to set up an account for each family member or coworker who uses the device—each account protected with a password known only to its user. Be scrupulous about logging out of your own account after each session.
- Make sure the operating system on each of your devices is always up to date. Software updates regularly patch security holes that might otherwise compromise your privacy. (I mention one example later, in the sidebar SSL Implementation Bugs.)

Those changes made, you can move on to specific privacy rules.

Create Privacy Rules for Yourself

Some pieces of information (refer back to Things You Might Want to Keep Private) are nearly always private in the sense that you likely want to control who knows them. And there may be some people with whom you almost always want to communicate privately, regardless of the topic—your doctor, lawyer, accountant, therapist, minister, AA sponsor, business colleagues, clients, and so on.

Only you can say which facts and conversations count as private for you. You can't foresee every situation, but you can identify information and people that deserve extra care when it comes to online privacy. For now, jot down a list of your privacy "triggers." For example, someone might list:

- My credit card numbers
- My new pseudonymous novel
- My chocolate chip cookie recipe
- My mistress
- My attorney
- My FBI handler

Or whatever. Then, as you read this book and learn about the specific privacy risks and options for various types of online communication, you can form these into simple rules, for example:

- I'll never send a credit card number or Social Security number by email unless it's encrypted (*and* I'm confident that the recipient will protect the information on the other end).
- I'll insist that my publisher use a secure Web portal for discussing "J.K.'s new novel." (No one will guess my true identity!)
- I'll talk about my ____ (invention, legal concern, addiction, etc.) only by phone or in person—never in writing of any kind.
- I'll use an anonymous Web browsing tool such as Tor (see Browse Anonymously) when researching competing cookie recipes.

Cope with Special Cases

Online privacy gets tricky when you encounter a situation you weren't expecting—one that isn't covered by your up-front fixes, ongoing habits, and regular rules. For example:

- You win the lottery, and suddenly you have a thousand new "friends" who want a piece of the action.
- You find yourself embroiled in a messy divorce.
- You witness or are otherwise close to a newsworthy event that results in reporters, lawyers, and scammers crawling out of the woodwork and paying you special attention.

- You find yourself in a delicate position involving your health, your insurance, and your employer.
- You or a family member are suspected of a crime.
- You have a fleeting error in moral judgment that may turn out to have far-reaching consequences.

In these and many other situations, your online actions could become subject to much greater scrutiny than normal—you now have to worry about being targeted personally.

No one likes to think about these things, but they do happen, and you're more likely to get through them unscathed if you've spent at least a little time thinking about the online privacy implications in advance.

My first piece of advice is: If humanly possible, avoid saying *anything* about the situation online in any way. The less digital information you generate that could come back to haunt you, the better.

Second, however tempting it may be, don't go crazy deleting things, shutting down accounts, ditching equipment, and the like. That looks suspicious, and could draw unwanted attention to your actions. (Besides, it won't matter, because nothing ever truly disappears from the Internet.)

Third, if the situation has any legal implications whatsoever, find yourself a good lawyer and follow her instructions to the letter.

After doing all those things and allowing yourself some time and mental space to think about your situation clearly, if circumstances permit (and your lawyer, if any, agrees), consider cranking all your privacy settings up to 11. That is, go back to everything in this book that you decided wasn't worth the effort or was too inconvenient, and do it anyway. Use a VPN all the time. Use only Tor (see Browse Anonymously) for Web browsing. Limit your email to completely commonplace, uncontroversial topics. Avoid Facebook, Twitter, and other social media until the situation stabilizes.

I hope you never find yourself having to take such drastic measures. (Unless you win the lottery, because I can totally help you out there.) But if you remember that online privacy is inversely proportional to your need for it, you'll be in much better shape.

That sets the stage for the final topic of this chapter: avoiding stupidity online.

Take the Pledge

Regardless of what measures you take to protect your privacy, there are certain things that should never, ever, under any circumstances or for any reason, be sent over any network. I would have thought this is obvious, but judging by frequent news reports, politicians, actors, professional athletes, and other celebrities still haven't gotten the memo that online privacy is the exception rather than the rule.

You don't have to be rich or famous to have your life ruined by online stupidity. Anyone with fingers and a Web browser can find millions of photographs, videos, email messages, tweets, Facebook posts, and other digital artifacts showing humans at their worst. And more often than not, this stuff is put online *deliberately* by the very people who stand to lose the most…

"Look how fast I can drive this train!" boasted a railway engineer online before recklessly causing a derailment that killed dozens of people.

"I'm sure my wife won't mind a bit of harmless online flirting with other women," said a public official whose wife—and constituents—turned out to mind very much.

"Stealing this car will be a piece of cake," said the guys whose every movement was being recorded on dozens of traffic cams.

"Why, yes, I think it would be a great idea for me to post a video of our drunken college orgy!" said a young lady who will find it difficult to get any respectable job in the future because her prospective employers know how to use a search engine.

Folks, the very best decision—for you and for the rest of the world—is to *stop doing stupid things*. But if you are going to do stupid things anyway, don't compound your stupidity by putting evidence of it on the Internet, which, as you'll recall, never forgets. As you've seen already and will learn in more detail throughout this book, it's nearly impossible to guarantee complete online privacy—and the worse you behave, the more likely it is that evidence of your behavior will emerge.

So, I'm not merely going to tell you to refrain from putting potentially incriminating information about yourself online. I'm going to ask you to *promise* me not to be stupid online. I ask you to join me in taking The Pledge.

Turn on your webcam, raise your right hand, and repeat these words:

> *I, (state your name), do hereby solemnly affirm before the all-seeing, all-remembering eye of the Internet that I will never, ever, under any circumstances, for any reason, or in any manner, knowingly cause or permit any of the following information to travel over any network:*

1. *Statements that are hateful, abusive, racist, or otherwise cruel*
2. *Nude or sexually suggestive pictures or videos of myself, my friends, my family, current or former romantic partners, or anyone else who might at some point deserve to have a life*
3. *Information that could implicate me, rightly or wrongly, in any crime*
4. *Any material that violates someone else's copyright, patent, or other intellectual property*
5. *Anything I'd be ashamed for my (current or future) children to see or hear*

> *I further acknowledge that any failure to keep this pledge disqualifies me from ever holding political office, practicing law or medicine, teaching in a public school or university, holding any government or public sector job, owning a puppy, living in a nice home, finding (or keeping) true love, receiving technical support, enjoying ice cream, or pretty much anything else that might bring me happiness.*
>
> *I therefore, voluntarily and without coercion, undertake to avoid extreme online stupidity for the rest of my days.*

By the way, there's a fine of US$1,024 (or the Bitcoin equivalent) for each infraction of this pledge, payable directly to me. Yes, I take PayPal.

Keep Your Internet Connection Private

Whether you're on a Wi-Fi, cellular, or wired connection, keeping your link to the Internet itself private is an important step that affects all the other traffic your devices send and receive—Web, email, video, and everything else. In this chapter I discuss some of the ways in which another person or company could eavesdrop on your Internet activities or even misdirect you into connecting to bogus sites in order to steal information from you. Then I describe steps you can take to reduce the most serious of these risks.

Understand the Privacy Risks of Your Internet Connection

The connection between your device (computer, smartphone, set-top box, etc.) and a server (Web server, email server, streaming video server, etc.) may involve numerous steps. For example, your laptop may connect to a wireless router via Wi-Fi, which then connects to a cable modem via Ethernet, and then to your ISP over coaxial or fiber-optic cable. Your ISP, in turn, sends requests for data through a series of routers and network operators until they reach the desired destination. Sometimes the simple act of visiting a Web page can involve requests going back and forth between dozens of routers and servers all over the world.

So, although you may have the impression that your computer is talking "directly" to a server somewhere, that's almost never the case. Internet connections, by their nature, are indirect. And at any point between your device and the remote server, the data could potentially be monitored or intercepted.

To get the bad news out of the way first, let's look at some of the likely trouble spots:

- **Wi-Fi connections:** If your device connects to the Internet wirelessly, as most do, someone nearby (even in another building) could "sniff" the Wi-Fi signal and watch or record all the data transmitted and received. This is easy to do when Wi-Fi connections are open, or unencrypted, and if a connection uses WEP, an older security method, it's only a tiny bit more challenging. Newer Wi-Fi security protocols, such as WPA, offer protection that's much better—although still not foolproof (especially if the network's password is weak or can be guessed by brute force).

  A compromised Wi-Fi connection can lead to not only to passive snooping but also active attacks. For example, a man-in-the-middle attack is one in which two parties think they're communicating directly but are instead manipulated into channeling their data through a third party, who can monitor and alter it in transit. (A man-in-the-middle attack can occur

anywhere, but it's especially easy to perpetrate on an open Wi-Fi network.) If I used a man-in-the-middle attack on an instant messaging conversation, I would see what each party types, but they would see only what I relay—which may or may not be what the other person said.

- **Cellular connections:** The cellular data connection between your phone or tablet and your ISP can also be monitored and intercepted. Unless you work for the carrier (which can presumably monitor anything that's not encrypted), doing so requires the use of specialized equipment and skills. It's not something a kid in a coffee shop is likely to pull off, but it's certainly within the capabilities of law enforcement and sophisticated criminals.
- **DNS disruptions:** DNS (Domain Name System) servers translate domain names (such as `apple.com`) into IP addresses (such as `17.149.160.49`). But if your device were tricked into using the wrong address for a server, you could end up at a fake but look-alike site designed to steal your password or other personal data—or perhaps just display ads. Several types of DNS attacks exist, including DNS hijacking, which often takes the form of malware that modifies your computer's DNS settings; and DNS spoofing (also known as cache poisoning), which inserts false information directly into a DNS server.
- **ISP monitoring:** Your ISP can (and likely does) monitor and log any data that flows through its routers—including your IP address, the addresses of any servers you connect to, and the quantity and type of data you transfer. Logs may be kept indefinitely and could be inspected by your ISP's employees, law enforcement, or (potentially) hackers. Besides monitoring data, your ISP could censor data—for example, blocking access to certain domains or the use of certain protocols.

  But, your ISP can't see the contents of encrypted data you send or receive, but it knows how much data was transferred, and who was on each end of the exchange.

- **Router monitoring:** What's true of your ISP is also true of any other router between your ISP and the servers you want to reach—and there may be many of these. For example, numerous countries have national firewalls that prevent anyone within their borders from reaching sites or services deemed to be unsuitable.
- **Malware:** If you have the misfortune to download a virus, worm, Trojan horse, or other malware, any number of privacy risks could exist. Some malware logs every keystroke you type in order to capture passwords, credit card numbers, and other personal data. Other malware may alter your DNS settings (as described earlier in this list), turn your computer into a spam-sending robot, or display an endless series of pop-up ads.
- **Location discovery:** I've mentioned how your IP address can give away your location and sometimes even your identity—and your IP address is known to every site and service

you connect to. Even if you use methods (discussed ahead in Prevent Snooping) to disguise your IP address, your computer or mobile device may determine and transmit your location using other methods, including the names of nearby Wi-Fi networks, triangulating on cellular radio signals, and using GPS coordinates (for suitably equipped devices).

Pretty grim, right? Could be, but fortunately, many of these privacy threats are easily overcome, as I explain in the rest of this chapter.

Prevent Snooping

If you take steps to secure the connection between your computer (or other devices) and the Internet, you eliminate one of the easiest methods available to an attacker who might want access to your private data—or who might simply be searching randomly for low-hanging fruit. Depending on your situation, you may use any or all of several techniques.

> **Note:** In later chapters, I'll talk specifically about additional steps you can take to Browse the Web Privately and Improve Email Privacy, among other things.

Here are some of the ways you can keep outsiders from snooping on your Internet connection.

Encrypt Your Wi-Fi Connection

Even if your main computer uses a wired Ethernet connection, you're bound to have some device—a laptop, smartphone, or tablet, for instance—that can connect only using Wi-Fi. Without any encryption at all, your Internet connection might look something like **Figure 1**.

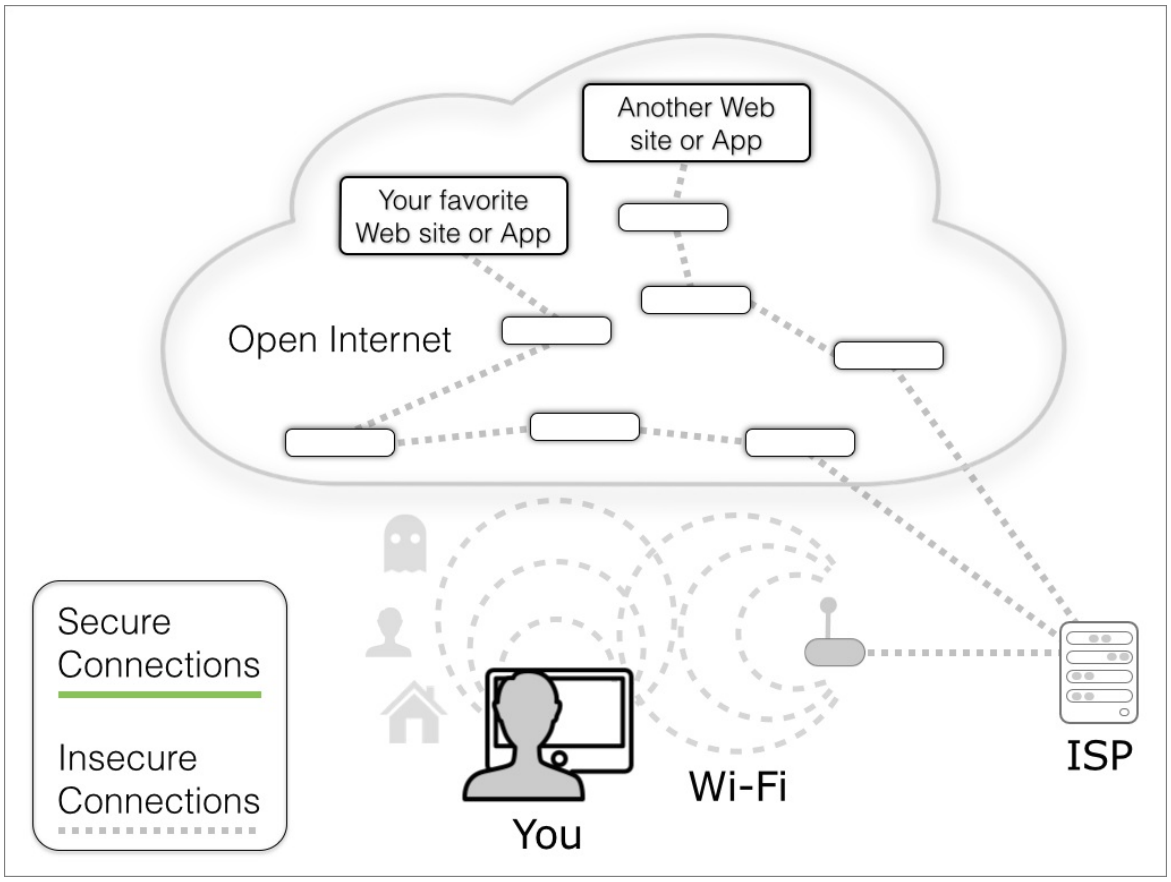


Figure 1: Without encryption, your Wi-Fi connection—the most local and most vulnerable portion of the path to other computers on the Internet—could easily be "sniffed" by someone nearby.

Assuming that you own or control the Wi-Fi router or base station, you should take immediate action to make certain no one else can eavesdrop on your communications—see the documentation that came with your router or refer to the manufacturer's Web site for specific instructions:

- **Use WPA.** Wi-Fi Protected Access (WPA) is the most secure standard for Wi-Fi encryption currently in widespread use. It comes in several flavors, so you may see options like "WPA/WPA2 Personal" and "WPA2 Enterprise" (**Figure 2**). I can't get into the details here, although I'll mention that if you use an Apple AirPort base station or Time Capsule for wireless networking, you'll find lots of good information in Glenn Fleishman's ebook *Take Control of Your 802.11n AirPort Network*.

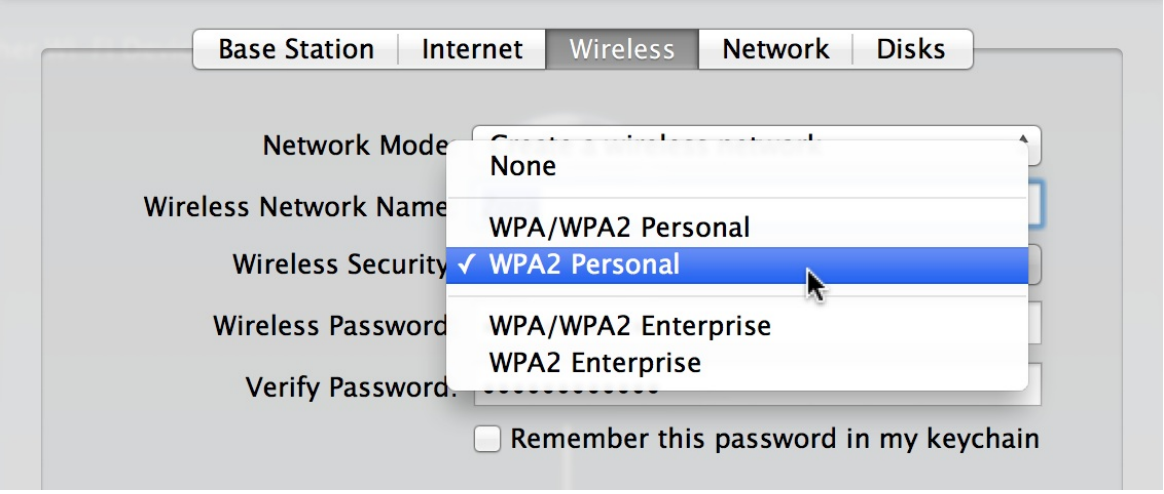


Figure 2: Wireless security options for an Apple AirPort base station. Choose any of the options including "WPA" and you should be fine.

Choose any variety of WPA, but *do not use WEP* (Wired Equivalency Protocol)—it's trivially easy to crack. And *do not skip wireless encryption*. You could choose "None" as the wireless encryption type, but don't; that's ridiculously insecure and never the right choice if you can avoid it.

Note: If WEP is the only option available on your base station, it's probably an old one. Now is a good time to think about replacing it.

With WPA-encrypted Wi-Fi, your connection looks like **Figure 3**

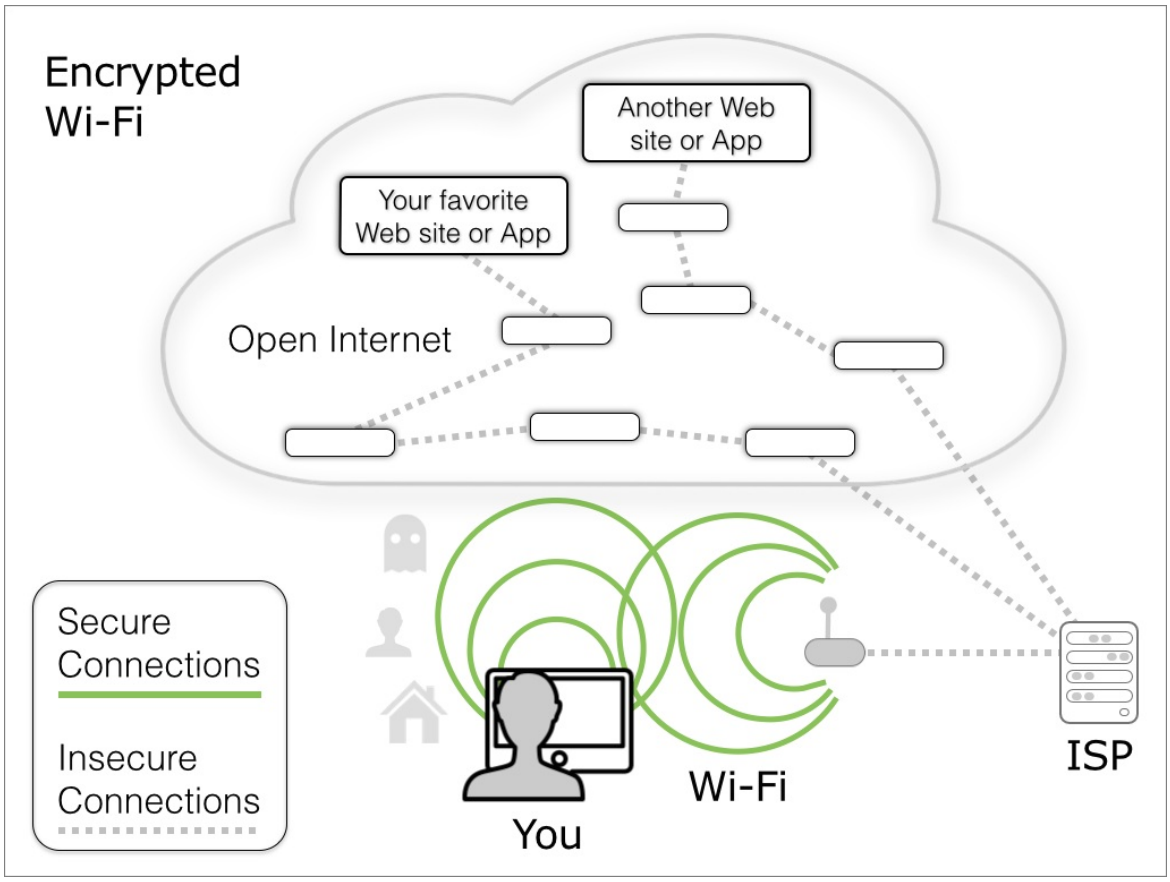


Figure 3: With encrypted Wi-Fi, you protect the local portion of your Internet connection from sniffing.

- **Use a good wireless network password.** The password you create to connect to the Wi-Fi network should be long, random, and complex to avoid automated attacks in which a computer systematically tries likely passwords until it finds the right one.
- **Use a good administrative password.** In addition to the password for your wireless network, your base station or wireless router has an administrative password, which you must enter in order to modify its settings. Be sure to change the default password—it's often "password" or something else similarly insecure. Ideally, the administrative password should be different from, but just as strong as, the password for your wireless network.

Tip: In my book *Take Control of Your Passwords* I talk about the risks of bad passwords, how to choose and remember great passwords, when and how to use a password manager, and more.

What if you're on someone else's Wi-Fi network? If it happens to use WPA, that's good, but since other people will know the password, your connection is somewhat more vulnerable to hacking than your own network would be. If the network uses no encryption or WEP—or if you want extra insurance on a public WPA network—you need to take matters into your own hands by using a VPN, as I describe next.

Use a VPN

A Virtual Private Network, or VPN, is a special type of network connection that encrypts all Internet traffic flowing between your device and a VPN server somewhere on the Internet. Think of a VPN as a tunnel running through your physical (Wi-Fi, cellular, or wired) Internet connection that's impenetrable from the outside but open on both ends (**Figure 4**). Since VPNs encrypt everything, they even make it safe to use an unencrypted Wi-Fi connection.

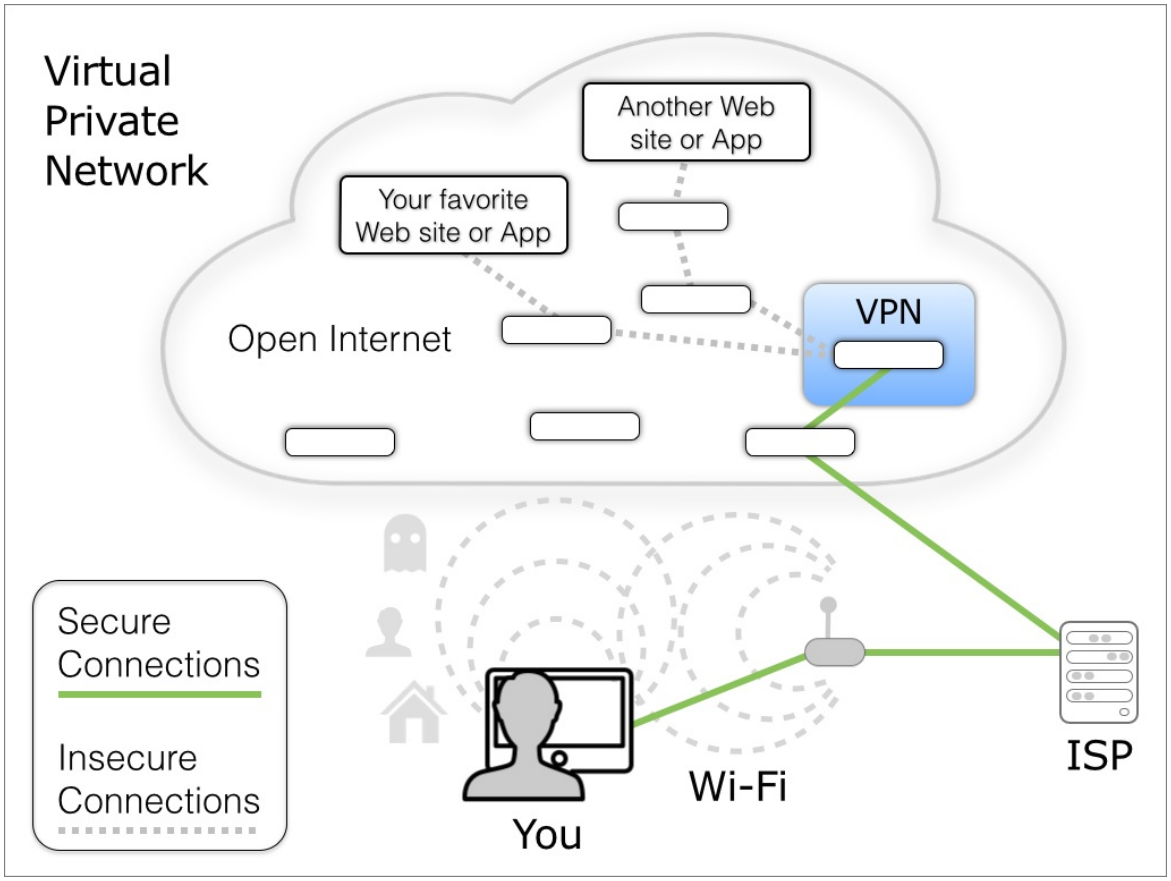


Figure 4: Using a VPN encrypts the entire Internet connection between your device and your VPN provider, protecting a greater portion of your data's path than encrypted Wi-Fi alone.

With a VPN, your computer or other device appears to be on the same local network as the VPN server. So, for example, if that server is located in your company's data center, connecting to it gives your computer the same access to your corporate network that it would have if it were in the same building—access that would otherwise be blocked from the outside by a firewall. And your IP address will be assigned by the VPN, so if the VPN server is in, say, France but you're physically in Los Angeles, your IP address will most likely appear (from the perspective of any server you connect to) to be in France.

Large corporations often run their own VPNs, and if you work for such a company, your IT people can explain how to get up and running. But ordinary citizens can also take advantage of VPNs by signing up for any of numerous commercial services. Some (such as Hotspot Shield) offer free, ad-supported VPN service, while others (such as Cloak and my personal favorite, WiTopia) require paid subscriptions. A quick Web search will turn up numerous other options.

Macs, Windows PCs, and most mobile devices have built-in VPN software, so in many cases, all you have to do is sign up for a service, enter a few settings (including your username and password), and click or tap a button to activate the VPN (**Figure 5**). In cases where a VPN requires custom software, it's nearly always a free (or free-with-purchase) download. In any case, the VPN service you select will provide detailed online instructions for setting up each of your devices.

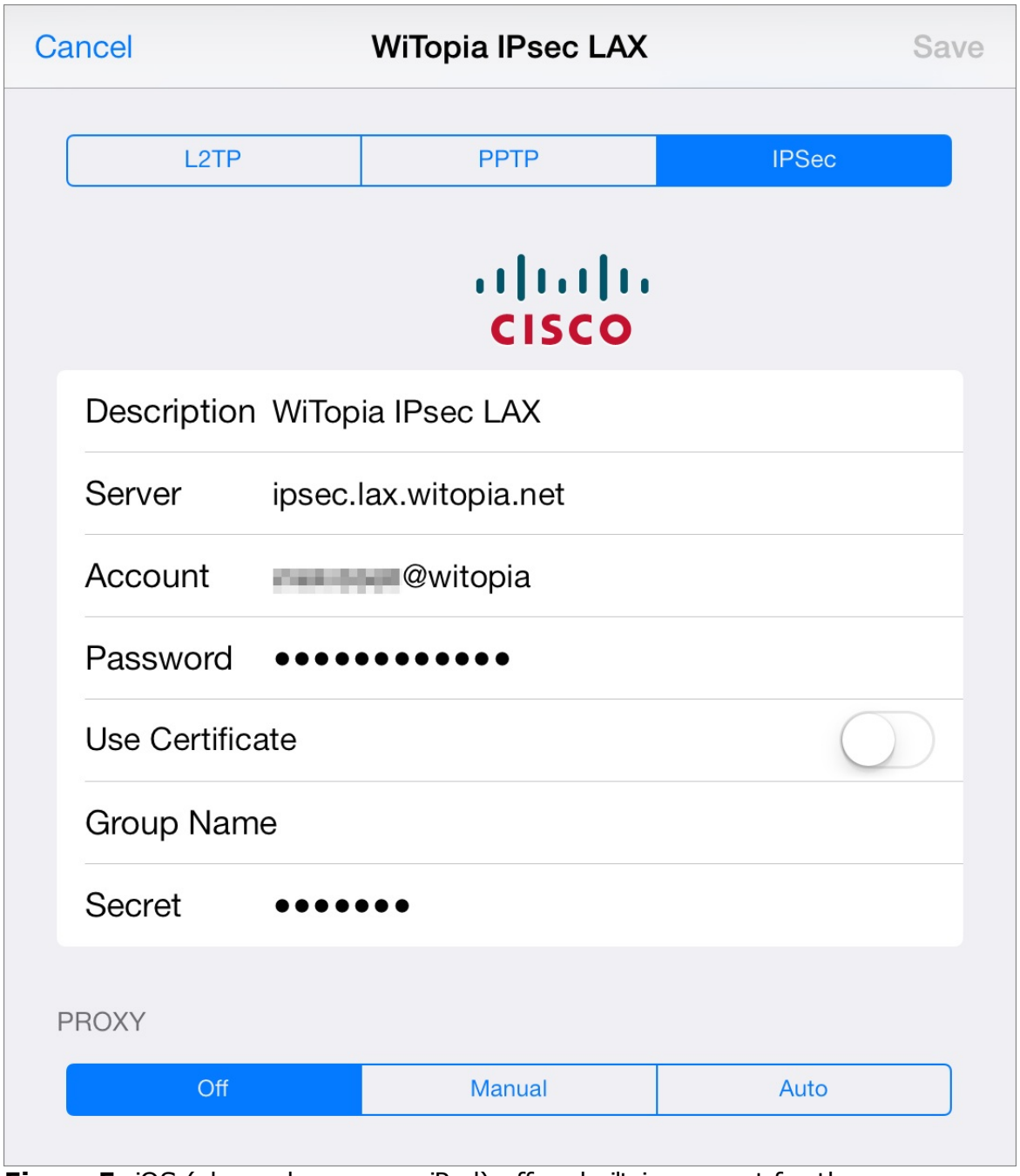


Figure 5: iOS (shown here on an iPad) offers built-in support for three common VPN types—L2TP, PPTP, and IPsec.

VPNs are great, and I use them all the time on public Wi-Fi networks, and sometimes even with my iPhone over a cellular connection. However, I should mention a few qualifications:

- In general, VPNs are active only when you explicitly turn them on. If your device goes to sleep, switches physical networks, or loses its connection, you may have to manually

restart the VPN. In fact, even when you stay on the same physical network, VPN connections have a way of flaking out—sometimes without any obvious sign that you've lost your secure connection—just when you need them most. Pay attention to make sure you're connected when you need to be.

- VPNs protect your local Internet connection but not the entire path to a remote site or server; I say more about this in the sidebar The Problem of End-to-End Privacy, just ahead.
- Certain types of VPNs (typically used in enterprise and education settings) split the traffic such that only data traveling to and from the institution's network is encrypted, whereas access to the outside Internet remains unprotected.
- Because of the overhead required to encrypt and decrypt data, VPNs are always slower than unencrypted connections. Whether that's noticeable will depend on your hardware, software, VPN type, and the location of the server you connect to. But it could cause problems for activities that require lots of bandwidth or low latency, such as streaming video or fast-paced games.
- In general, a VPN connection must be made individually from each device—and you may have devices (such as set-top boxes) that can't use VPNs. A brilliant, if somewhat pricey, solution to this problem is the CloakBox Pro VPN Router from WiTopia. It's a router that makes a permanent VPN connection to any of numerous servers around the world, and then passes that encrypted connection to any devices you connect to it via Ethernet or Wi-Fi. I used one of these myself for a few years, and can vouch for its effectiveness. But bear in mind the impact on bandwidth and latency (above), which can be substantial and will affect your whole network.

The Problem of End-to-End Privacy

When you use a VPN, your Internet connection is encrypted only between your device and the VPN server. Whatever site or service you connect to may be several steps beyond the VPN server, and for that portion of the journey, your data is not protected unless you use SSL (discussed next).

The same phenomenon exists with encrypted email (see Encrypt Your Email, a bit later in the book) and most other online communication. The steps you can take to protect your privacy may be both powerful and effective within a certain scope, but once your data is in someone else's hands, your privacy depends on the recipient.

None of this should put you off using VPNs, which are quite effective at securing the most vulnerable part of your Internet connection; I'm only saying that VPNs alone can't guarantee end-to-end privacy.

I'll mention another, related option here: *proxy servers*. A proxy server, like a VPN, can disguise your physical location by routing your Internet connection through a device somewhere else in the world. Some proxy servers do additional tricks, such as filtering or

caching data. But proxy servers don't offer the encryption of VPNs, so although they might keep your identity private from the server on the other end, they are less likely to improve privacy in your immediate vicinity.

Use SSL If Possible

I'll come back to this in several later chapters, but I want to mention it here, too: whenever possible, use encrypted connections to the servers you visit. For Web sites, that means preferring sites that use HTTPS (discussed in Browse Securely); for email servers, that means using SSL/TLS (see Transfer Email Securely); for remote terminal sessions, it means using SSH instead of Telnet; for file transfer, it means using SFTP, FTPS, or WebDAV HTTPS instead of FTP (read Share Files Privately). All these types of communication offer end-to-end encryption between your device and the remote server, whether or not your Internet connection is encrypted (**Figure 6**). That limits your potential privacy exposure considerably.

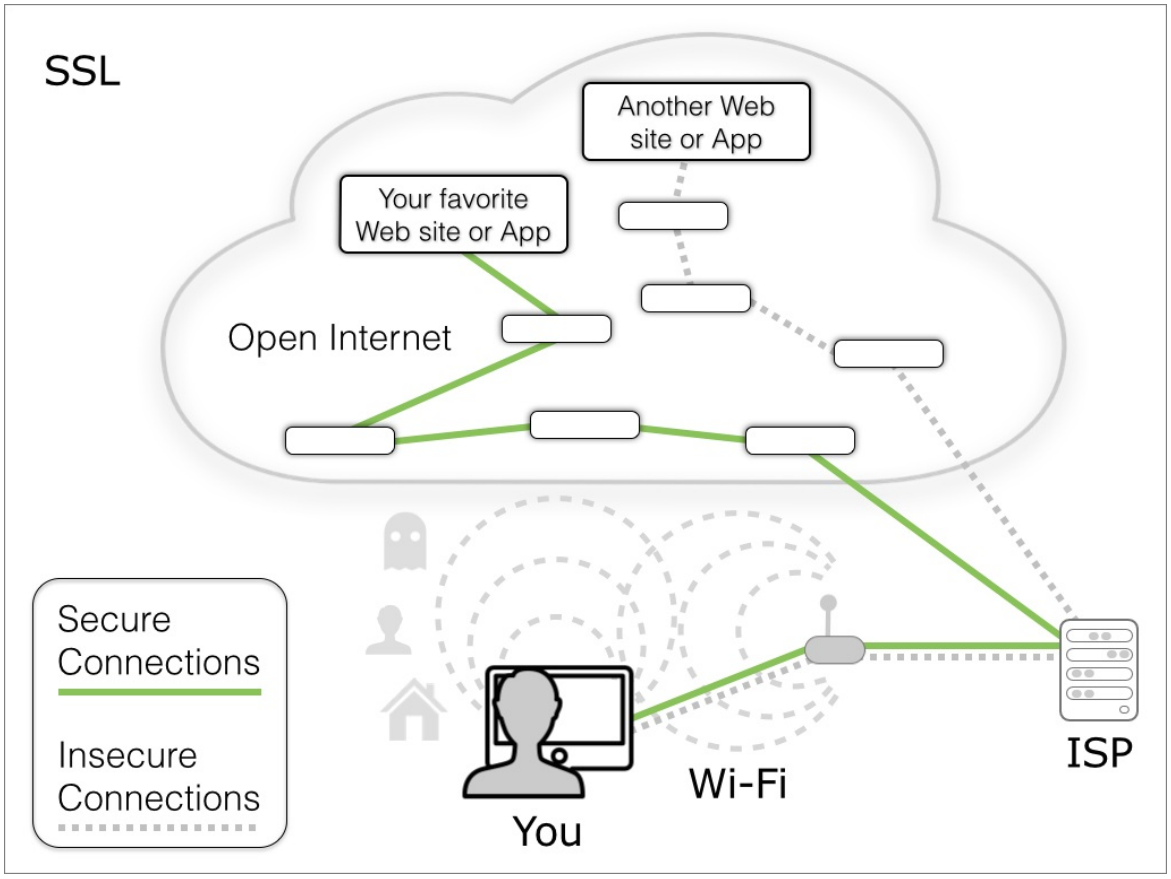


Figure 6: Using SSL encrypts an entire communications channel between your device and a particular remote computer. But other insecure connections may be active at the same time.

SSL Implementation Bugs

Although using SSL is much better than not using it, numerous bugs and vulnerabilities have been found in various SSL implementations over the years (and some may even have been planted deliberately to facilitate government surveillance).

To take a recent example, a bug in iOS 6 and 7, OS X 10.9 Mavericks, and Apple TV that affected SSL connections meant that under certain conditions, an interloper could eavesdrop on Internet data that should have been encrypted—including email passwords and message data, Web traffic, calendar syncing, and FaceTime calls. Apple fixed this bug in iOS 7.0.6, OS X 10.9.2, and Apple TV 6.0.2 in late February 2014. To learn more about this bug, read Dan Moren's Macworld article What you need to know about Apple's SSL bug.

Although this particular problem has apparently been solved, it's a cautionary tale: Don't rely entirely on any one type of security, because things can (and often do) go wrong.

Avoid DNS Mischief

I mentioned threats such as DNS hijacking and DNS spoofing that can lead you to a server that looks real but is only impersonating (inserverating?) the one you want to reach. How can you prevent this?

The best place to start is to *change your DNS provider*. Your ISP provides DNS services automatically, but you're free to connect to any DNS server you like. Some third-party DNS servers offer much better performance than your typical local ISP, and if you choose one with a good security reputation, you'll reduce the risk of DNS mischief too.

I've long been a fan of OpenDNS; Google Public DNS and Recursive DNS from UltraDNS are also good choices. All these services are free; you have merely to change the network settings on your computer or your router, and your DNS queries will be processed by the new server. (All three providers include detailed configuration instructions.)

OpenDNS goes a step further by offering a free download for Mac or Windows called DNScrypt. This app not only configures your computer to use the OpenDNS servers, it *encrypts* all your DNS requests, which prevents DNS spoofing and man-in-the-middle attacks.

Avoid Malware

Recent versions of Mac OS X and Windows are highly resistant to malware, especially if you keep up to date with all security updates and turn on the built-in firewalls. If you practice common sense—don't click links in email messages when you aren't absolutely certain of the message's authenticity, don't download pirated movies and suspicious software, stay away from sketchy Web sites, and so on—you have a reasonably good chance of avoiding viruses, worms, and other nasty programs that could compromise your privacy.

Installing third-party antivirus software, of which (as I'm sure you're aware) there are a gazillion choices, will improve your odds even more. However, I urge you not to put your entire trust in any anti-malware program. Even the best ones aren't perfect, and malware authors are always finding clever ways to defeat them. You still need to compute with both eyes open.

The vast majority of malware is designed to affect Windows, and thus you should use anti-malware software with Windows; however, a number of prominent security experts—including TidBITS Security Editor Rich Mogull—feel that anti-malware apps are currently unnecessary for most Mac users (see Rich's article Do You Need Mac Antivirus Software in 2013? for details). Having tested many Mac anti-malware apps myself, I tend to agree—Mac anti-malware software rarely identifies genuine threats while often imposing performance and usability penalties—but if you think it's a good idea for you, I won't try to talk you out of it.

Anti-malware is less crucial on mobile devices—and is irrelevant on iOS, as Apple implements security measures that reduce the risk of malware to near zero.

Turn Off Unnecessary Services

Your computer has a number of built-in features that enable other devices to connect to it over the Internet—file sharing, screen sharing, printer sharing, location services, Find My Mac, and so on (**Figure 7**). In most cases, these services are good and valuable, and if you actively use them, by all means, keep them turned on.

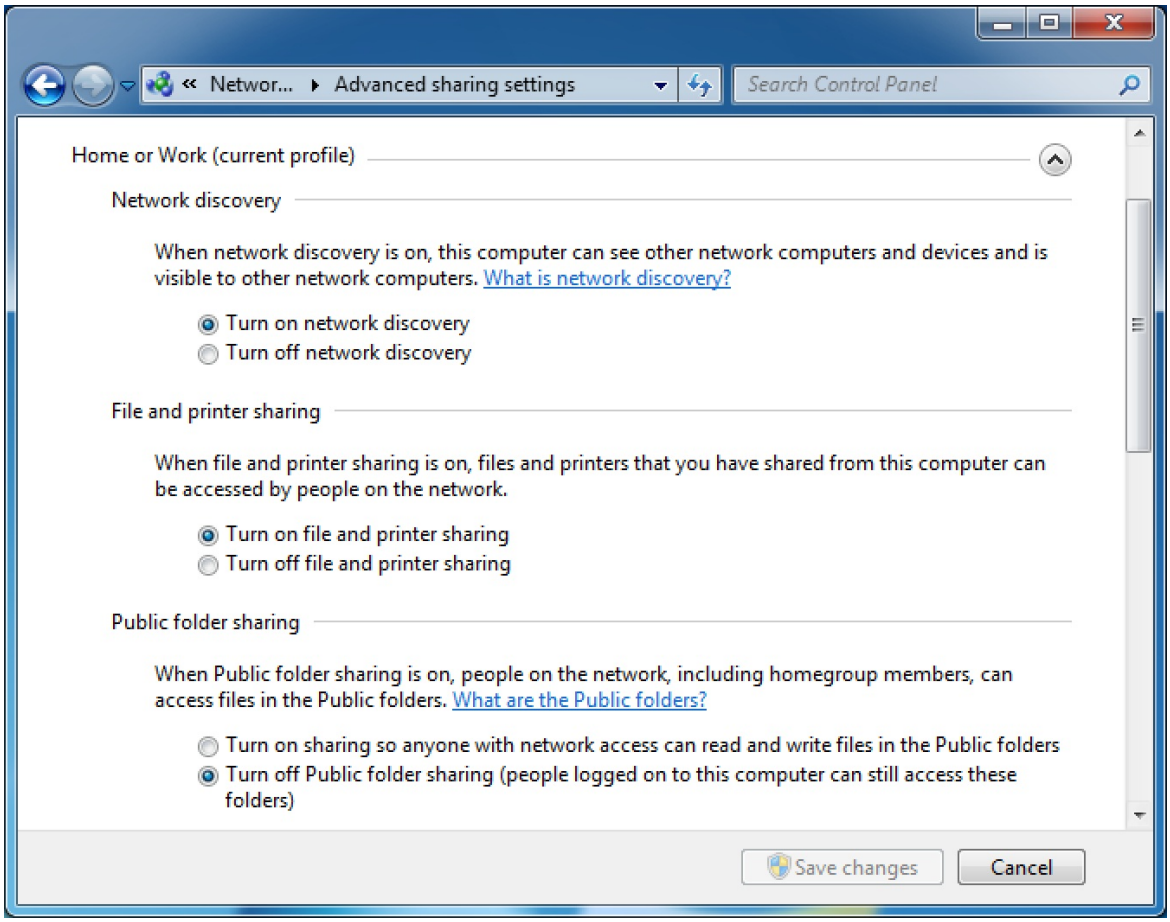


Figure 7: Windows lets you share files, printers, and other resources (as does Mac OS X). Turn off sharing services you don't actively use.

However, any service that lets other devices connect to your computer also represents a potential privacy concern (as well as a security concern). What if someone unknown to you guesses your password and connects to your computer without your permission? All sorts of damage could occur.

So, I'll simply give two pieces of advice:

- Turn off any sharing or location services you don't use. (And, if you use a service only rarely, consider leaving it off until it's needed.)
- Be sure your computer has an excellent login password. For advice on creating, remembering, and storing highly secure passwords, pick up a copy of my book *Take Control of Your Passwords*.

Set-top Boxes and the Like

Computers, smartphones, and tablets aren't the only devices that connect to the Internet. My television, Apple TV, TiVo, Blu-ray player, telephone, and home alarm system all have Internet connections too. So it's worth asking to what extent you need to worry about online privacy for those devices.

Such products can tell providers and advertisers a lot about your tastes and interests. For example, if you stream videos from Amazon or Netflix to your TV, the provider will know what you watch and at what time of day; from this, they can probably deduce facts like your age, gender, political persuasion, and whether there are any children in your home. Furthermore, your privacy controls are limited—you may not be able to configure settings or install extra software as you can on a computer or mobile device, and using a VPN is generally out of the question. (One exception is WiTopia's CloakBox, described previously under Prevent Snooping—it can provide a VPN connection to all your devices, albeit with a speed penalty. But video providers still know who you are and what you watch because you must log in, so you're not gaining much privacy that way.)

As privacy concerns go, I have trouble working up much anxiety about this one, and there's not much I could do about it anyway (other than to stop using these devices). But you should at least be aware of the sorts of data you may be giving away.

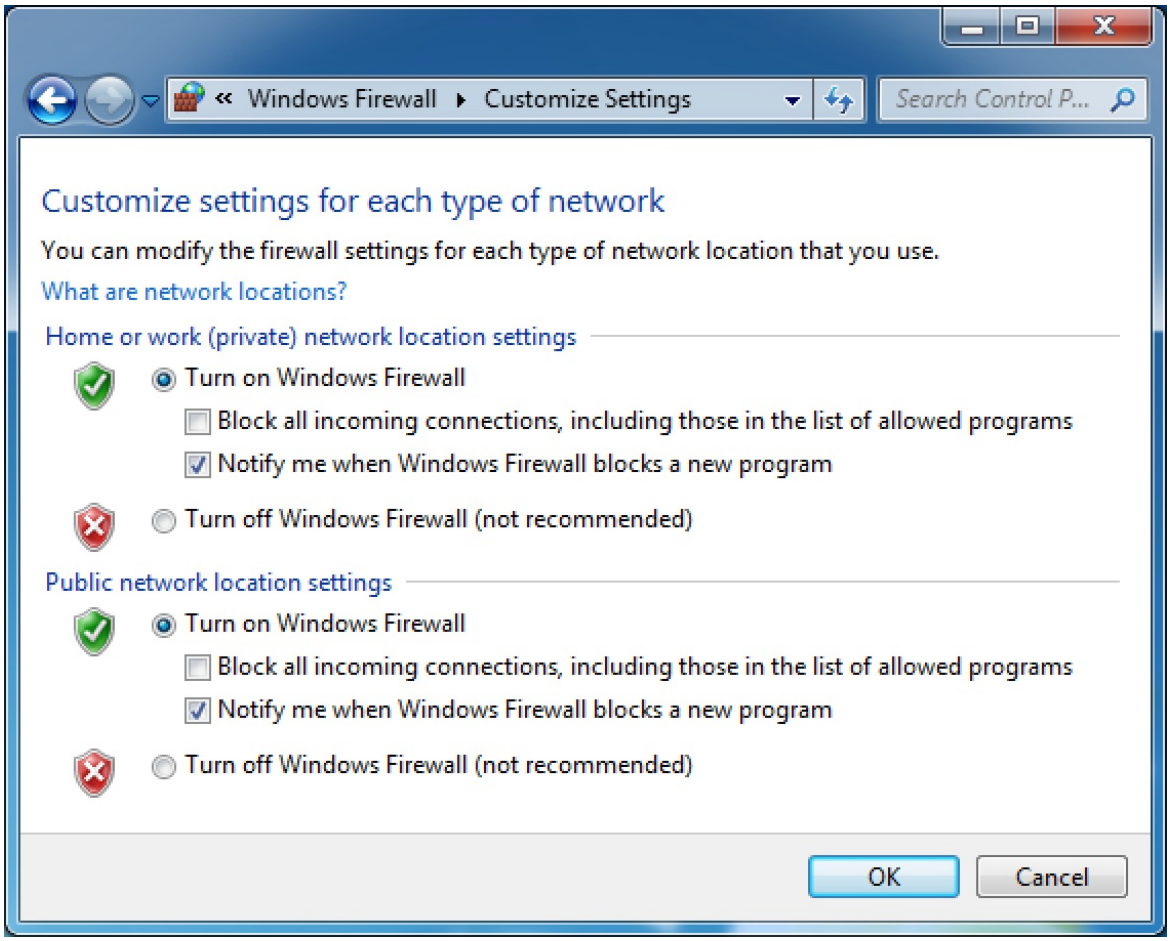
What about devices like thermostats, light bulbs, light switches, and door locks, all of which could be Internet-accessible? Other appliances—such as refrigerators, washers, and dryers—and home automation systems are also increasingly connected. (Everyday objects like these with Internet connections are often referred to collectively as "the Internet of things.") These are more concerning—what if hackers (or even advertisers) could use these objects to determine when you are and aren't home, for example, or even what room you're in? Time will tell what privacy choices may be available to users of such devices.

Use a Firewall

A *firewall* is a program that monitors all *inbound* Internet activity and selectively allows or blocks connections based on a series of rules applied to particular ports, protocols, or IP addresses. Firewalls are usually designed to protect your computer from malicious access over the Internet, although they can also censor data and perform a variety of less-helpful activities.

Mac OS X and Windows both include built-in firewalls; you can activate them with a couple of clicks, and then customize them later if you want to allow or block certain types of access. A firewall can only help you, so I suggest you check to see that yours is turned on right now (**Figure 8**). You can find instructions to do this in the Help menu or by using your favorite search engine. For the vast majority of users, sticking with the default settings is just fine.

Note: If your computer uses NAT (as is the case for most computers that connect to the Internet via a home broadband router), you already have a certain amount of protection against outside access, but it's not foolproof—and it doesn't hurt to use your computer's firewall too.



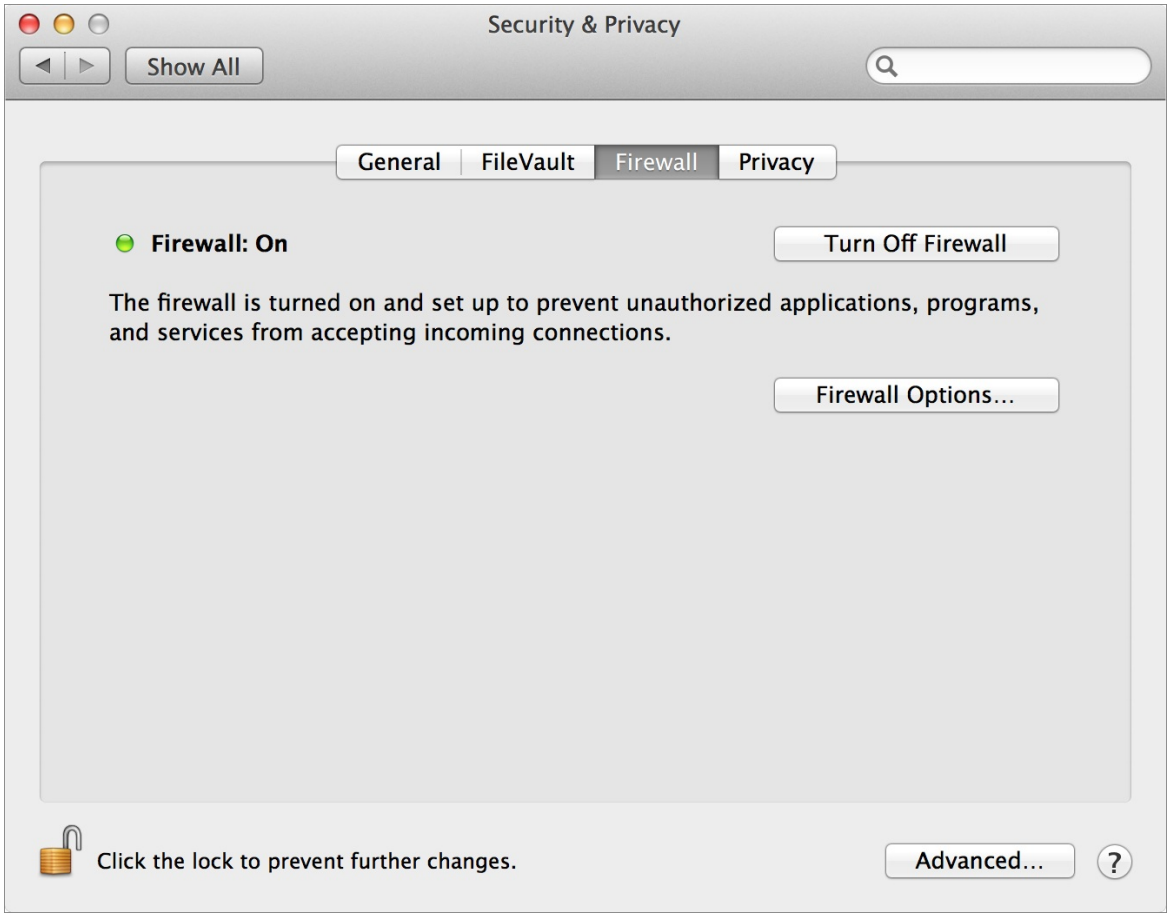


Figure 8: Built-in firewalls in Windows (top) and Mac OS X (bottom).

If for any reason you find your computer's built-in firewall inadequate, you can install any of numerous third-party firewalls instead or in addition. I'll leave that research to you.

Use an Outbound Firewall

I said a moment ago that a firewall monitors inbound Internet traffic, which is generally true. However, some firewalls monitor *outbound* traffic (instead of, or in addition to, incoming traffic). The main reason is to make you aware of—and enable you to block—software that might be sending out private information invisibly in the background.

Lots of software connects to the Internet without a visible interface, and it's nearly always perfectly legitimate. Your email program downloads your messages in the background, many apps check periodically for software updates, Dropbox syncs newly changed files, and so on. These activities are fine, but if you downloaded malware that secretly logs your keystrokes and tries to connect to a server somewhere to send them to an attacker, that's a problem. And, while some software "phones home" to validate licenses or send registration data, a few unscrupulous developers have been known to collect and send personally identifiable information without users' consent, and that's totally uncool.

I've tried a few outbound firewalls, and I'll be the first to admit that they're annoying—given default settings, they're constantly popping up alerts about outgoing connections, most of which are innocuous but all of which (thanks to the firewall!) now require attention. (To be fair, you can approve any outgoing connection so you're interrupted only the first time it appears—but I still find this happens often enough to be irritating.) But if you are worried about data being sent from your computer without your knowledge, you might want to give one a try.

On the Mac, the best-known outbound firewall is Little Snitch. On Windows, you might try ZoneAlarm or Windows 7 Firewall Control. (There are many other options on both platforms, too.) I can't say that you'll like using them, and for most people they're overkill, but they can in some cases be useful in protecting your privacy.

Beware Analog Snooping, Too

I frequent coffee shops that are full of people with laptops, sometimes seated quite close to other customers. I'd have little difficulty positioning myself such that I could watch over someone's shoulder as they type a password. An incautious person could also have private information stolen while entering a PIN at an ATM or retail counter, scanning a passport at the airport, using a smartphone on the bus, or even talking loudly on a mobile phone.

When it comes to online privacy, this sort of low-tech analog snooping is just as much of a threat as hackers hunched over keyboards in dark rooms far away. Be prudent when using your electronics in public—always keep an eye out for people keeping an eye on you!

Browse the Web Privately

In the previous chapter, I told you how to keep your connection to the Internet private. That can close quite a few holes that might put your privacy at risk—but even if you do all that, as soon as you open a Web browser, new risks emerge.

Simply browsing the Web reveals a great deal about you personally, your computer, your location, and your habits. There are many steps that you can take to reveal less about yourself, although some entail some loss of convenience. Never is this more the case than when shopping on the Web. This chapter explores the risks, the measures you can take to avoid them, and certain negative consequences of those measures.

Understand the Privacy Risks of Web Browsing

Assuming you've taken *all* the steps in Keep Your Internet Connection Private, browsing the Web privately comes down to two main things:

- Preventing information about your browsing activities from being stored on your own device (see On Your Device)
- Preventing the sites you visit (including search engines) from collecting information that can identify you personally (see On a Web Server)

(If you have *not* taken all the necessary steps to secure your Internet connection, there's a third factor to worry about—having information intercepted in transit on its way to or from a Web site you visit. We'll come back to that momentarily, in In Transit.)

Both of these categories are often misunderstood, and your actual risk may be greater or less than you imagine.

If information is stored on your computer, it's available to anyone who has physical or network access to your computer (assuming it's not protected in some other way, such as by using full-disk encryption or keeping it in a locked cabinet). To use the obvious example, your spouse or roommate might sneak a peak at the list of Web sites you've visited when you're not looking. But some of this stored information, including cookies, is *also* available to advertisers and other online entities as you browse the Web. One person may not care whether someone in his home or office sees what's on his computer, but may have a principled objection to advertisers knowing about his browsing habits. For another person, the opposite may be the case—advertisers might be irrelevant, but it would be problematic if a family member, coworker, or (let's just say) the FBI found out what sites she's visited.

Even if your computer is squeaky clean, every site you visit may record what pages you've read, what search terms you've entered, and much more (see On a Web Server, ahead). Unless you've logged in to a site with a username and password, it probably won't know who you are by name, but the other information the site logs could very well be enough to identify you uniquely, given sufficient effort and ingenuity.

Finally, information you send to, or receive from, a Web site could be intercepted in transit. If you use an encrypted Wi-Fi connection, you eliminate one avenue that could be used to eavesdrop on your Web surfing. If you activate a VPN, you eliminate another. And if you connect to a site that uses HTTPS (which I talk about ahead, in Browse Securely), you reduce the likelihood of in-transit eavesdropping to the point that most of us need not worry about it at all. In the absence of any of these protections, I'd be extremely hesitant to enter or view any sensitive personal information on the Web.

That's a long list of risks. But before freaking out about all the potential privacy risks of Web browsing, remember to ask yourself what data you're trying to keep private, and from whom. Do you care what someone could find physically on your computer? Do you care what advertisers know about you? Both? Neither?

If you're downloading stuff or doing things online that could lead to jail time, a lawsuit, a divorce, losing your job, or a combination thereof, you could always, you know, *not do that*. Regardless of what you do to protect your privacy, someone will probably find out and it will end badly for you. So seriously, *stop it*.

For what I'll call "lesser offenses," you'll want to be aware of, and take steps to avoid, certain types of data collection.

On Your Device

On your computer or mobile device, you should be aware that browsing the Web typically results in *at least* the following information being stored, for each browser you use:

- **Browsing history:** A list of every Web page you've visited, in each browser.
- **Download history:** A list of every file you've downloaded—again, in each browser.
- **Cookies:** Textual information stored on your device by the sites you visit, or by the companies who place ads or other code on those sites. Cookies (see Live Data, ahead) are most often simple settings or random-looking strings of characters that identify your browser uniquely, but they can also include your username, password, location, or any number of other details. Cookies can then be read when you revisit the same site—or other sites using the same ad network, analytics service, or social networking software.

- **Flash cookies:** Records similar to cookies that are stored outside your browser when you visit sites with Flash content, including movies. The same thing goes for sites using Microsoft's Silverlight plugin.
- **Web caches:** The contents of pages you've visited recently, especially images (so the page can load more quickly if you return to it) and *favicons* (the little icons that appear in your browser's address bar next to the URL). Some browsers also store thumbnail images of the pages you've visited.

The above is only a partial list. Some sites use even sneakier techniques to squirrel away various information about you in a variety of places (see Live Data, ahead, for further detail). In addition to all these things, your device may store a global cache of recent DNS lookups—that is, somewhere outside your browser there may be a list of the domain names you (or your apps) most recently visited along with their IP addresses. If you're sufficiently curious or motivated to want to remove this cache, you can search the Web for "delete DNS cache" to find the procedure for your operating system.

In Transit

The worry about Web transactions being observed in transit is that data such as passwords, credit card numbers, and other personally identifiable information could fall into the wrong hands. In fact, the sky's the limit—literally anything you type on a Web page or any content displayed on a Web page you view—could get out. Fortunately, this is the least likely privacy threat when it comes to browsing the Web and the easiest one to guard against (see Browse Securely, ahead, and also refer back to Keep Your Internet Connection Private).

On a Web Server

Modern Web servers can store an astonishing number of facts about every single page request, including (but not limited to) the following:

- **Time stamp:** The date and time of the request.
- **Time zone:** The reported time zone of the device making the request.
- **IP address:** The numeric address of the device you're using, which may or may not uniquely point to you, but which normally does reveal your approximate geographical location.
- **Item requested:** The URL and size of the page or other resource you loaded. If you visit a page that contains 20 graphics, they'll register as 20 separate requests.
- **Referrer:** The URL of the page on which you clicked a link to get to this page (if applicable).

- **Search terms:** If you reached this page from a search engine, the terms you searched for may be logged.
- **User agent:** The name and version of your browser. (Many browsers let you change this at will, so what the site records may only be what you *tell* it your browser is.)
- **Browser plugins:** The names and versions of all your browser plugins or extensions.
- **Operating system:** Your operating system's name and version.
- **System fonts:** All the fonts installed on your device.
- **Screen characteristics:** The dimensions (in pixels) of your screen, along with color depth.

Furthermore, the server may be able to tell how far down a page you scrolled, how long you spent looking at a page, which links to external sites you clicked on, and a good deal more.

Although none of these items has your name on it as such (again, assuming you haven't logged in with unique credentials), you can probably see how a combination of them might point to you uniquely. And if that isn't already obvious, I invite you to visit a site run by the Electronic Frontier Foundation (EFF) called Panopticlick. It examines much of the above data to create a "fingerprint" of the device you're using, and it tells you how unique that fingerprint is. I tested one of my Macs and found that only one in more than three million browsers has the same fingerprint as mine. That means an advertiser (or anyone else monitoring my Web activities) could be reasonably certain that I was the person who requested any given Web page.

Go to the Right Site

One of the most surprising privacy threats on the Web is impostor sites that look almost exactly like the real thing, but are merely clever copies designed to trick you into supplying your password, credit card number, or other private data. Sometimes these sites appear if you make a slight typing error when entering a URL or if your DNS settings have been compromised, but they're most commonly reached by clicking a link in a phishing email message. (These messages often warn you that you must "update" or "confirm" your account settings or suffer dire consequences.)

Here are some tips to avoid bogus sites:

- If you haven't already done so, follow the advice in Avoid DNS Mischief in last chapter to avoid most DNS exploits.
- Don't click links in email messages. If you get a message that appears to be from your

bank, PayPal, Amazon.com, Apple, or whoever insisting that you log in to correct some problem and you're worried that it might be a legitimate message, open your Web browser and *manually* type the site's address. Then log in and see if there are any messages waiting for you. If not, the message is almost certainly fake.

- Check the site's certificate. Real banking, commerce, and similar sites nearly always use HTTPS (see Browse Securely, next), and you can usually click a lock icon in your browser's address bar to verify the site's SSL certificate. If there's no certificate, if you see a certificate warning, or if the site doesn't even use HTTPS, you may be dealing with an impostor.
- Let technology help. Most browsers have built-in checks to warn you of sites that might be bogus (see Browser Privacy Settings), as do some third-party plugins (see Web Privacy Software). Be sure to enable these features. In addition, most password managers (see Protect Passwords and Credit Card Info) confirm each site's identity before entering your credentials.

Browse Securely

Security and privacy are two different things (see the sidebar Privacy vs. Security vs. Anonymity), but sometimes security provides privacy as a side-effect. That's certainly the case with Web browsing: if you can ensure that the connection between your browser and the server is securely encrypted, you can also be confident that no one in between can violate your privacy by reading what you send or receive.

The standard way for a Web site to do this is to use *HTTPS,* a secure version of the HTTP protocol. A site must install an SSL certificate, which confirms its identity and enables two-way encryption; your browser can independently verify that the certificate is valid and that it's being used by the correct site. 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 (usually in green, along 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.

Increasingly, sites that transmit or receive any 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 and misused. 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 EFF offers a free browser extension for Chrome and Firefox called HTTPSEverywhere (sorry, no Safari or Internet Explorer versions available). This extension maintains 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.

You won't be at all surprised, I'm sure, to learn that HTTPS, for all its virtues, is not foolproof. I've read of numerous hacks and exploits that could enable an attacker to intercept and decrypt a secure Web session. (Refer back to the sidebar SSL Implementation Bugs for an example.) However, these are rare, and are generally fixed in short order. So, your best defense is to make sure you keep your operating system and browsers (including any security updates) current.

Manage Local Storage of Private Data

In On Your Device, I mentioned several types of (potentially) private data that may be stored on your device as you browse or use Internet-enabled applications. Here, I want to provide a bit more detail about this data and tell you what you can do about it.

It may be helpful to conceptually divide the stored data into two categories: *live data*—that is, information that may be sent from your browser to the sites you visit in real time—and *historical data*, which is accumulated on your device but not transmitted. Both types of data are normally stored separately for each browser you use, on each device.

Live Data

When you visit a site and it sets a cookie, that by itself is generally harmless; it's just a bit of text stored on your device. When you visit the same site later, it will read that cookie before displaying the page. Cookies are often helpful because they enable sites to save preferences for you, keep track of your login information so you need not enter your credentials each time you visit, and offer continuity (such as remembering which articles you have read) on successive visits.

Cookies have become a privacy problem because they're often used for tracking you *across sites*. An ad, social networking widget, or analytics code on one site creates an identifier on your device that it can use to look up what you did there. If the next site you visit happens to use an ad, widget, or code from the same network, it can read the cookie to see what you've done in the past, and add information about your current visit. This process continues indefinitely, such that you may randomly visit a site for the first time and instantly see ads that are mysteriously targeted to your interests and location, including items you've searched for recently on Amazon.com, Google, or other sites.

In these cases, it's not the site you're visiting that's setting and reading tracking cookies, but a third-party site or network that has placed code on the page to track you. That's why you'll see these types of cookies referred to as *third-party cookies*. A site may use its own cookies (first-party cookies) for useful purposes such as saving your preferences but permit third parties to use cookies for tracking and other less-noble reasons. Some popular news sites have *hundreds* of tracking cookies, which pose a privacy risk and cause pages to load much more slowly (and help chew through your data cap). (Browsers don't normally go out of their way to tell you what cookies a given page has set, but see Web Privacy Software, ahead, to learn one way to keep track of them.)

Browser cookies aren't the only sort of live data that your device may store and send to sites as you browse. When you use media plugins such as Flash and Silverlight, they may also collect, store, and transmit data in much the same way as conventional cookies—but they do so separately from your browser, which means disabling cookies in your browser may have no effect on this data. Numerous other plugins and extensions can also do this sort of thing, but, without a doubt, Flash cookies are the most common.

Even if you block or delete cookies of all sorts, you may not be in the clear. Some especially aggressive trackers use a variety of techniques (sometimes known as evercookies or zombie cookies) to *respawn* cookies you've deleted or to track you using other methods involving your image cache, JavaScript, and/or HTML5 Web storage.

What's HTML5 Web storage, you ask? It's another way a Web page or application can store data in your browser and access it later. It was designed to be not only faster and more secure than cookies, but also to hold larger quantities of data. And in principle there's nothing wrong with it—HTML5 Web storage can do neat things like cache webmail or map images so you can read them offline. But it's still an imperfect system that can be used for undesirable purposes.

Historical Data

Cookies normally stick around on your device for quite some time, so in addition to sending live data about you as you browse the Web, they serve as historical evidence of the sites you've visited and some of the activities you've performed there.

Your browser may also store lists of pages you've visited (browsing history), files you've downloaded (download history), searches you've performed (search history), and information you've entered into form fields. Barring a bug or malicious exploit, your browser doesn't transmit any of this data, but someone could examine your device after the fact and get a detailed record of where you've been.

As I said earlier, live data and historical data have entirely different privacy implications. You may find live tracking to be creepy and offensive but have no qualms about someone examining the browsing history on your computer; or you may have no issues with advertisers knowing what you're up to but prefer to keep that information from, say, your employer (who might take a look at your computer when you're not at your desk—or even use monitoring software).

Avoid or Remove Local Data

Broadly speaking, you can manage local data storage in either of two ways:

- Prevent data from being stored on your device in the first place—using browser settings, a private browsing mode, or third-party plugins/extensions.
- Erase stored data after the fact—either manually or using an automated tool.

You can use a number of methods for either approach, as I describe in a moment. But which way is best?

I think most people would agree it's preferable to avoid getting sick than to cure an illness. By preventing data from being stored locally in the first place, you eliminate both the threat of live tracking and the potential for historical examination. Furthermore, clearing cookies and other local data after the fact may prevent you from being tracked from one session to the next, but not during a single session.

However, depending on your browser, operating system, and device, you may be unable to prevent data from being stored—or at least not with the granularity you prefer. For example, if a browser's only option is to block *all* cookies, that may make your Web browsing experience worse because it prevents the use of helpful, first-party cookies.

So, what are your options for managing local data?

Private Browsing Modes

Safari and Firefox have Private Browsing (in Safari, choose Safari > Private Browsing; in Firefox, choose File > New Private Window). Google Chrome has Incognito windows (choose File > New Incognito Window; see **Figure 9**). Internet Explorer has InPrivate (click the gear icon and then choose Safety > InPrivate Browsing). Most other browsers have something similar. While you're in one of these modes, your browser typically avoids storing data such as cookies; browsing, download, and search histories; form/autofill data; and page or image caches. Because the data isn't stored at all, it eliminates both tracking and after-the-fact analysis.

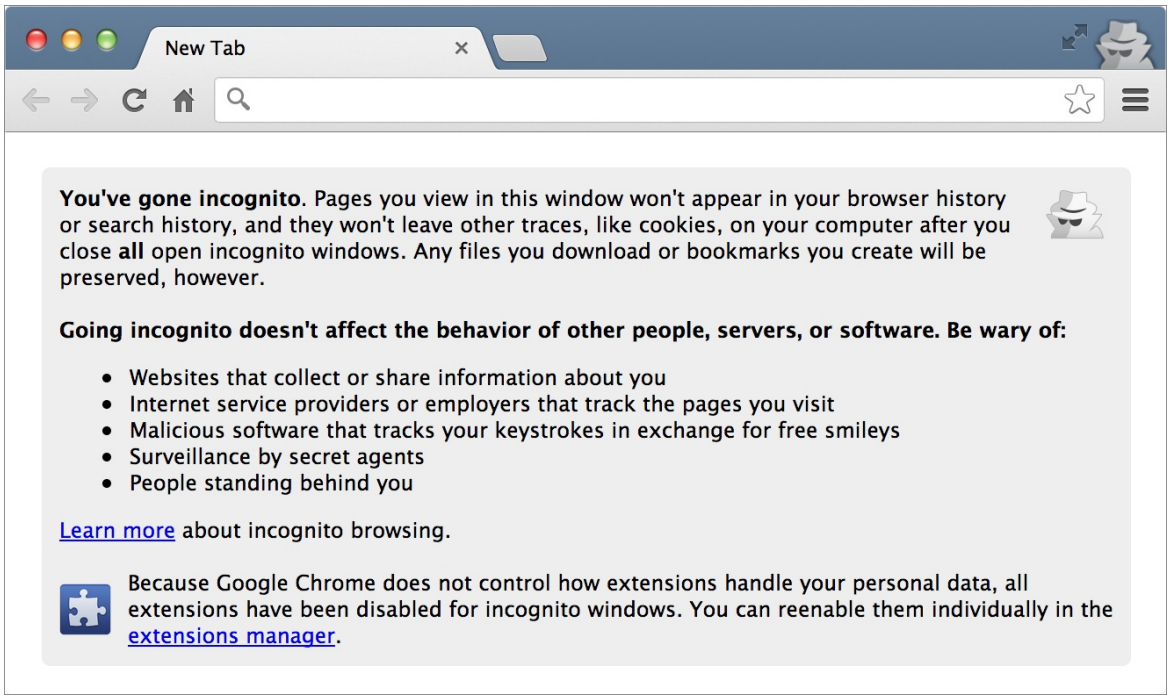


Figure 9: Chrome's Incognito window spells out what information it protects, as well as what possible privacy risks remain.

Note: Private browsing modes are somewhat less common (or at least harder to find) in mobile browsers, but options are improving. For example, in the iOS 7 version of Safari, open a new page and tap Private at the bottom. In the iOS version of Google Chrome, tap the Chrome menu ☰ button and tap New Incognito Tab. (See Browse Anonymously, ahead, for other mobile private browsing options.)

Private browsing modes are great for people who only occasionally—for specific sites or tasks—want to remain private. Turn them on when you need them; turn them off when you don't. That way, the bulk of your Web browsing still has the benefits of first-party cookies, histories, and so forth, but you keep the private things private.

However, please keep the following in mind about private browsing:

- Plugins and extensions—including Flash—could still store data locally if they remain enabled, and there's no guarantee that an unscrupulous tracker hasn't invented some other sneaky trick to store data even when browsing privately. *Browser beware.*
- If you download a file, that file may not appear in your download history, but it'll still be on your disk.
- Private browsing doesn't stop you from *manually* bookmarking pages.
- Although your browser doesn't store search terms while browsing privately, the search engine might (see Search Privately).
- DNS queries, which happen outside your browser, could still be cached on your device.
- Someone sniffing your Internet connection may still be able to see what sites you connect

to, and server logs will still be kept.

Browser Privacy Settings

Whereas private browsing modes are temporary, you can usually fine-tune a browser's preferences to specify permanent settings for which sorts of data should be stored locally (**Figure 10**). You can usually also examine or delete data already stored.

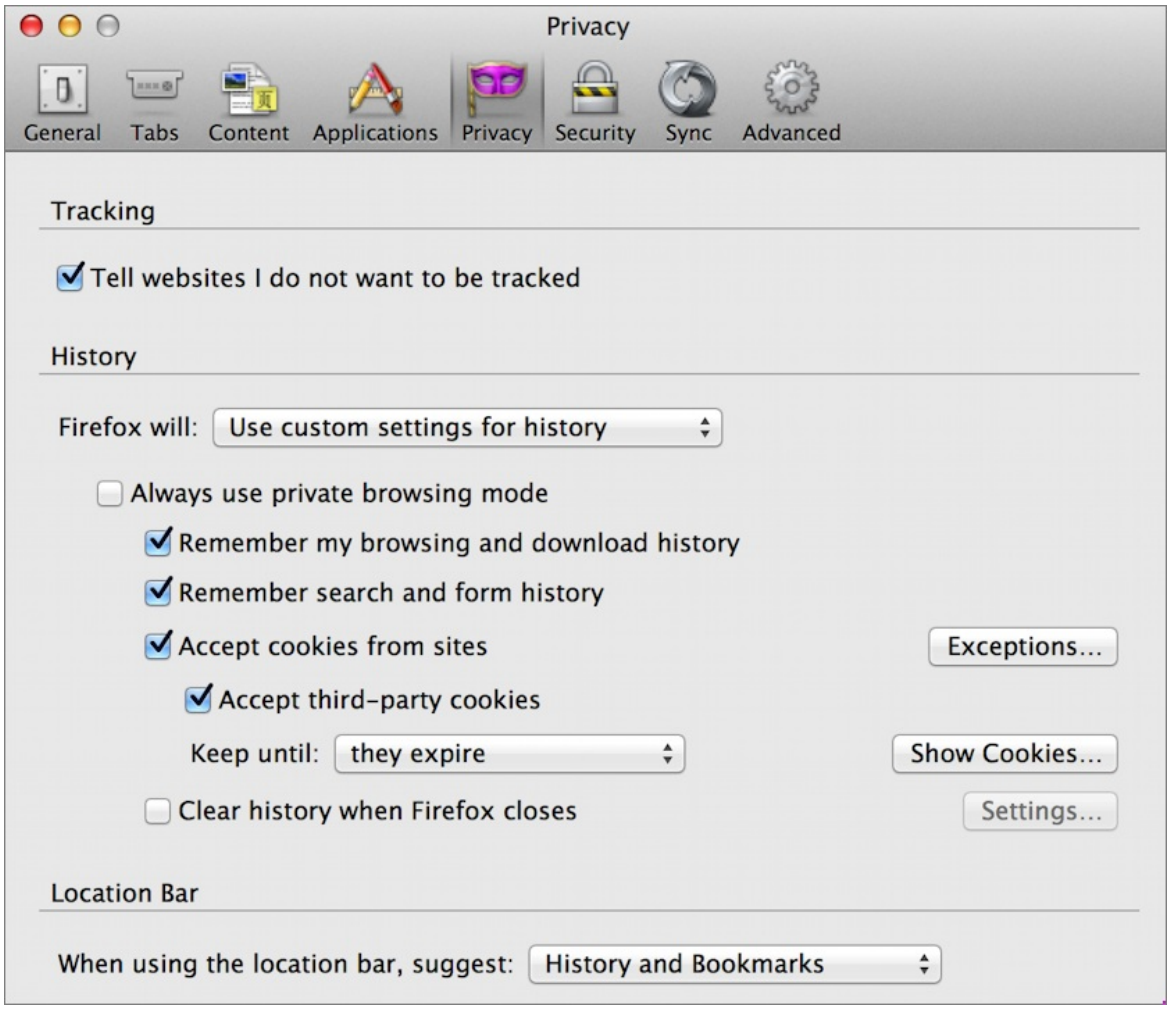


Figure 10: Firefox offers a variety of privacy settings; most other browsers have a similar range of options.

Once again, the range of choices varies by browser and platform, and I can't cover every detail here. I will say, however, that you can usually make at least the following choices:

- **Cookies:** Block all cookies; accept all cookies; or (my recommendation) block only third-party cookies. You can also usually view all the stored cookies and delete any of them individually, or all of them en masse.
- **Do Not Track:** Your browser can ask sites not to track you, and I suggest you enable this feature—but sites may ignore the request. (See the sidebar Do Not Track, ahead.)
- **Phishing and malware protection:** Alert you to sites that may be fraudulent (especially phishing sites) and those suspected of containing malware. By all means, turn

this on.

- **Location tracking:** Your browser may report your location in order to provide you with more useful results (for example, local weather, movie times, and stores) without your having to manually specify where you are. I generally find location tracking helpful, and I figure I'm already giving away my location by my IP address when not using Tor (see Browse Anonymously, ahead) or a VPN, so this isn't much worse—although, to be fair, location data derived from Wi-Fi triangulation and GPS can be much more precise than what your IP address alone indicates. You can usually enable or disable location tracking on a per-site basis or globally, as you prefer.
- **Search suggestions and history:** When you start typing a search term, your browser may try to fill in the rest for you as a convenience feature. To do so, it may use a locally-stored list of your previous searches, but it's probably also telling the search engine what you've typed so far (each and every keystroke!) and ask for a list of matches. This is usually beneficial, but can sometimes reveal more about you than your search terms alone. If you don't want your browser storing your search terms or search engines trying to pre-guess what you want, turn these features off.

Here's how to access privacy settings in a few popular desktop browsers:

- **Firefox:** Choose Firefox > Preferences and click Privacy (choose Use Custom Settings for History from the pop-up menu in the History section for additional options). Some privacy-related settings are also found on the Security pane.
- **Google Chrome:** Enter `chrome:settings` into the address bar. Then click the "Show advanced settings" link and look under Privacy. (Note that you must click Content Settings and Clear Browsing Data to access some of the settings.)
- **Internet Explorer:** Open the Internet Options control panel and look on the Privacy tab. You'll need to click Sites and Advanced to see certain important settings.
- **Safari:** Choose Safari > Preferences and click Privacy. Also click Security for some additional privacy-related settings.

Do Not Track

Most modern browsers can (at your option) transmit a special Do Not Track header when they load a Web page that asks the site to pretty please not track your visit. And, by all means, you should turn this feature on because some sites will heed your request, and even those that don't should know that you prefer it that way.

Unfortunately, Do Not Track is at this point merely a request. Advertisers, analytics companies, and social networks are free to ignore it, and often do. A movement is afoot to make Do Not Track more than a request—to enforce it technologically and also enact legislation that would punish sites that track users in violation of their requests. I'm not optimistic that either will happen, but I've been surprised before.

Web Privacy Software

Besides using private browsing modes and fiddling with browser settings, you can also install software that purports to enhance your Web privacy. I say "purports" because programs of this sort vary widely in their capabilities. Some are excellent, while others promise more than they can deliver, and some offer little that you couldn't achieve simply by clicking a few buttons in your browser.

I couldn't begin to review the full range of options. A Google search on "privacy software" turned up nearly three *billion* hits. So, I'll just give a couple of examples.

One tool I'm quite fond of is Adblock Plus, a free extension available for Google Chrome, Firefox, Opera, and Android. (Although Adblock Plus isn't available for Safari, there is a shareware extension from a different developer called AdBlock for Safari that has many of the same capabilities.) Adblock Plus is highly customizable, letting you selectively or globally block ads, tracking cookies, and social media buttons (which let you tweet, like, or otherwise spread the word about a page—and track you in the process) without interfering with normal browsing and local storage the way private browsing modes do. It also offers protection against domains that could infect your computer with malware.

Another fantastic free tool is called Ghostery—available as a cross-platform browser extension for Firefox, Google Chrome, Internet Explorer, Opera, and Safari; and as a stand-alone iOS Web browser. It displays a list of all the trackers of various sorts—both honorable and ignoble—present on any given Web page (**Figure 11**) and lets you enable or disable them (individually or by category). It's highly educational as well as effective in increasing your privacy.

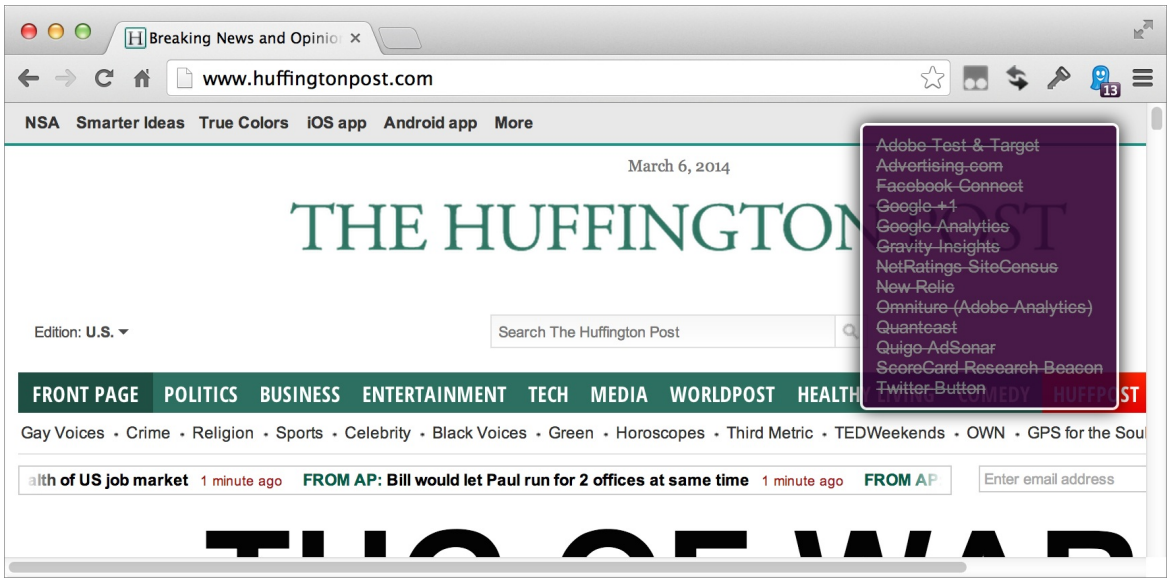


Figure 11: Ghostery briefly displays a pop-up showing which trackers it's blocking when you load a site; you can individually enable or disable them as you like.

Then there are apps that strike me as a waste of money, such as SecureMac's PrivacyScan for Mac and Symantec's PC Tools Privacy Guardian for Windows (PC Tools Privacy Guardian was recently discontinued, but I've mentioned it because you may see it reviewed or already have a copy).

Both of these apps merely delete locally stored browser data (including browsing histories, conventional and Flash cookies, and so on) after the fact. To be fair, they can do this for multiple browsers at once, identify local data that your browser may be unaware of, and securely overwrite the data to prevent it from being undeleted. But it's certainly possible to do all this manually, without any extra software. And in my opinion, such software misleads users by portraying "privacy" as merely preventing someone from seeing what's on your computer. It does nothing to protect private information in transit, avoid the collection of tracking data as you browse, or disguise your identity in servers' logs.

My overall recommendation about privacy software is to read the fine print. If a piece of software claims to solve all your privacy problems, take that claim with a grain of salt. Look into the details to see what it truly does, and whether that's something you can't achieve in a simpler way. And remember: prevention is nearly always preferable to cleanup.

Protect Passwords and Credit Card Info

Your passwords and credit card information are certainly among the items you'll most want to keep private, but you can't do very much on the Internet without entering a password, and most online shopping requires entering a credit card number. So you can't realistically avoid ever sending these things over the Internet, but you can take steps to keep them private:

- **Use a password manager.** You may be familiar with password managers—apps such as 1Password, Dashlane, and LastPass that can generate, securely store, and enter passwords for you (see **Figure 12**). Users of Apple devices running OS X 10.9 Mavericks and/or iOS 7 can use a built-in password manager called iCloud Keychain (see the sidebar Security in iMessage and Other Apple Services).

  You can also use password managers for credit card numbers, secure notes, and other private data. In addition to their obvious benefits, these apps can verify that you're on the right site before handing over your password—yet another way to avoid phishing and DNS spoofing attacks.

Note: Most browsers have built-in password-filling tools, but they tend to be both less capable and less secure than full-blown password managers.

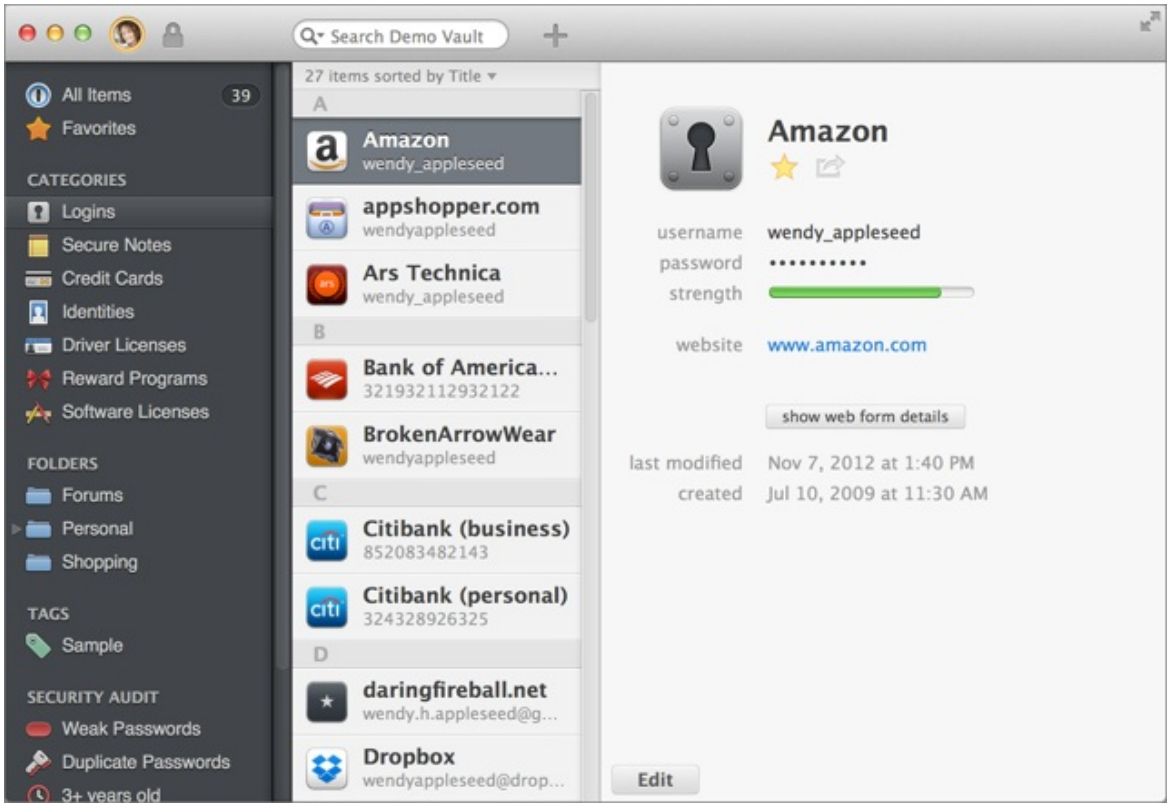


Figure 12: 1Password (Mac version shown here) securely stores passwords, credit card numbers, and other personal data, and syncs them among your devices.

I discuss password managers and other password strategies further in my book *Take Control of Your Passwords*. (And, if you decide to use 1Password as your password manager, I have a book all about that too: *Take Control of 1Password*.)

- **Check for HTTPS.** As you saw in Browse Securely, an encrypted Web session makes it much safer to send private data, and an unencrypted session is asking for trouble. So look for that lock icon before filling in any Web form containing private information.

Just ahead, in Shop Online Privately, I discuss further issues involving online commerce.

Search Privately

You know already how you can use a private browsing mode (or change your browser settings) to avoid having your search terms stored on your device. But the search engine could keep a record that someone at such-and-such an IP address performed a certain search at a certain time and date. Furthermore, if you're logged in to the search site—for example, you're logged in to your Gmail account while you do a Google search in the same browser—the site will store those search terms in your account and it knows exactly who you are, by name. Later, you may use the same search engine on an entirely different device and see those earlier terms pop up again! That could be either helpful or disconcerting.

Google does let you temporarily or permanently Turn off your Google Web History, and most other search providers do too. But you might forget, or might not have done the right things in every browser or on every device.

If you want to use a pretty good search engine that won't log your results, period, try DuckDuckGo. All searches are completely anonymous. Nothing is logged, no tracking occurs...and there are no ads. And although the results aren't always as thorough as with Google or Bing, DuckDuckGo is getting better all the time.

Browse Anonymously

So far I've talked only about *private* Web browsing, but sometimes you may need greater assurances that your Web activities are *anonymous*, meaning they aren't associated with you individually.

Note: You should never assume that anonymity on the Internet is absolute or permanent. Anonymity means making it extremely difficult to discover your identity—and although that's often good enough, anonymous statements and activities can sometimes be traced back to the person who originated them.

I said in the Introduction that this is a book about ordinary privacy for ordinary people. And frankly, the picture I'm about to paint is far from ordinary. This is something a political dissident or a journalist in a highly secretive country might need to worry about, not a day-to-day privacy concern for regular folk. Still, it's worth knowing about.

Imagine that your local Internet connection is encrypted using a VPN, which also hides your real IP address. Then you use your browser's private browsing mode to eliminate all local data storage, and connect to a Web server using HTTPS, so the entire transaction is encrypted. That's about as private as you can get—it's extremely unlikely that any party

between your device and the Web server will be able to see your information, and similarly unlikely that anyone who examines your device later on will be able to discover evidence of the session either.

However, don't forget that the server still logs your visit. Server logs may provide enough other information (see On a Web Server to learn about browser fingerprints) to uniquely identify your computer. Furthermore, even though the server doesn't know your real IP address, your VPN provider does, and it may have kept a log of your session that could be traced back to you. Finally, even though an encrypted connection protects the contents of the transmitted data, it doesn't protect low-level routing information, which indicates the data's origin and destination. (They can't: intervening routers and switches need that information to pass your data along.) So, by combining all that information, someone could still discover that you were the person who visited a certain page at a certain time. For certain types of Web activity, that could put you in deep trouble.

If you need of near-complete anonymity when browsing the Web (including using webmail), you should be aware of something called Tor. Tor, which originally stood for "The Onion Router," is a system that not only encrypts data but also does so multiple times, sending it through a series of randomly selected relays called nodes (see **Figure 13**)—each of which knows only about the previous and next node in the chain, but not the information's origin (unless it happens to be the "entry" node) or destination (unless it's the "exit" node). This process makes it extremely difficult to determine the source of any Web transaction. In addition, a component called Torbutton offers a fair degree of protection against browser fingerprinting.

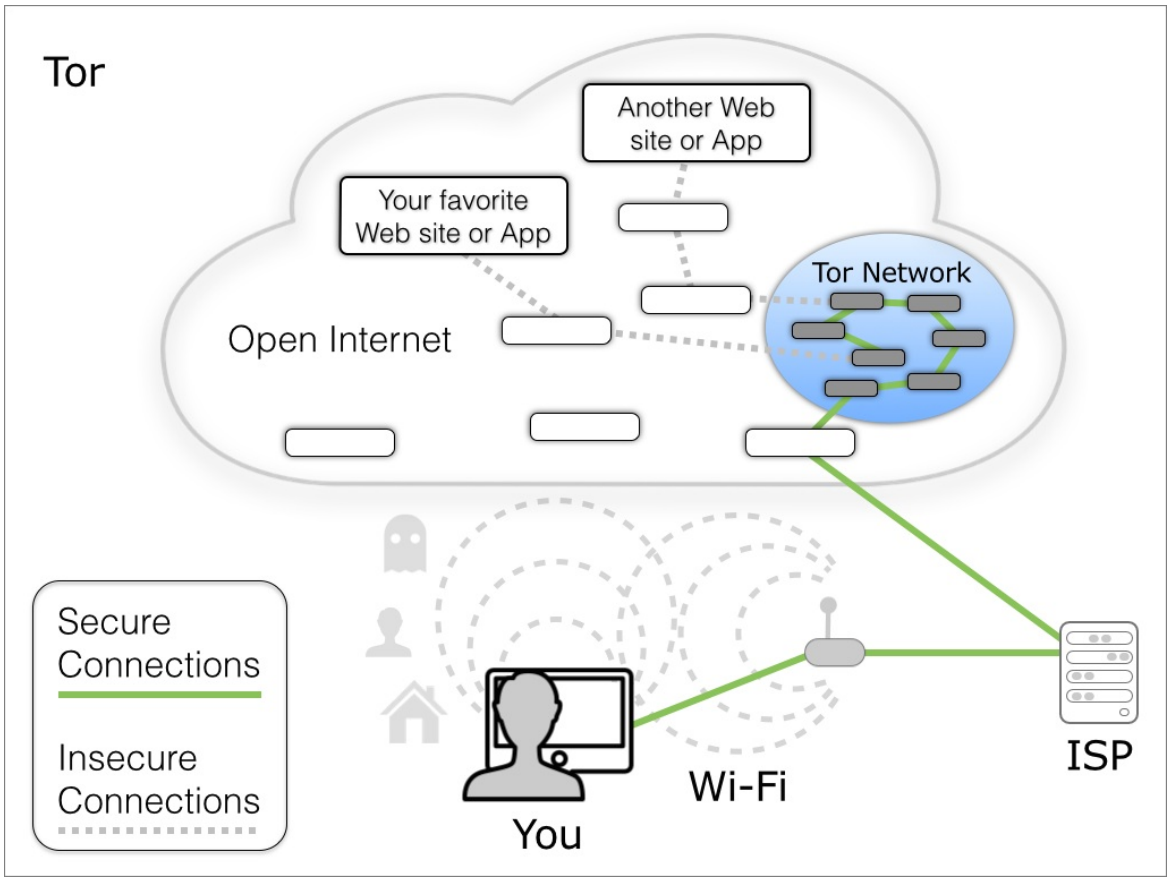


Figure 13: When you use Tor, your connection to any server goes through a random series of nodes, each one adding a layer of encryption and further obscuring the sources of requests.

To use Tor on a Mac or Windows PC, you download software called Tor Bundle, which includes a customized version of Firefox and several other components, all with extremely strong privacy settings enabled by default (**Figure 14**). Full instructions for installation and use are on the Tor site. For Android, you'll want Tor's Orbot package; for iOS, you can use the third-party Onion Browser.

Figure 14: The Tor browser (left) along with Vidalia, another app in the Tor Bundle whose job is to establish anonymous connections.

Tor can dramatically increase the chances that your Web activities will be anonymous, but it's not without its drawbacks. For example:

- Several weaknesses in the Tor system have been discovered that could be exploited under the right conditions to reveal private data. For example, someone who runs a Tor exit node could monitor unencrypted traffic flowing between it and the rest of the Internet—and indeed, it's widely believed that the FBI runs a large number of Tor exit nodes to do just that. Using end-to-end encryption such as SSL/TLS reduces the risk of eavesdropping significantly, even if the exit node is compromised.
- Someone monitoring your Internet connection can tell that you're using Tor, even though they can't necessarily tell what you're doing with it. Some ISPs and countries block all known Tor traffic. There are ways to work around this problem in some instances, but they make the process of Web browsing that much more cumbersome.
- Merely using Tor could result in unwanted attention from the NSA, including having your encrypted communications retained indefinitely.
- Using Tor makes Web browsing *slow*. No, I mean *really* slow. And forget watching videos, anyway—Flash, QuickTime, and other plugins are blocked because they pose too much of a security risk.

Privacy is hard. Anonymity is *extremely* hard.

Shop Online Privately

I've already talked about steps you can take to protect the privacy of your Web connection and your credit card information. As long as you're using an encrypted connection, any purchase you make online should be strictly between you and the vendor. Well, you and the vendor and the vendor's payment processor and your bank. And perhaps the fulfillment or shipping company. I can't tell you how to shop *anonymously* online, but most online purchases from reputable companies are already as private as they can be.

One common source of anxiety is giving out your physical address. If you're purchasing physical goods online, you have to provide a mailing address. Even if you're buying digital goods with a credit or debit card, you'll still be asked for your billing address (which helps to prevent credit card fraud—a good thing!). Other than renting a private mailbox, there's not much to be done about that. You may not have to provide your *home* address, but you will have to provide *some* valid address at which you can receive statements. As long as you can do so over a secure connection, that shouldn't be anything to worry about.

Another concern is the security of one's credit or debit card number, even over an encrypted connection. What might happen to it once it's in the vendor's hands? Is it safe?

I can't work up much fear about this, because laws and bank policies protect consumers against fraudulent use of a credit or debit card—or at least limit liability, as long as you report

any suspicious transactions promptly. So, keep an eye on your bank statements online and call your bank immediately if anything appears amiss.

If that's not good enough for you, I can offer a few other suggestions:

- When an online vendor asks to store your credit card to simplify future purchases, say no. If you're using a password manager to enter credit card details, it's only a matter of a few clicks anyway. However, even if you follow this policy generally, you might consider making exceptions for sites you shop from frequently, especially those with one-click checkout systems like Amazon and Apple. (It's rare for a week to go by without my purchasing something—an app, album, ebook, or some other digital media—from one of these vendors, and I have become extremely fond of one-click shopping convenience.)
- Use PayPal if that's an option. Now, I know a lot of people dislike PayPal for one reason or another, but one significant advantage is that it prevents vendors from seeing your credit card number (and, except for goods that must be shipped, your mailing address). Yes, you're trusting PayPal with a credit card or bank account number, but at least that limits your exposure.
- See if your bank offers single-use credit card numbers for online purchases. Mine doesn't, but many do, and if you want to be sure a credit card number isn't misused after a single purchase, that could be an option.

Many other online payment systems exist—some of which go to greater lengths to protect your privacy. The best known is Bitcoin (which is accepted at an increasing number of online and brick-and-mortar businesses), but numerous other cryptocurrencies have sprung up. Feel free to experiment with these if you're willing to accept some financial uncertainty. At this point, the entire field is too unpredictable for me to make any specific recommendations.

Improve Email Privacy

When we began discussing this book, Take Control publisher Adam Engst told me that his rule is, "don't write anything in email that you couldn't stomach appearing on the front page of the *New York Times*." I said I didn't think that was a very good rule, and we discussed it (by email, naturally) in what became an increasingly contentious debate. I won't repeat the entire exchange here, because I'm sure you'll read it soon enough in the *New York Times*.

But to summarize, Adam was trying to make the point that you can never have an ironclad guarantee of privacy when it comes to email. In that respect he's absolutely right, for reasons I'll explain in a moment. My point was that in many cases, email is the only practical means of communication, and yet it's completely impractical for me to avoid ever sending personal facts, business secrets, colorful language, or anything else by email that wouldn't cause serious problems if made public. I think I'm right about that, too.

But email privacy is extraordinarily difficult to achieve, and the more control you try to exert, the more cumbersome it becomes. By the end of this chapter, you should have a better appreciation of what makes email privacy so tricky. But you'll also learn how to keep most email safe from casual snooping, how to make top-secret email messages as private as they reasonably can be, and when it's best to choose an entirely different means of communication.

Understand the Privacy Risks of Email

If you send me an email message, you might have the impression that you and I are the only two people who can read it. Such assumptions are unwise. Let's look at a few of the places email might be visible to someone other than the sender or recipient:

- **On your end:** Your email client may keep a copy of the messages you send. If so, anyone who gained access to your computer (including thieves and people reading over your shoulder—not to mention your employer) could see what you've sent.
- **In transit:** At minimum, an email message must travel from the device where you compose it to a server, and from a server to the recipient. (If both you and the recipient happen to use the same email server, no further hops are required, but usually messages go to an outgoing email server and then take one or more extra steps over the Internet to the recipient's email server.) An email message could be intercepted along any segment of this journey—for example, by someone "sniffing" an open Wi-Fi network, or by ISPs, corporations, or government agencies monitoring a router. As I'll explain shortly, the

message data might be encrypted during part of its journey across the Internet, but you can't count on this, even if you use SSL to communicate with your email server.

- **On email servers:** The email server you connect to in order to send a message may hold onto that message only for as long as it takes to send it, and then delete it. Or it may cache the message for much longer—even indefinitely. Unless you run the email server yourself, you have no way to know for sure. Once it reaches the recipient's email server, it'll stay there at least until the recipient reads it, but more likely it'll stick around forever, because most modern email systems work best when the server stores the master copies of incoming messages, which then sync to client devices. In any case, for whatever period of time the message is on a server somewhere, anyone with access to that server could conceivably read the message without you or the recipient ever knowing.

Note: The U.S. government currently needs a search warrant to access *unopened* email that's been stored online for 180 days or less—older unopened messages can be obtained with a (simpler) subpoena. But don't assume opened messages older than 180 days, or more-recent unopened messages, are off-limits; the law is murky enough that any message on an email server could be fair game.

- **On the recipient's end:** Everything that's true on your end is also true on the recipient's end, with the additional complication that you have no control at all over what the recipient does with a message received from, or sent to, you. And, if the recipient uses multiple devices or services for email, your message may be on any or all of them.
- **In backups:** You, the recipient, and whoever runs email servers that process your messages most likely back up your data to one or more other locations such as local hard disks and cloud storage. (Good for you! Backups are mighty important.) Those backups may be encrypted, but if they aren't—or if someone with access to the media on which the backups are stored can crack or bypass the encryption—that's another way your email message could be read.

This isn't even an exhaustive list, but I hope that it explains Adam's contention that complete privacy of email messages between you and the other party is little more than wishful thinking. Someone who wanted to know what you sent or received by email would have many potential ways to do so.

Note: There's yet another risk: accidentally sending confidential email to the wrong recipient (or even to a mailing list)! I've done it myself, and I've also received confidential email addressed to me by mistake. Double-check the address(es) before clicking Send!

None of this means someone is reading your email. I'd wager that the overwhelming majority of email messages are never read by anyone other than the sender and recipient. But if you discuss anything sensitive by email, you should be aware that the possibility exists. And, if

the contents of a message are such that someone may have financial, legal, or political motivation to read it, the odds of exposure increase. Unfortunately, because email messages are out of your control the instant you hit Send, it's impossible to quantify the risk.

Are Gmail Ads an Invasion of Privacy?

If you use Gmail, you undoubtedly know that Google scans your messages for keywords to display ads associated with those words. This process is essentially the same one that results in relevant Google AdSense ads appearing on the Web sites you visit, but it may feel more intrusive in this case because of the impression Google is reading email messages that should be none of their business.

But in fact, delivering ads *is* pretty much Google's entire business. Displaying more-relevant ads means advertisers make more money and therefore buy more ads. So it's in Google's best interest to show you the ads that are most likely to result in a purchase. The fact that Google earns money from advertising to you is the sole reason the company gives away Gmail accounts for free. You pay, in effect, by agreeing to look at ads, with the qualification that ads should have some relevance to you based on what's in your email messages.

I always thought Gmail's free-with-ads concept was both clear and reasonable, but many users feel keyword scanning constitutes an invasion of privacy. To this complaint, I have three responses:

- Were Google to display ads randomly rather than based on what you're likely to find interesting, the ads would be even more annoying because they'd be less relevant.
- Remember that ads are matched with messages algorithmically. A computer sees the word "iPad" in an email message and looks for an ad that also designates "iPad" as a keyword. Neither Google's computers nor Google employees know or care what you're saying about iPads; it's a one-way, blind system designed for the sole purpose of selling you stuff. In other words, it's nothing personal.
- If you can't stomach the idea of targeted ads, you can avoid seeing them. Ads don't show up in an IMAP or POP client, for example, and ad-blocking software (see Web Privacy Software) works on the Gmail site too. But, neither technique prevents Google from scanning your email in the first place. If you want Google to stay out of your email entirely, the only right answer is use a different email provider.

Reduce Email Privacy Risks

Now that I've told you how hopeless complete email privacy is, I want to cheer you up a bit by talking about meaningful steps you can take to reduce—not eliminate—the potential for your email messages to fall into the wrong hands. In this case, you protect your privacy by increasing security. The more of these things you do, the fewer opportunities an attacker will have to read what you send and receive. In most cases, they'll be enough. And since you now understand that email privacy can't be perfect, you'll at least be able to make smarter decisions about what should and shouldn't go in an email message.

Log In Securely

In the spectrum of email privacy mistakes, perhaps the worst one is to transmit your username and password to your mail server in unencrypted, human-readable *cleartext*. If you do that, anyone who intercepts the communication between your device and the server can

easily obtain your username and password and then log in to your account and read all your email—and send email under your name. Luckily, this is also among the easiest problems to solve.

Numerous methods are available for authenticating—that is, logging in with a username and password—to incoming and outgoing email servers. The good news is that most of these methods encrypt your password in transit, even if your email and the conduit through which it travels are unencrypted. Odds are excellent that your email app is already set up to authenticate securely, but it never hurts to check.

In your email client (such as Apple Mail or Microsoft Outlook), navigate to the preferences or account settings for one of your email accounts (**Figure 15**). Near your username and password, you'll usually see an Authentication setting, often in a pop-up menu. If this says Apple Token, GSSAPI, Kerberos, anything with "MD5" (such as CRAM-MD5, Digest-MD5, or MD5 Challenge-Response), NTLM, or TLS Certificate, you're in good shape. In addition, if your client is set up to use SSL (see Transfer Email Securely, just ahead), then any authentication method will, by definition, be encrypted. However, if you are *not* using SSL and the authentication method is set to Login, Password, or Plain, your password is probably being sent in the clear.

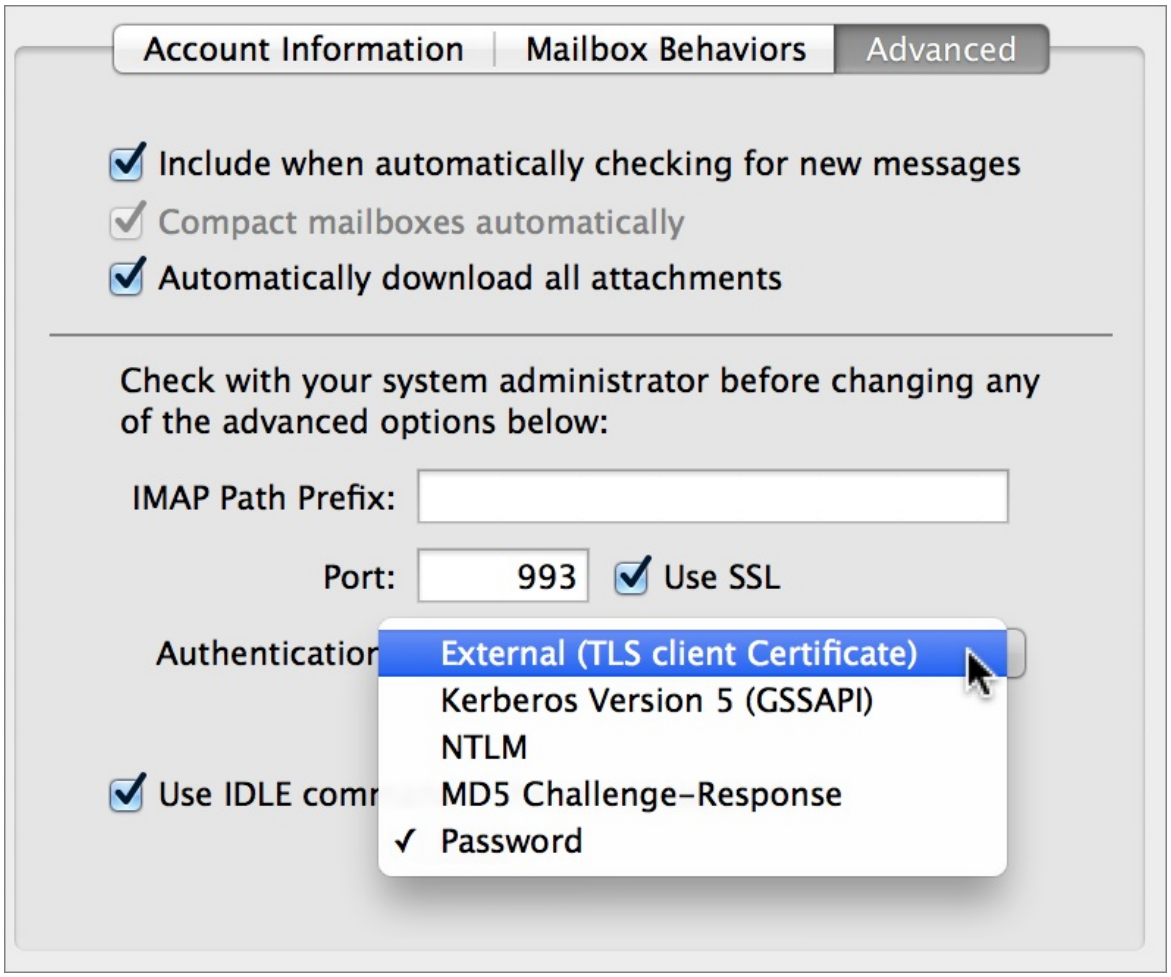


Figure 15: Apple Mail lets you choose, for each account, which authentication method to use for incoming mail (shown here) or outgoing mail. Remember, "Password" is fine if (and only if) the account uses SSL, which this example does.

Unfortunately, you can't arbitrarily select a different authentication method; you must choose one that your email server supports. Look at your email provider's Web site, or contact its technical support department, to find out what your options are. While you're at it, check on whether SSL is supported—if it is, that's your best bet, and then the authentication method is unimportant.

Keep in mind that in most cases, you must go through this process twice for each of your email accounts—once for the incoming (IMAP or POP) server and once for the outgoing (SMTP) server. Microsoft Exchange accounts are an exception to this rule; they use the same server and settings for incoming and outgoing mail.

Transfer Email Securely

After secure authentication, the next logical step to keeping your email private is to use SSL (Secure Sockets Layer), also known as TLS (Transport Layer Security), to secure the connection between your email client and your email server. With SSL enabled, not only are your username and password encrypted on their way to the server, but so are the contents of your incoming and outgoing messages. In this way, SSL prevents eavesdropping on email

traveling between your computer or mobile device and your email server, even if you connect to the Internet via an unencrypted Wi-Fi connection.

If you check your email in a Web browser rather than a stand-alone email client, SSL still applies—you'll know you're using it if the URL starts with `https:` instead of `http:`, or if your browser displays a lock icon—usually in or near the address bar. If it doesn't, consult your webmail provider's documentation to see how you can enable that feature.

Now, I must be clear about the limits of SSL. It protects messages *only* while they're in transit between your local device and your email provider (going in either direction). SSL does not mean that email messages are stored in an encrypted form on your device, at your email provider, or on the recipient's device. And, crucially, SSL is only rarely used for email servers talking to each other. So, even if I use an SSL connection to send a message from my computer to my email server and the recipient of my message does the same thing, my message will most likely travel in unencrypted cleartext from my email server to the recipient's email server, and it could be intercepted as it moves along that path.

In addition, a flaw in SSL's design or a bug in an SSL implementation could open the door to hackers—Apple's SSL bug being one recent example, as I mentioned in the sidebar SSL Implementation Bugs.

Even so, SSL is an incredibly good idea, and if I ruled the world, it would be used by default on all email clients and servers. Even though I don't (yet) rule the world, SSL adoption has been increasing rapidly, and it's a default setting more often than not. But sometimes you have to turn it on manually, and in a few unfortunate cases, email providers—notably, certain large ISPs—don't even offer it as an option.

Enabling SSL/TLS is usually a matter of selecting a checkbox in your email program, which in all probability will be in the same place as your username, password, and authentication setting (refer back to **Figure 15**, earlier in this chapter).

As with secure authentication, you must enable SSL separately for incoming and outgoing email, for each of your email accounts on each device. If you enable it and your email stops working, your email provider might not support SSL (shame on them), but check with your provider's tech support to find out one way or the other. If your provider says SSL isn't available at all, you might consider looking for a new provider that does offer SSL.

And, as a reminder, if you have SSL enabled, your username and password are automatically encrypted along with all other data on that connection, so you can use authentication methods that would send your password in the clear were you not using SSL.

IMAP vs. POP Privacy Implications

IMAP and POP are the two most common protocols for delivering incoming mail from servers to clients. I've long been an advocate of IMAP, which typically keeps the master copy of each received, sent, and filed message on the server but synchronizes these messages with each of your local clients. Compared to POP, which usually deletes messages from the server after you download them, IMAP makes it much easier to use more than one device for email. (For more on POP and IMAP, including common misunderstandings about IMAP, see my article FlippedBITS: IMAP Misconceptions.)

An IMAP privacy concern is that if your password were compromised, someone could see *all* your email messages, not just a handful of recent messages in a POP account. A combination of an excellent password and (if available) two-factor authentication (see the sidebar About Two-Factor Authentication) reduces the threat considerably.

I've also heard people say they prefer POP for privacy on the theory that the less time messages are stored on the server, the lower the risk that an unauthorized person might read them there. However, I am skeptical that downloading messages from a POP server and deleting them on the server provides significantly better privacy. If, for example, a government agency had a black box in your email provider's data center capturing all email, it would catch incoming POP messages before they were deleted. And, even though POP messages may be deleted from a server after they're downloaded, they could be backed up or cached without your knowledge. If you think of POP as a magic bullet to circumvent snooping, think again.

Meanwhile, it's often possible to change the settings in an email client that's using IMAP so that only some messages (such as those in your Inbox) are automatically synchronized. And that, in turn, could increase your privacy if someone gets access to your device, because the messages wouldn't be sitting there waiting to be read. (You would, however, want to change your password in the event of loss or theft to prevent someone else from connecting to your IMAP account and downloading more messages.)

Email Your Doctor, Accountant, or Lawyer Privately

Members of certain professions, such as doctors, accountants, and lawyers, regularly discuss highly personal and sensitive topics with their clients. Given everything I've said about the privacy risks of email, you may be wondering whether you can communicate safely with such people by email. The short answer is maybe.

Privacy laws have led to the widespread adoption of secure Web portals for communicating with doctors and some financial institutions. The way these work is that both you and the person on the other end connect to a secure Web site with a username and password, and all email remains solely on that site—it works very much like any other webmail service, except that all messages are stored encrypted on the server, and are not accessible via POP or IMAP (or to Gmail, Outlook.com, or other email services).

In some cases, a secure Web portal may send you a conventional email message to let you know a secure message is waiting on the server, and that you should log in to read it. That may seem awkward, but there's a good reason for it: sending the message directly to you outside the secure system may be not only risky but also illegal.

Confusingly, the rules and policies governing secure email vary by country and profession, and they're always changing. When I lived in France, I regularly exchanged ordinary email messages with my doctor, but my bank pushed me to use a Web portal. Here in the United States, my doctor will only use a Web portal, but my banker sometimes sends me conventional email.

If you want to send confidential email to a doctor, accountant, or lawyer, ask if she has access to a secure Web portal or a comparably secure method of communication. If not, a phone call might be a better choice. And, if you're a professional in one of these sensitive occupations and don't use a Web portal to communicate with clients, I strongly recommend reviewing the relevant laws and professional conduct standards for your area to determine your best course of action. Be careful sending confidential information over ordinary email—you could be exposing yourself or others to legal liability.

Encrypt Your Email

Even if you use SSL with all your email accounts, you've seen that messages are unencrypted while they sit on various email servers, and often for their journey from one server to another. The only way to be sure they're private from end to end is for you as the sender to encrypt them, and for the recipient to decrypt them.

Encryption, like SSL, is a great idea, and in an ideal world, perhaps all messages would be encrypted all the time. In a moment I'll mention a few ways you can go about encrypting messages if you choose to. But first, let me try to talk you out of it. That's right: I think encrypting email is a less-than-optimal solution for most people, most of the time. Here's why:

- Once the recipient has decrypted your email message, anything could happen to it, and it's entirely out of your control. A message may stay private all the way to Mr. X, but if he's not careful (or if his computer or phone is stolen or hacked), your message could still get out.
- Configuring an email client to encrypt messages can be (depending on the platform and software) a cumbersome process. Once you've done that, encrypting individual messages is usually simple, but requires that your recipients use the same type of encryption, and set up everything correctly on the other end. Even then, in some cases you must go through extra steps to obtain a public key or certificate from the other person before you can send secure email; in other cases, both parties must find some way other than email to swap passwords. You wouldn't want to go through this bother for every message you send.
- Although encryption protects the *contents* of your messages, it doesn't protect their

headers, which means that someone with access to your encrypted email while in transit or on a server could still see the message subject, sender and recipient's email addresses, date and time, and other information that may itself be private.

- As things currently stand in the United States, the NSA can retain indefinitely any encrypted email messages it happens upon, presumably to help the agency learn how to break that encryption. Unfortunately, the very fact that you encrypt messages—regardless of their content—may mark you as a suspicious person subject to more in-depth monitoring. Encrypting email messages not only draws attention to yourself but could mean that any messages that are intercepted will be kept until the NSA can figure out what they say or decides it's not worth knowing.

Those qualifications aside, if you still want to go for it, there are three main techniques you might use:

- **S/MIME:** Almost all modern email clients, including Apple Mail on Mac OS X and iOS, Outlook, and Thunderbird, support an industry standard called S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME uses a form of public-key cryptography: you give me a public key (in the form of a file called a certificate) that I use to encrypt a message I send you, and then only you can decrypt it with your corresponding private key. To reply to me, you reverse the process, encrypting a message with my public key; I decrypt it with my corresponding private key.

  Before you can use S/MIME, you must obtain the necessary certificates and install them on your device; it's a tedious and non-obvious process. (I describe how to do this in Apple Mail—for both OS X and iOS—in *Take Control of Apple Mail*.) Your correspondents must also use S/MIME, and you'll need their public certificates to send them encrypted messages.

- **PGP/GnuPG:** The commercial PGP (Pretty Good Privacy), owned by Symantec, and the compatible, open-source GnuPG (Gnu Privacy Guard, also known as GPG) represent another flavor of public-key cryptography. Conceptually, PGP/GnuPG is roughly comparable to S/MIME (in fact, newer versions of GnuPG also support S/MIME), although the implementation is different.

  You'll typically need to install extra software on your device to use PGP or GnuPG, and it may not be available for your favorite platform or version. However, the process of obtaining public/private key pairs is simpler than with S/MIME, and both systems optionally use keyservers, which let you obtain someone else's public key by looking up a name or email address rather than having to contact that person first. Although it's rare for webmail services to offer encryption, Hushmail does support PGP.

- **Encrypted attachments:** A somewhat simpler, lower-tech approach is to send an ordinary email message containing an attachment that's encrypted; inside the attachment is the private content you want to transmit. A popular tool to do this is WinZip—despite the name, it's available not only for Windows but also for Mac OS X and iOS. If you and the recipient are both Mac users, you can also use Disk Utility to create an encrypted disk image.

  In any case, this approach is great for one-shot communications, such as when you need to send someone a Social Security number, credit card number, or some other isolated piece of sensitive information but don't need whole email messages to be encrypted regularly. However, there's just one problem, which is that the recipient needs the password, and you can't send that by email! The sidebar ahead discusses what to do.

Transferring Passwords Out of Band

When you need to send someone information using a different communication method than the one used for the main content of the message, that's called *out-of-band* communication. Even if the out-of-band channel isn't secure, the fact that you're conveying the password by a different means than the message itself reduces the likelihood that the same person will intercept both pieces of data.

For example, say you've sent me an encrypted file and you need to tell me the password. How might you do that? Here are some ideas:

- **In person.** The best and most reliable method, if practical, is to tell me the password face to face.
- **By phone.** Phone calls can be tapped or overhead, but it's harder to do and may be trickier legally than eavesdropping on email.
- **By chat or private message.** Exchange the password with an encrypted text or voice messaging system such as Skype or Apple's iMessage. The former is known to have a government back door while the latter is currently believed to be highly secure. As with all electronic communications, there are no guarantees, but they're safer than email.
- **Via shared knowledge.** If you know the recipient well, you may be able to construct a story that implies the password without spelling it out. For example, "The comment that girl next to you at the concert made about your shirt, plus your sister's age when we first met."

Send and Receive Email Anonymously

In rare cases, email privacy requires anonymity; revealing your name, your real email address, your IP address, or other personal facts could get you in trouble. I'm thinking, for example, of a confidential source contacting a reporter, an informant telling the police about suspected illegal activities, or someone making politically hazardous statements. In such situations, you may need to disguise the source of the message in such a way that it can't easily be traced back to you specifically.

Numerous services exist for just such a purpose. A quick Web search turns up options that let you send anonymous email with a simple Web form (such as SendAnonymousEmail) as well as services that let you set up an account that provides disposable return addresses (such as Anonymous Speech). With some research you're bound to find many others, including one that suits your particular needs.

However, as usual, I must caution you to read the fine print. Some of these sites log your IP address or other details in such a way that messages could be traced back to you if necessary, and no matter how secure a site claims to be, vulnerabilities could exist that might expose you. And be aware that textual analysis could provide clues to your identity based on word usage and writing habits. Tread carefully if you feel you must use such a service.

Use Email Alternatives

Regardless of encryption or anonymity, you may encounter situations in which email doesn't make sense as a means of communication. In particular, if you're worried about something you write being found on someone else's computer in the future, email is not a good choice.

In the sidebar Transferring Passwords Out of Band, I mentioned several ways you might send someone the password for an encrypted file; all the same methods can be used as alternatives to email if you have something to say that you simply can't take any chances with. And I go into more detail about one such category in the next chapter, Talk and Chat Privately.

Another option I should mention is the self-destructing digital message. Although these take various forms, the general idea is that you send someone a link to a message on a Web site, or using a mobile app—and once viewed, that message is visible for only seconds or minutes, after which time it's permanently deleted. Although such systems aren't foolproof—the recipient might, for example, take a screenshot of the secret message before it self-destructs, or use file recovery software to undelete it after the fact—they do reduce the risk that a private message will later be discovered on someone else's device, at least by technically unskilled people.

I found many such services and apps on the Web, although I haven't tried them personally, so I can't speak to how effective, secure, or easy to use they may be. A few examples:

- DestructingMessage.com
- Self-Destructing-Email
- Snapchat
- This Message Will Self-Destruct

Talk and Chat Privately

I am old enough to remember the days when, if someone wanted to converse with another person who wasn't nearby, both people would talk into analog devices called "telephones" to have real-time audio conversations. Perhaps you've seen such devices in old movies or read about them in antique documents called "books."

I kid, but analog telephones are rapidly on the way out. My home phone, which I used to refer to as a "landline," bypasses the phone company altogether and relies on a box that plugs into my broadband router. I happen to use Vonage for my home VoIP (voice-over-IP) telephone service, but I could have chosen a similar service from my broadband provider or from any of numerous other companies. In other words, for me, telephone service is a variety of Internet service.

And then there's my smartphone, which is almost never out of reach. I use it for conventional audio phone calls maybe once a week on average. Of course, I constantly use it for email, instant messages, SMS, Twitter, and video chats—most of which, again, travel over the Internet—and even those occasional audio calls are more likely than not to use a VoIP app such as Skype.

Meanwhile, my computers and tablets have software for a long list of services that provide real-time text, audio, and/or video communication—not just Skype but also Google+ Hangouts, AIM (AOL Instant Messenger), Apple's FaceTime and Messages, and numerous others you may or may not have heard of, to say nothing of the chat services built into games, Facebook, and other social networking services. Xbox, PlayStation, and Nintendo game consoles all support messaging and voice chat too.

The question is: How private are any of these real-time communication services?

Understand the Privacy Risks of Real-Time Communication

One of the best ways to acquaint yourself with the risks of real-time communication is to watch the HBO TV series The Wire. Yes, all five seasons. (Go ahead and do that, if you haven't already, and then come back to this page.)

I've mentioned The Wire because a lot of it has to do with electronic surveillance (hence the name)—but the main target of this surveillance is ordinary mobile phones. On the show, law enforcement agents need both special equipment and legal permission to monitor the mobile

phone use of suspected criminals. But the process ultimately poses little technological challenge, and the people being monitored have no way to know their conversations aren't private.

Now, think about that and consider the fact that monitoring real-time communication over the Internet is potentially *easier*. And, although government and law-enforcement entities have greater access to this sort of data than ordinary citizens, professional hackers and even casual snoops likely have the capability to see (or hear) far more of this data than you might suspect.

As with everything else I've discussed in this book, precisely what that means to your personal privacy depends on what you say and to whom, but in principle there's almost no limit to your potential risk. However, let me now backpedal a bit and point out a few mitigating factors:

- Audio data is more difficult to store and analyze than textual data, and video data poses a bigger challenge than audio data. Because of the sheer inconvenience of dealing with such large amounts of data, it's far less likely that your audio or video calls will be kept or searched than email, text messages, or chats. Of course, if your VoIP connection were compromised, a computer could attempt to transcribe every word of a conversation and turn it into conveniently searchable text without having to store the audio or video itself. So although there are no guarantees, on the whole, I consider voice and video communications over the Internet to be safer than any sort of text-based communication.
- The previous point notwithstanding, available technical details and anecdotal reports suggest that Apple's encrypted iMessage service—which can be used for text messages and file transfer between Macs and iOS devices—is highly resistant to hacking and eavesdropping. (See the sidebar just ahead for more information.)
- Communication that takes place entirely over the Internet (for example, Skype-to-Skype calls or FaceTime chats) or entirely over analog phone lines is probably safer than communication that crosses between the two (such as using Skype or a VoIP service to call a landline phone) because calls that traverse multiple networks have more potential points of interception.

Security in iMessage and Other Apple Services

If you're curious to learn exactly what security measures Apple uses with iMessage, iCloud Keychain, and other services, you can find them in the PDF iOS Security, which also applies somewhat to Macs. For a less technical summary of the iCloud Keychain portion of this document, read Rich Mogull's TidBITS article How to Protect Your iCloud Keychain from the NSA.

And, to learn much more about how iCloud Keychain works and how to use it, see my book *Take Control of iCloud*.

Improve Your Real-Time Communication Privacy

If you have money to burn and a powerful need for a "secure line," you can buy secure telephones (landline) or crypto telephones (mobile) with built-in hardware encryption. There are also various hardware and software products (for example, Silent Circle) that can work with existing phones to achieve the same effect. But end-to-end encryption means both parties will need interoperable equipment or software.

For the purposes of this book, I'm assuming you don't need such a heavy-duty solution. For improving your day-to-day privacy in real-time communication, I suggest the following:

- **Read the privacy policies.** Your mobile carrier, ISP, VoIP provider, instant messaging service, and other such companies will have boring pages of legalese, but you should at least be able to scan them to see if the services encrypt your data, and under what circumstances they may share your information with others.
- **Use encryption when available.** Encrypted connections don't necessarily mean that no one can eavesdrop. For example, Skype (now owned by Microsoft) encrypts communication but recent disclosures suggest the service has back doors that make the contents of calls (even audio and video) available to the U.S. government. Even so, more protection is better than less. But that brings me to…
- **Use obscure products.** Tens of millions of people use Skype and AIM, making them attractive targets for both official surveillance and hackers. Newer and less-popular communication services—more of them are popping up all the time—might not be large enough to attract that sort of attention. Of course, they also may not have the expertise or resources to engineer or operate a high-quality service.
- **Favor higher-bandwidth communication.** All things being equal, if circumstances permit, choose video before audio, and audio before text—simply because anything other than text makes it less convenient to capture, store, and analyze your conversation (and all the more so if it's encrypted). Remember, none of this means audio or video is entirely safe from snooping, but the odds are more favorable than when using text-based

communications.

Keep Social Media Sort of Private-ish

At the risk of stating the obvious, *social* implies interaction with other people, which is somewhat at odds with privacy. On the Internet, it's best to think of "social" as synonymous with "public" (even though that's not necessarily true), because once you've shared something online—in any of a hundred senses of sharing—whoever you've shared it with can, in turn, share it with someone else.

As a result, the very best advice I can give you about privacy when it comes to social media is *not to expect any*, regardless of your privacy settings. You may imagine that the things you post or tweet are just between you and your friends (or "friends," as the case may be), but that's optimistic at best. Instead, assume anything you put online using social media—including chats and private messages on Facebook, direct messages on Twitter, and profile details such as your name, location, and date of birth—could be discovered by anyone in the world, and could be online forever. If you're unwilling to make any of that information public, don't share it in the first place.

However, there are still better and worse approaches to social media, and you should know how to protect yourself to the extent possible.

Understand the Privacy Risks of Social Media

Wait, didn't we just cover that? Yes, any data you put online using any social network can potentially become public. I know you know that.

What I'd like to emphasize here is how that could be a problem for you.

As I mentioned early in this book, everyone from Local Villains to Big Data can easily find you on social media. You might be astonished how much private data could be culled from years of Facebook updates, tweets, LinkedIn updates, Instagram pictures, Yelp reviews, blog posts, and a long list of other social media activities.

It's easy to discover not only basic facts about you and your family but also where you've been, who you hang out with, which causes you support, what your political and religious beliefs might be, and, perhaps most important of all, *what sort of person you are*. Even if no individual statement tells the story, the combined data from all these sites and services can do something akin to browser fingerprinting (see On a Web Server)—it can paint a vivid and precise picture of you. So…

- If you're trying to get a job, a prospective employer may use social media to determine whether you're likely to be trustworthy, polite, punctual, and loyal—and to see how you've behaved in other jobs.
- If you're applying to a college or university, admissions officers may use online profiles to judge your seriousness and confirm any personal details you've submitted.
- If you're dating, someone thinking about starting a relationship with you could also learn a lot about your tastes, biases, character, and history with previous partners.
- If you're ever suspected of a crime, the police or prosecutor could scour social media for evidence of bad behavior—or a defense attorney could try to demonstrate a pattern of selflessness.
- If you ever run for political office…well, I hope you're a saint, because anything you've ever said online can and will be used against you.

And those sorts of concerns merely involve the historical record. Day-to-day social media posts can also cause privacy problems:

- You mention on Twitter that you're going on vacation (or just going to a concert), and burglars break into your house.
- You post geotagged pictures on Flickr that show your location and the time you took them—today, just after you called in sick to work.
- Your Facebook relationship status says "It's complicated," but your romantic interest didn't think so.

I could go on, but you get the idea. The stakes when it comes to social media are much higher than you may imagine. Your social media history can win you—or cost you—a job, love, or even your freedom.

Check Your Privacy Settings

Every social media site and service has a privacy policy (see What about Privacy Policies?). You should read it, if only to be aware of how much data you're inevitably giving away.

Beyond that, examine each account's privacy settings. Some services offer very little privacy control—for example, your only real options for Twitter are to protect your tweets (meaning you must personally approve each follower, and those followers can't retweet you—not a terribly engaging way to use the service, if you ask me) and to hide your physical location. Facebook has changed its privacy settings repeatedly. It currently offers more control (**Figure 16**), letting you limit who can see various categories of information (for example,

everyone, only friends, or friends of friends)—but even limiting sharing to your friends is no guarantee that one of those friends won't share it, or that a programming error or misbehaving app might not reveal it.

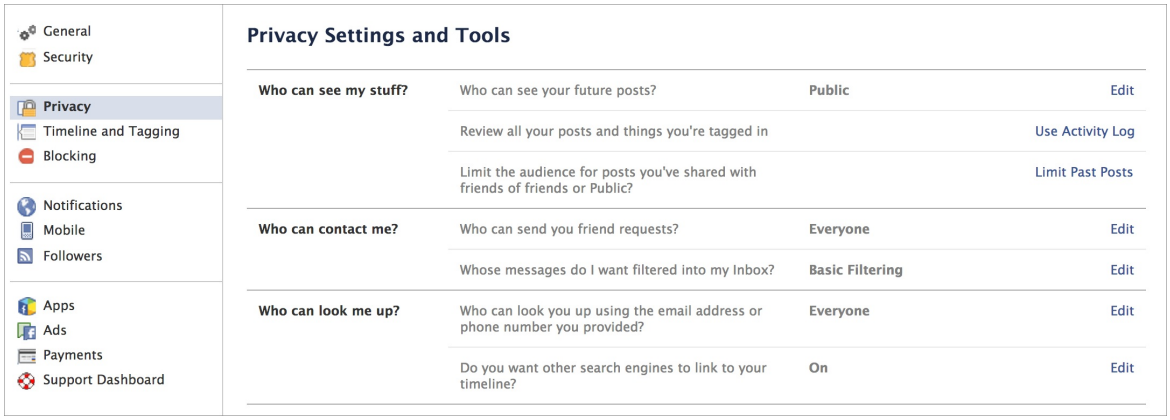


Figure 16: Facebook's privacy settings are less detailed than many would prefer, but they're better than nothing.

In other words, do pay attention to the settings and configure them as best you can, but don't count on them. They aren't foolproof.

Here are direct links to access the privacy settings for a few of the most popular social networks:

- Facebook
- Twitter
- Google+
- LinkedIn
- MySpace

Use Other Social Media Precautions

Apart from the obvious advice not to post anything on social networks that you'd mind being public, allow me to offer a few privacy tips:

- **Limit your friend lists.** Most people assume the more Facebook friends you have, the better. But if your list includes people you know only a little or not at all, you can't think of them as *friends*—you can't trust them to take care of your private data. Everyone has their own rules, but I wouldn't want anyone to be a Facebook friend who I wouldn't invite into my home for coffee.

  The situation is different with Facebook pages, Google+ circles, Twitter followers, and other one-way relationships. You may think of these as being more private because you're

not required to friend or follow the other person, but that doesn't stop them from reading everything you post about yourself. If you can't control who sees your photos, videos, or updates, censor yourself accordingly.

- **Don't assume "private" messages really are.** You can send messages on Facebook that function much like email messages, or have a live chat. You can send direct messages to another user on Twitter that don't appear in your public timeline. And many other social networking sites also offer seemingly direct, seemingly private modes of communication with other members. But these messages aren't sacrosanct. Site administrators may be able to read them, and can almost certainly provide them to anyone who showed up with a court order. And there have been cases where, due to a programming error or other security breach, the contents of such discussions leaked out.
- **Don't assume "secret" services really are.** A whole category of services has recently sprung up that lets you share thoughts and feelings with other people anonymously with mobile apps such as Secret and Whisper. Unfortunately, as the Wall Street Journal's Geoffrey A. Fowler pointed out in Psst, Secrets You Share Online Aren't Always Safe, such apps can store and transmit enough information about you to give away your identity (and are subject to hacking and bugs, just like everything else).
- **Limit apps.** On Facebook and other sites that let you install apps, *just say no*. Although each app is different, some of them can read everything you write and spread your data around in ways you might dislike.
- **Use HTTPS.** On sites that support it (including all those listed above), use HTTPS to log in to prevent eavesdropping (see Browse Securely).
- **Use good passwords.** As I said in Protect Passwords and Credit Card Info, be sure to use passwords that can't be guessed by human or machine. Long (think 14+ characters), random passwords are usually best way to go. And, if a site offers two-factor (or two-step) authentication, enable it (see the sidebar About Two-Factor Authentication, just ahead). That will greatly reduce the chance of your account being hacked. Be sure to keep those excellent passwords safe—don't share them, and log out of your user account before letting someone else use your computer.
- **Think carefully about pseudonyms.** You may use an alias rather than your real name on Twitter, Tumblr, or other sites. Although pseudonyms like this can protect your privacy, they're not impenetrable—so again, don't stake anything critical on them. Furthermore, sometimes pseudonymity can work against you, as I describe in the sidebar When Privacy Hurts, ahead.

About Two-Factor Authentication

Two-factor authentication, sometimes known as two-step authentication, is when a site or service needs more than your username and password—it also needs another *factor*, which could be a physical token, a fingerprint scan, or any of numerous other options. One common implementation is to require a numeric code sent as a text message to your mobile phone or generated using a mobile app such as Google Authenticator.

Two-factor authentication is less convenient than using a password alone, but it drastically reduces the chances of an account being hacked, because the attacker would need both your password and your mobile device (or other factor).

When Privacy Hurts

For the most part, I assume more privacy is better than less. But there are counterexamples—situations in which you'll be safer or happier with *less* privacy. For instance:

- If you try to get a reservation with Airbnb, the host may want evidence that you're someone reasonable enough to invite into their home. Profiles with your real name and information about your real college, job, friends, and background could put someone at ease, while a fake profile (or none at all) could put them off.
- The same employers, insurers, lenders, and other institutions that could ding you for negative information in social media could reward you for positive information.
- New friends might feel more comfortable letting you into their lives if they can find out more about the real you online.
- If the police want to know where you were on the night of the 16th, you might be able to point them to exculpatory photos or tweets—but you better be able to prove they're really yours!

I can't make any blanket statements about what you should or shouldn't keep private; I can only say, as I said before: privacy cuts both ways.

Share Files Privately

In my world, "sharing files" generally means exchanging business documents such as word processing files, PDFs, and screenshots—maybe the odd font or disk image. I may be atypical in that regard. I have heard stories suggesting that people sometimes share less-wholesome files, including pirated movies, games, and software. If you're tempted to do that, I invite you to skip back to Take the Pledge and follow the instructions there for avoiding online stupidity.

Having dispensed with that obligatory disclaimer, the fact is that *what* you have to share is none of my business or concern. You may have digital content of some kind that, for any of numerous legitimate reasons, you want to share online, but for which you have a privacy concern. In this chapter, I talk briefly about the privacy risks in file sharing and explore a few ways of addressing them.

Note: If you're looking for the ultimate guide to sharing illegal stuff without getting caught, sorry—this isn't it. I'll outline the basics of private file sharing here, but remember: this book is about ordinary privacy for ordinary people.

Understand the Privacy Risks of File Sharing

To put it as concisely as I can, most privacy concerns with file sharing fall into one of the following categories:

- You want to share files with a specific person or group without letting anyone else know what you were sharing or with whom.
- You want to share files publicly, but without anyone knowing you were the person who uploaded or downloaded them.

Most methods of sharing files offer neither sort of privacy protection, which is why you may want to use extra precautions.

And what are the risks if you don't? That all depends on what you're sharing. Perhaps a competitor sneaks a look at trade secrets in confidential business files you're sharing with your employees, clients, or contractors. Maybe the public gets early access to the top-secret new album, software, or game that you were only previewing for your agent or investors. Or the other side in a legal dispute sees potentially damaging information in a file you intended for your lawyer's eyes alone. And, if you're sharing copyrighted media, the copyright holder can rain all sorts of legal trouble on you.

Encrypt Transfers, Files, or Both

A danger when sharing files is that their contents could be intercepted in transit between your computer and the recipient's computer. You can reduce the risk of eavesdropping if you Encrypt Your Wi-Fi Connection or Use a VPN, but these measures protect data only for part of its journey. For end-to-end protection, the connection between your computer and the remote computer must be encrypted.

When you're connecting to a file server, that generally means using protocols such as SFTP (SSH File Transfer Protocol), FTPS (FTP over SSL), FTP over SSH, or WebDAV HTTPS. Whatever you do, you should not use plain FTP (File Transfer Protocol), which is about the least secure file transfer method there is. (Not only is ordinary FTP not encrypted, but even your password is sent in the clear!)

However, protecting files while in transit may not always be an option—and even when it is, it only solves part of the problem. If a file is going to be sitting on a server someplace, and if you want to restrict access only to trusted parties, you might want to encrypt it as well.

Back in Encrypt Your Email, I mentioned that you might use a program such as WinZip to encrypt files, or, to transfer files solely between Mac users to create an encrypted disk image in Disk Utility. The same advice holds for files you share with other methods—whether you upload to a public server or use any of numerous file sharing services such as Dropbox, Google Drive, SugarSync, or SpiderOak.

But wait! Don't these and most of the other cloud storage and syncing services already encrypt files you upload? Yes! Sort of!

I'll take Dropbox as an example, because it's the most common of these (and because I wrote a book about it, *Take Control of Dropbox*). All the files you put in your Dropbox are indeed encrypted, but Dropbox holds the encryption key, so the company could decrypt your files if they had to (for example, in response to a subpoena). Even if that's not a worry, Dropbox has two different methods of sharing files:

- **Share a link:** Dropbox generates a link to a file or folder you've stored online, and you can do whatever you want with that link—post it on a Web site or send it by email, say. Anyone who follows the link gets the contents of the file or folder—unencrypted. In other words, once you've shared a link, the only thing protecting it is the URL's obscurity. If anyone learns that URL, Dropbox's encryption is moot.
- **Invite someone to a folder:** You can share a folder in such a way that only people you invite can share it, and those people must all be Dropbox users too. This method enables the files to stay encrypted on the server all the time, although of course you can't control

what any of the other participants in the folder may do with your files.

So, for Dropbox, if you're sharing a *link* and you want to ensure that a file stays private, you should encrypt the file *before* putting it in Dropbox in the first place. Then you can share the password with the recipient (see the sidebar Transferring Passwords Out of Band).

Other services have their own methods (so you'll need to read the fine print), but the general rule is that if you're sharing a link in such a way that the link is the only thing someone needs to access the file, the service's encryption is irrelevant—you should instead encrypt the file yourself first.

Finally, let me mention that if a file is sensitive enough to encrypt, you should pay attention to its *name* too. Sometimes filenames themselves give away important information, and if that may be the case, obscuring the filename is a smart idea.

Keep File Syncing and Backups Private

What about files you store in the cloud using a backup or sync service, but *don't* share with anyone else? Those should be safe from prying eyes, right?

Well, yes—*usually*. Any cloud syncing or backup service worth its salt encrypts your data both in transit and while stored online, which means that it should be safe from anyone but you, the person who chose the password. However:

- A weak password could enable someone else to break in.
- Even a strong password might not prevent the provider itself from accessing your files, if the provider holds the encryption key. Some (such as Dropbox) always do; some (such as SpiderOak) never do; and some (such as CrashPlan) give you the choice. I say more about this in *Take Control of Dropbox* and *Take Control of CrashPlan Backups*, but basically: if you don't control the key, you should take extra steps to encrypt any sensitive files yourself.
- If you've synced files to multiple devices, and if one of those devices is stolen, then those files could be visible to the thief (unless you've protected them in other ways, such as using FileVault on a Mac or some other form of full-disk encryption).

But generally, as long as you're reasonably careful, files you sync or back up to an encrypted cloud service should be fine as long as you don't share them with others.

By the way, just as you should encrypt backups in the cloud, you should do the same for backups stored on a local disk if that disk could ever leave your physical control (for example, if you keep an extra backup disk offsite). CrashPlan, Apple's Time Machine, and numerous other backup apps can encrypt local backups.

Use Peer-to-Peer File Sharing

Another type of file sharing relies on *peer-to-peer* (or P2P) file sharing networks, of which the best known is BitTorrent. Peer-to-peer file sharing has many perfectly valid, legal uses, including distributing large files without incurring massive storage and bandwidth fees.

Sometimes you'll even see musicians and movie studios using P2P networks to distribute media to the public. But P2P is often associated with illicit sharing of copyrighted materials—fair warning.

In a P2P network, someone makes a file available for others to download, but as soon a recipient downloads a portion of the file, that person's computer also turns into a server, making that portion available to other downloaders. Thereafter, anyone trying to download the same file may connect to multiple computers at once, fetching only small pieces of the file from each one; the client software reassembles all the pieces at the end. This makes file transfers more efficient, but (slightly) harder to track than conventional client-server transfers.

Note: There's an official BitTorrent client, but many third-party client apps also work with the BitTorrent protocol.

How does your P2P client know which other computers are currently sharing all or part of a certain file (and if only part, which part)? That's the job of a computer called a *tracker,* which maintains a list of all the file's pieces, but doesn't actually store the file itself.

And how do you find a tracker that knows about a file you want to download? Using BitTorrent, that information—basically details about the file and the address of one or more trackers—is stored in a tiny file called a *torrent*. Torrents can be sent by email or posted on any Web site, but most users get torrents from innumerable Web sites that index and distribute torrents by the thousands.

Frustratingly for those fighting copyright violations, a torrent itself (or a site that indexes them) doesn't contain any of the files' potentially copyrighted contents, only the address of a computer or service that coordinates the files' distribution, piece by piece. The only sure way to know who's transferring what to whom on a P2P network is to join one yourself; in the process of transferring a particular file, you'll also see the IP addresses of the other computers uploading and downloading portions of it. IP addresses, as we've seen, can often be traced back to individuals. So, Big Media frequently hires specialized firms to monitor P2P sharing of movies and other copyrighted files in order to find out which IP addresses should be the targets of legal action.

Warning! Possibly an even bigger danger than privacy risks using BitTorrent and similar networks is that pirated media files often contain malware or digital watermarks that can harm your computer and/or further endanger your privacy. Be suspicious!

Now then... What most people want from P2P networks is the public yet *anonymous* transfer of files. That is, you're not hiding the files' contents from anyone; you simply want to prevent

anyone else from knowing that you were the one who uploaded or downloaded it. If that's the case, you can consider several options:

- **Hide your IP address.** If you use a proxy server or a VPN (see Use a VPN)—or even better, an *anonymous* VPN that does not log connections (examples include BTGuard and TorGuard)—you greatly reduce the risk that any particular file transfer can be traced to you, at the cost of slower performance. (Of course, this doesn't help you if someone finds the file in question on your computer!)
- **Avoid suspicious public indexes.** You may have heard of a site called The Pirate Bay—I won't link to it here because I'd like you to stay away from it! Same goes for IsoHunt. These are among the biggest torrent indexers, and they're also places most likely to lead you to torrents that are tracked, contain malware, or both. With some research you can find less common indexes, including some that are invitation-only.
- **Avoid seeding.** In P2P terms, *seeding* means making an *entire* file available to downloaders—either as the file's originator or as a public service after you've downloaded the whole thing. Seeding is considered a kindness among P2P users, but it also arguably increases your legal liability.
- **Try a friend-to-friend network.** Most P2P networks, including BitTorrent, are public—anyone can join. A subset of P2P networks is the friend-to-friend (F2F) network, which is basically a private peer-to-peer network among friends who agree to participate with each other—only members can easily see what's being transferred within the group. Retroshare is an example of such a network.

There are many other varieties of peer-to-peer file sharing systems, and numerous apps, services, and techniques designed to keep them more private. But if you have to go through that much effort, you may be better off creating your very own personal cloud, as I discuss next.

Create a Personal Cloud

What if you could combine the simplicity of Dropbox with the security of a friend-to-friend network and the assurance that all the data and hardware is safely under your control? And what if, in the bargain, you got up to 3 TB of file storage that you can access from any computer or iOS device, with no monthly fees? If you have a lot of data to share privately, you may be interested in a device called the Transporter.

Transporter is a small gadget containing a hard drive and a network interface, much like a NAS (network-attached storage) device. (A version called Transporter Sync omits the internal hard drive and works with any external USB hard drive you have.) The difference is its

software, which makes it function very much like Dropbox. All transfers to and from your Transporter are encrypted, and if you have two or more of them, they can automatically sync any or all of their files with each other, regardless of where they're physically located. So, merely by connecting a Transporter or two to the Internet, you effectively create a personal cloud for file sharing.

I've had a Transporter for nearly a year, and although it's not ideal for most of my needs (see my TidBITS article Bypassing the Cloud with Transporter), I like the fact that it has none of the complications of peer-to-peer networks. If I wanted to share large files with a few friends and have near-zero risk of intrusion or detection, that's how I'd do it. (You can even share files in a way that other users need not have their own Transporter.) But remember that anyone with physical access to one of your Transporters, or who can learn your password in any way, could obtain your data, so be sure to take appropriate security measures.

Transporter isn't the only device in this class. A number of other NAS devices (such as Synology's DiskStation products and TonidoPlug) also offer private sharing over the Internet, but Transporter stands out for its size, cost, and simplicity.

It's also possible to create a personal, Dropbox-like system for syncing and sharing files using only software—for example, with the free BitTorrent Sync. But because this runs on your computer(s), you'll have to leave at least one computer turned on, awake, and connected to the Internet at all times to maintain access to your data from other devices.

Maintain Privacy for Your Kids

Everything else in this book has been about managing your own privacy. But if you're a parent of a young child, you have an additional challenge: maintaining your child's privacy. Speaking as the father of both a preschooler and an adult child, this isn't as easy as you might think.

At a certain age, your child will begin making his own decisions about what to share online. I can't tell you what that age is or should be; I can only say it will be too young and you will likely be horrified at some of your child's choices. You'll have to sit down with your child and have the online privacy talk, which could be even more stressful than the sex talk. You'll try to lay down the law, but your child will push back and find ways around whatever controls you exert. Regardless of when and how this plays out, you should brace for the certainty that your child's online privacy will eventually be out of your control, and remember that kids always make poor decisions on their way to learning how to make good ones.

Note: In the United States, 13 is a "magic" age when it comes to online privacy. COPPA (Children's Online Privacy Protection Act) prohibits Web sites or online services aimed at children from collecting personally identifiable information from children under 13 without parental consent, a requirement that many sites meet by refusing to let younger kids have accounts at all.

What I want to talk about is what comes before then—the time between your child's birth and the moment you hand over the keys to the digital world. This is the period when your child's online privacy depends mainly on you, and the choices you make now can affect your child forever.

My mother has snapshots of me as a young child that were great for embarrassing me in front of college girlfriends, but the photos were kept in boxes or albums and dragged out only on special occasions. At worst, a girl might tell a story about a picture she'd seen, but she couldn't show anyone else.

But pictures don't work like that anymore. If you snap a cute shot of your young daughter in some comically brilliant situation, it's much more likely to go on Facebook or Twitter than on paper in an album. A few years from now, her classmates will be able to see it. All her future friends, love interests, employers, and children will be able to see it—so will unsavory characters you'd like to protect her from. And anyone who sees it will be able to share it with anyone else in the world. Is there any possibility your daughter might live to regret your choice?

Everything you say about your child online—every picture and video, every story told or fact revealed—becomes part of your child's *permanent* Internet record. You can't ever take it back, and you can't ever control how it might be used. And things that seem innocent now might cause all sorts of problems for your child in 10 or 15 years.

None of this means you should never talk about your child online or post photos or videos. It only means you should do so circumspectly and sparingly. You'll have to determine your own rules, but here are my tips:

- Never post anything online that could be used to predict your child's location (including a route to or from school), at least when a parent isn't around. This includes images with signs or landmarks in the background.
- No matter how cute your kid is in the bathtub, seriously, don't post any nude photos online. (You did Take the Pledge, right?)
- Blog posts and other stories about your child's behavior problems might have far-reaching consequences. Keep it positive.
- Kids say and do the darnedest things, but even though your children's antics may entertain other adults, they could result in untold cruelty in the hands of a class bully a few years from now. Be super careful about sharing anything that has the potential to embarrass your child in the future.

As your child starts using online services without your supervision, you will undoubtedly want to teach him good privacy habits, and I hope the information in this book (especially in Take the Pledge) provides a useful starting point for discussion. If you instill a healthy sense of wariness from a young age, your child will be better equipped to fully take over the management of his own online privacy when the time comes.

Teach This Book

This book helps you understand threats to your online privacy and take steps to reduce them. But what if you need to help other people make better online privacy choices? If you'd like to use the material in this book as the basis of a presentation, class, training program, or other teaching opportunity, we'd like to offer our assistance:

Share a Cheat Sheet

Lots of people won't read a book like this but still long for better online privacy. So we've developed a free, one-page PDF handout to cover the main points and key tips in this book. You can give it to anyone who needs quick advice. Download it here, and you can print copies for colleagues, send it to them via email, or share it online.

Order Classroom Copies

You can buy discounted copies of this book for classroom use. If you want to teach a group about online privacy, classroom copies are an inexpensive way to ensure that each participant has a copy of the book.

Download Training Materials

Not sure what to say in a course about online privacy? You can download a free, simplified presentation (in an iPhone- and iPad-friendly PDF format, with the option to purchase an editable Keynote or PowerPoint file) that covers the main points in this book (contact us for purchasing details). Be sure to download the cheat sheet for your students too.

Hire the Author

For the ultimate experience, you can hire Joe Kissell to speak to your group about online privacy in person (or, if you prefer, by video). He's an entertaining and engaging speaker, and can work with groups of any size. Besides teaching the material in this book, he can customize a presentation to meet your organization's needs, answer participants' questions, and work with you to develop effective online privacy policies. For more information and a price quote, please contact Joe.

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 a Senior Editor of TidBITS, a Web site and email newsletter about Apple and the Internet, and the author of numerous books about Mac and iOS topics, including *Take Control of Your Passwords*, *Take Control of Dropbox*, and *Take Control of Backing Up Your Mac*.

He is also a Senior Contributor to Macworld, was 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 or speaking, Joe likes to travel, walk, cook, eat, and dream (in both senses of the word). He lives in San Diego with his wife, Morgen Jahnke; their son, Soren; and their cat, Zora. To contact Joe about this book, send him email.

Shameless Plug

Although I currently write and speak about technology as my day job, I have a great many other interests. To learn more about me, read other things I've written, and find out what I'm up to beyond the realm of Apple products, visit my home page at JoeKissell.com. You can also follow me on Twitter (@joekissell) or App.net (@joekissell).

About the Publisher

Publishers Adam and Tonya Engst 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.

Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who has reached the age where he can read, understand, and find mistakes in the Take Control series.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Geoff Duncan
- Production Assistant: Oliver Habicht
- Take Control logo: Geoff Allen of FUN is OK
- Cover design: Sam Schick of Neversink

Copyright and Fine Print

Take Control of Your Online Privacy
ISBN: 978-1-61542-425-2

TidBITS Publishing Inc.
50 Hickory Road
Ithaca, NY 14850 USA

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

This electronic book doesn't use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. 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.

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

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 ebook 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.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

Featured Titles

Click any book title below or visit our Web catalog to add more ebooks to your Take Control collection!

Take Control of 1Password (Joe Kissell): Slowed down by entering passwords repeatedly? Learn how to let 1Password do the heavy lifting.

Take Control of Apple TV (Josh Centers): This essential guide covers everything you need to know about the Apple TV!

Take Control of Backing Up Your Mac (Joe Kissell): Set up a rock-solid backup strategy so that you can restore quickly and completely, no matter what catastrophe arises.

Take Control of CrashPlan Backups (Joe Kissell): Join backup expert Joe Kissell as he shares real-world advice about protecting your data with CrashPlan's onsite, offsite, and cloud backups.

Take Control of Dropbox (Joe Kissell): Discover the many features—especially the non-obvious ones!—that make Dropbox an exceptionally useful and popular Internet service for file transfer and collaboration.

Take Control of iCloud (Joe Kissell): Understand the many features, get set up properly, and enjoy iCloud!

Take Control of iTunes 11: The FAQ (Kirk McElhearn): This FAQ-style ebook helps you wrap iTunes around your little finger and enjoy your media more.

Take Control of Your Paperless Office (Joe Kissell): With your Mac, scanner, and this ebook in hand, you'll finally clear the chaos of an office overflowing with paper.

Take Control of Your Passwords (Joe Kissell) Overcome password overload without losing your cool—and view the comic that goes with this ebook!