Protect Your Privacy!

17 Ways to Keep Your Information Secure Online

JAMES ELDREDGE

Protect Your Privacy!

By
James Eldredge

About This Book:

Protect Your Privacy! is a short book designed to help the average computer user stay safe and protect their privacy and their data in the modern age.

Inside this book, you'll learn about common security misconceptions, discover ways that attackers try to steal your data, learn how to protect your data in multiple ways and discover advanced methods for keeping your private information safe. Everything is in plain English and is easy for users of all experience levels to understand (even complete beginners).

James Eldredge has worked in the computer field for thirteen years, working as a system administrator, database engineer, programmer and much more. Through his years of experience, James has cultivated a unique way of communicating complex ideas and instructions to beginners and has used this skill to build up an impressive number of clients who all rely on his expertise on a daily basis. His no-nonsense, plain English and no-jargon approach has carried over into his books, which are directed toward both the complete novice and moderately skilled user.

Want to get free books and awesome technology tips and tricks? Sign up for the free AppSna.gr newsletter right here!

More Books from James Eldredge:

The Top Essential Windows 10 Tricks You MUST Know!
TV Without Cable: Your Complete Guide to Streaming TV & Over-the-Air Free TV

Table of Contents

I – The Importance of Data Privacy

The Internet is, in my opinion, one of the most fundamentally important and game-changing inventions in the history of man. In just a few decades we've managed to collect together a huge portion of the world's knowledge into a centralized location that anyone can use. Websites like Wikipedia make it easy for anyone to learn anything about everything. MIT's open courses enable people around the globe to receive a free college education. We can instantly communicate with anyone we want, anywhere we want and at any time we want.

Of course, all of these positives have come at a tremendous cost. The modern Internet is filled with companies whose only purpose is to get as much information about you as possible. What do they want to do with this information? Sell it, of course! Information is the new currency, and companies—both legally and illegally—are trying to gather as much of it as possible.

Did you know that when you visit most websites, a piece of data (called a 'cookie') is placed on your computer that tracks where you go online? These tracking cookies come in many forms and from various companies, some which you've heard of and some which you haven't. This type of thing is perfectly legal, but it can still be damaging to your privacy. Intrusive advertising can reveal information about your private life that you don't want others to know. Companies can sell detailed records of where you go and what you purchase online to other companies, or they can be compelled to hand it over to the government.

And what about the people who are illegally collecting information? Hackers, malware authors and people who steal banking information, email addresses and other personal information are all doing it to make money as well. There is an entire underground industry that has sprung up around one goal: getting your information and making money from it. Unfortunately, companies that legally collect your information can be vulnerable to having that information stolen by people engaged in illegal activities.

Whether your information is being gathered by companies like Facebook or Google or by someone sitting in a dark room writing a virus to steal credit card numbers, the bottom line is this: **you need to secure yourself**. There are a whole range of ways you can do this, and the methods range from simple (using a different browser) to the complex (encrypting the data on your hard disk so no one

but you can read it).

In this book I'll be describing a multitude of ways that you can help to secure your information and protect your privacy. Whether you choose to follow just a few of these methods or all of them is up to you and your personal situation and opinion on the matter of data privacy. Regardless of what you do, though, I urge you to carefully consider what you read and what you decide to do. As the Internet continues to change and evolve, the importance of data privacy and information security will continue to grow, not lessen.

II – Change Your Browsing Habits

Choosing the Right Browser

When I'm browsing the web, I use two browsers: Firefox and Google Chrome. I don't use anything else, except in cases where the website I'm visiting (and these are almost always government websites) won't work in anything except for Internet Explorer.

The reason I restrict myself to Firefox and Chrome is simple: they're relatively secure by themselves, and they support *plugins*, which can make them even more secure. Internet Explorer doesn't support plugins, and while other browsers might, Chrome and Firefox have the biggest share of developers creating and updating plugins for them. It just makes sense to use them.

While you don't need to install both Firefox and Chrome to get started on the path towards better browser security, each browser has its own advantages and disadvantages. Chrome tends to work faster than Firefox in my experience, though it tends to use up a lot of memory along the way. Firefox's memory usage has been lower than Chrome, but it's a bit slower than Chrome and isn't as flashy or modern feeling.

You can install Firefox and Chrome from the links at the top of this section, and you don't need to worry about them interfering with each other or with any other browsers on your computer. They may take a little bit of getting used to, but as you'll see, the security upgrades make them more than worth it.

Browser Plugins

Once you have Firefox and/or Chrome installed you'll be ready to get started with some browser plugins. These are little pieces of software that run inside the browser and change how it interacts with the Internet. For example, some plugins will prevent you from seeing advertisements on websites while other plugins will change how the browser displays text on certain pages. I've outlined a few plugins that you can install (along with installation links for both Chrome and Firefox) that will help you stay more secure online.

Advertisement Blocking (Firefox | Chrome)

Installing one of the myriad of ad-blocking plugins is always first on my list whenever I set up a new installation of Firefox or Chrome. The plugins that are linked above are my personal favorites, but you can search around and find different ones if you prefer.

The purpose of an ad-blocking plugin is simple: it keeps your browser from displaying ads from a known list of advertising sources. This has a number of positive effects. First, it reduces the load time of web pages, making them faster and snappier. It also reduces the amount of data your browser uses, which is critical for those who have small data plans. Ad blockers also reduce the risk of your computer being subjected to a 'hit-and-run' virus, where an attacker places a malicious advertisement on a webpage that forcers your browser to install it. This type of attack has grown more common as Internet advertising has reached new heights, and even hugely popular websites and ad services have not been immune to this type of attack. Take a look at the following two images from a popular news agency's website to see the startling difference between the page without and with an ad blocker in place.

Example of a page without an ad blocker

The exact same page, with an ad blocker

Ad blockers also help protect your privacy. How? Whenever ads load on a page, they usually set a cookie on your computer. This cookie can track you across multiple websites, and pass the information on what sites you're visiting back to the advertising company. This, in turn, can lead to a browsing experience that borders on the creepy. There have been instances where I've browsed online with my ad blocker disabled, and searched for a piece of software or a product I was looking at. Immediately after doing so, all of the advertisements I saw were for that product or competing products. This continued on for weeks after I had done my original search, too! What's worse is the data that is collected about your search and browsing habits is routinely shared and sold between companies, resulting in more comprehensive profiles being built, all behind the scenes where you can't see what's going on.

That type of intrusion and tracking doesn't sit well with me, which is why I don't like to browse the web without an ad blocker in place.

Flash Blocker (Firefox | Chrome)

Flash is a technology that's still widely used on the Internet despite the fact that it's woefully out of date. Flash is used for dynamic websites, videos, media consumption and even online games. In fact, online games are one of the largest places where Flash is used, because of how easy it is to develop games using Flash.

Unfortunately, Flash has become a large target for virus and malware writers in recent years. It's gotten so bad that technology executives have encouraged browser companies to ban Flash altogether. Due to how much Flash is integrated, though, this is unlikely to happen for some time, but you still need a way to stay protected when you're interacting with websites that have Flash content on them.

Enter a Flash blocker plugin. This plugin, when enabled, will automatically block any and all Flash content from being loaded in your browser. If you wish, you can selectively allow some Flash content to be enabled, but you should only do this if you trust it. Some examples of sites that still use flash are the streaming video site Twitch and the video site Youtube, both of which use Flash but which also have content that, for the most part, can be trusted.

Ghostery (Firefox | Chrome)

Ghostery is a plugin that fills in the gaps that ad-blocking and Flash-blocking plugins leave open. Remember how I talked about how advertisements on pages leave tracking cookies on your computer that follow you and record where you go on the Internet? Well, unfortunately, companies that deliver banner and video ads to your browser aren't the only companies that perform this tracking. There are a myriad of other tracking companies that exist solely to track and aggregate data on individuals browsing the web. Ad blocking plugins may block some of them, but not all of them.

A popular news website had 22 different trackers that Ghostery blocked!

That's where plugins like Ghostery come in. Ghostery has a database of hundreds upon hundreds of different companies that track you across the web. Anytime one of those sites tries to load a tracking cookie on your computer, Ghostery will block it and, as a bonus, alert you to the block. Smaller websites don't implement tracking technology as much as larger ones, but on larger websites you could easily see a few *dozen* tracking cookies get blocked by Ghostery whenever you visit a page.

Why, you might ask, would a website want to track you? It's pretty simple: money. Let's use an example of a fictitious online retailer called 'Gramazon' as an example. If Gramazon sells computers and computer parts, they will want to put advertisements on their website for computer related accessories and ensure that visitors to their site stick around to buy computers, right? If Gramazon starts

tracking its visitors, it can see things like what pages are the most popular, how many people leave before buying an item and if there are any pages that cause a large number of people to leave before buying something.

By using tracking technology, Gramazon can improve its website and make more money by selling more products to more users. Tracking companies might provide this type of service for free to Gramazon, but in exchange the tracking company would get to keep a profile of all of Gramazon's customers. This list could then be used by the tracking company to deliver ads to Gramazon's customers in the future for things that the tracking company knows they might want to buy. The result of this alliance is a win for both the store and for the tracking company, all while leaving the customer's privacy in shambles as a result.

A Word of Warning

As social media, tracking technologies and cookies become more and more integrated into modern websites, more cases are cropping up where websites don't work as intended if you use blocking plugins to get rid of ads, protect yourself from Flash vulnerabilities or block tracking websites. If you visit a site with any blocking plugins enabled and the site doesn't work like you'd expect, you might want to go somewhere else. If you can't or don't want to (which I completely understand; I do the same thing sometimes), then you can try disabling the blocking plugins for the site or page that you're on.

Most blocking plugins have an icon that they install in the upper right corner of your browser. If you click that icon, you can usually find an option to disable blocking on the page or website that you're on, or to temporarily turn off the blocking service altogether. Use caution when disabling blocking, though, as it's a key part of helping to protect yourself online, both against people who want to collect information about you and against nefarious parties who want to infect your computer with malicious software.

III – Habits to Stay Safe Online

If you’re browsing the web with a program like Firefox or Chrome and you’re using blocking plugins, you’re already much safer online. However, there’s still a *lot* more you should do to keep yourself and your data safe when you’re online.

Email

Free email services like Gmail and Hotmail have gotten quite good at filtering out spam emails, but there are still some that slip through, especially if you use a private email service that doesn't have advanced spam filters on it. Whether it's spam or specially crafted emails from a malicious person who wants to get access to your computer systems, you should remember one thing: use extreme caution when clicking on any links or opening any attachments in emails that you receive.

If you receive a link or an attachment from someone you don't know and aren't expecting, don't click or open it. Just delete the email and keep on going. If you receive an email or attachment from someone who you do know, you should contact that person via a non-email method to ensure that they sent the email. Now, I know what you're thinking right now, 'But James, that's crazy! I can't contact *everyone* I know who sends me an email!'

I agree, it sounds very over-the-top, which is why it's good to use some common sense and moderation. If you receive a ZIP file from a friend who you haven't talked to in a long time, it's a good idea to contact that person over the phone, by text message or some other way and make sure they actually sent the email. I've had more than a few emails sent to me from a person who I knew, but who never actually sent the emails. Instead, their email accounts were hacked, and the hackers sent emails to every person on their contact list. The emails included links to malicious websites that, if visited, would try to install malicious software on your computer.

If, on the other hand, you get a ZIP file from someone who you talk to on a regular basis and you know that they occasionally send you attachments, it's a little bit different. That's a situation where I would consider it perfectly fine to open the attachment (after doing a quick virus scan on it first, of course!) and see what's inside.

Web Browsing

Blocking plugins are great, but they can't protect you from everything. There are some types of dangers that blocking plugins can't block, and you need to be aware of them if you ever encounter them.

Have you ever gotten a popup in your browser telling you that you need to install some sort of update, usually for Flash or for some type of video player? These popups occur a lot on older expired domains that have been snatched up by authors of malicious software and they're designed for one purpose: to install adware or malware on your computer. If you click on the popup, your browser will download an EXE file to your computer. If you run this EXE file… well, you're in trouble. Most of the time these files contain an advertising package that will generate popup advertisements on your computer. Some, though, are more malicious and will collect your personal data (passwords, emails, bank account numbers and more) and send it off to someone in another country to use or sell. Remember: don't click on popups!

On a similar note, you should keep a close eye on the address (URL) bar of your browser. That's the bar at the top that tells you what page you're on. It's very common for malicious people to purchase domains that are *almost* like popular websites (like **faec**book.com instead of **face**book.com, for example). They then try to trick users into clicking through to these fake websites, which are designed to look like the real thing, except when you try to log in, your login credentials are stolen and used for nefarious purposes. This is extremely common with websites that deal with financial information, like banks or PayPal. Remember: always check the URL bar and make sure you're on the website you think you are before you enter in *any* information.

Lastly, you have the 'zero-day exploit.' Unfortunately, there's not much you can do against this type of exploit. The zero-day exploit is a type of exploit, usually in the web browser itself, or a piece of related software (Flash, Acrobat or your computer's very own operating system) that was discovered very recently and has not yet been patched. Exploits like these can be used virtually anywhere, and they're nearly impossible to defend against until they're patched. So how can you avoid them? The best course of action is to ensure that you keep your operating system and all related software patched and updated on a regular basis (we'll talk about this in the next chapter).

You can also practice caution when choosing what websites you go to. Just like in the real world, there are portions of the web that are inherently more dangerous

than others. Websites that claim to offer free pirated software, TV shows or movies are perfect targets for zero-day exploits, popup downloads and other malicious attacks. Try to avoid websites that feel ‘off’ to you; remember: if something sounds too good to be true, I can promise you that it most certainly is.

IV – Securing Your Operating System & Software

A significant number of threats compromise systems due to a combination of negligence and software that is not up to date. Now that we've talked about some good habits to develop when using the web, let's talk about the other side: keeping your computer's operating system and software up to date.

Update Your Operating System

Most readers of this book will undoubtedly be using either the Windows or Mac operating systems. (If you're using Linux, you likely already know how to update your operating system, so we're going to stick with covering Windows with a bit of Mac as well.) Both of these operating systems have automatic update programs built in which you should take full advantage of. Whenever your computer tells you that an update is available, you should apply the update as soon as possible.

Updating the Mac OS X operating system can be done both manually and automatically, and Apple has a great support article that details how both of these actions can be performed. If you use a Mac, you should become familiar with how to update the operating system through this article on Apple's website.

Likewise, the Windows operating systems have manual and automatic update support built in. If you're using Windows 7, 8 or 10, you can check for updates and turn automatic updating on by following Microsoft's instructions at this support link.

While having automatic updates turned on can cause your computer to reboot at inopportune times, I'm personally in favor of leaving it enabled. The inconvenience of dealing with your computer rebooting on its own to apply updates is small compared to having an operating system that is out of date and vulnerable to attacks. My only caveat to this is if you're very strict about checking for and applying updates on your own. If you're willing to stay on top of checking for and installing updates *at least* once per week, then turning off automatic updates should be fine.

Individual Software Updates

While following Apple and Microsoft's update instructions will help keep your computer's operating system secure from malicious attacks, the operating system is only one vector for attacks on your computer. Each piece of software that you install introduces another potential vulnerability on your computer, particularly if the software package interacts with the Internet in any shape or form. Web browsers, email clients, accounting software and more are all potential ways for attackers to break into your computer.

If you'll recall the discussion in the last chapter about 'zero-day' vulnerabilities, that discussion is applicable here. Zero-day vulnerabilities can be discovered in operating systems, but they are most commonly discovered in other software packages. Internet browser vulnerabilities are some of the most highly prized by hackers, as they offer a direct way for malicious users to access the data on your computer since virtually everyone who uses a computer uses an Internet browser of some sort.

So what can you do? **Keep your software up to date**. Whenever a piece of software prompts you that a security or other update is available, back up your data and then upgrade the software. Running out-of-date software packages is one of the top ways to have your information compromised on the Internet. All it takes is one vulnerability in a program to be exploited and all of the data on your computer is potentially compromised.

On the flipside it's important to be mindful of the updates you apply. Some updates, while well-meaning, may cause unexpected issues on your computer. I had a problem like this just a few days ago when I went to upgrade my email client to the latest version. After updating the client, I discovered that it no longer functioned properly, so I had to revert back to the previous version. I feel comfortable in doing this due to the fact that the latest version was more focused on feature improvements instead of security fixes, but there may be cases where you have to weigh functionality versus security.

In those cases, I recommend falling back on your common sense. If a software upgrade is known to cause issues, hold back on applying the update, but pay more attention to how you use the software. Use caution when accessing the web, opening files or uploading data with the application. If you try your best to stay safe when you use programs that access the Internet, you'll usually be just fine.

V – Password Safety

Passwords are often the only thing standing the between your data and the world at large. They’re used for accessing your money, your computer, your tax records and your medical information. For something so vitally important to virtually every computer user, passwords are often the weak link when it comes to computer security. Why is this, and why does password security seem to be so hard to carry out properly? Let’s discuss how proper password safety can be both easy and secure at the same time, if you know how to do it correctly.

Choosing & Securing Your Passwords

There have been mixed schools of thought about how to properly choose and secure your passwords. Some people believe that you need to make up passwords that are easy for you to remember, but hard for others to guess, and just remember them in your head. While this is a valid approach, it becomes cumbersome once you move beyond just a few passwords.

Why not use the same password for every website, you ask? Unfortunately, that's one of the worst possible things you can do. If your account password on one website is compromised due to your computer being hacked or the website you signed up with being hacked, you have a huge problem on your hands. Instead of having to deal with just one account being compromised, all of your accounts on every other website are potentially in trouble too. This is because hackers, upon breaking in and stealing a list of passwords and usernames from one website, will use those login details to try to get into many other sites on the web. If you use the same password on every site, then you can quickly have more and more accounts compromised.

So what's the solution? Well, you can either keep potentially dozens or more passwords memorized and try to recall them all when needed, or you can use a simple piece of software to do it all for you: a password manager. A good password manager is an invaluable piece of software, and one that you'll want to use for the rest of your life (or at least until passwords aren't necessary anymore). A password manager stores your account usernames and passwords in an *encrypted* file. This encrypted file is then locked with a single master password that you use to access it. Without the master password, the file is literally *impossible* to open. This has the effect of storing all of your website, account and other passwords in a safe and secure place that only you can access.

Let me tell you how I use my password manager of choice, KeePass. If you don't like KeePass, you can try Password Safe, but these are the only two password managers I recommend. **I highly recommend that you do NOT use a password manager that stores passwords in the 'cloud.'** I don't care how secure these services claim to be, or what type of encryption technology they use; transmitting or storing your passwords on the Internet through a third party is, in my opinion, a *terrible* idea. All it would take is for one of these high value (and thusly, highly targeted) services to be compromised, and tens of thousands of people's passwords could become exposed, resulting in a huge amount of privacy, data and monetary losses. This hasn't happened on a large scale yet, but I certainly don't want to be someone who's caught up in the very first instance; do you?

Anyway, back to how I use KeePass. When I first set up my KeePass password file, I thought up a password that is over 50 characters long. It's a string of words, numbers and symbols that I took a few days to memorize, and which forms a long sentence that I can easily remember. This is the master password for my file. Without it, no one can access the hundreds of passwords I have stored inside my KeePass file.

With my KeePass file secured, I then face the question of what to do when I sign up for a service. Well, the cool thing about a password manager like KeePass is that it has a password generator built right in. So, whenever I sign up for a service, I choose my username or email (more on securing this in the next section), and then let my password manager randomly generate a password for me. **This means that I never actually know the password for any service I sign up with, which is incredibly secure**. Whenever I go to sign in to an account on the web, I just copy and paste the password from KeePass (which clears out the contents of my clipboard a few seconds later) and I'm logged in and ready to go.

With a password manager, all of my accounts are secured with different, randomly generated passwords that are *very* secure, and they're protected in a file that can't be accessed without the master password, which only I know. This method of password securing is one of—if not *the*—most secure ways to keep your online accounts protected, secured and isolated from each other.

If you don't use a password manager today, you should start doing so *immediately*. I know, it may seem cumbersome at times, but what's worse, spending a few extra seconds to copy and paste a password from your password manager, or potentially losing multiple accounts to hackers because you used the same password in multiple places? The random password generation and protected storage offered by password managers like KeePass and Password Safe is invaluable, and in my opinion it is the best tool you can have in your arsenal to defend your privacy online.

Username Security

We touched on this briefly in the last section, but it's something important enough to be discussed on its own. Remember how we talked about how important it is to use a different password for each account you sign up for online? Well, the same is true for the email address or username you use to sign up for online accounts as well. Like using the same password, if you use the same username for every account you sign up for, if one account is hacked, all of your other accounts are at a much greater risk due to the fact that you used the same username across all of the accounts. That type of link makes it trivial for hackers to run automated software that tries to login to your accounts on other services, leading to potential compromises. If your Twitter account is compromised, do you really want it to be easy for hackers to log into your credit card or bank account? If you use the same username and/or password on both accounts, that's exactly what you're doing, making it easy for hackers to do what they do.

If you're using a password manager to create different passwords for each service, you're doing great so far, but let's take it to the next level and use different usernames as well. For services that don't use an email address as a username, this is easy: just sign up with a different username on each service. Add numbers or letters to the end of a username you like to make them slightly different. Or, if you're like me, come up with totally different username for each service.

When it comes to email-based, then it gets a bit trickier. Some email services, like email, use a **plus** system that lets you create a new email address whenever you want. It works like this: suppose your email address at Gmail is **myaccount@gmail.com**. If you send an email to **myaccount+purple@gmail.com**, that mail will go straight into your inbox. Likewise, if you send an email to **myaccount+gosportsteam@gmail.com**, that too will go straight into your inbox. Gmail has a special filter that is uses, where anything after the "+" is essentially ignored.

How is this important? Well, for starters, it means you can easily 'create' a 'new' email address for every account you sign up with. If I sign up on Amazon, I could sign up with **myaccount+amazon@gmail.com**. Then if I sign up for Facebook, I could sign up with **myaccount+facebook@gmail.com**. Then I could sign up for other sites, too, like **myaccount+twitter@gmail.com, myaccount+yahoo@gmail.com** and on and on. All of those 'new' emails will all go directly to my **myaccount@gmail.com** email address, but each one is different (fulfilling our need to have a different username for each account we sign up with).

There’s another bonus to this system beyond security that I absolutely adore: spam filtering. Some services will sell your email address to spammers, and if you use the exact same email for every service, it’s nigh-on impossible to determine who actually sold your email. If you use the “+” system I’ve described, though, then you can quickly figure out that it was **abadcompany.com** that’s spamming you when you start receiving spam emails that are addressed to **myaccount+abadcompany@gmail.com** in your inbox. You could then set up a Gmail filter to automatically delete any emails sent to **myaccount+abadcompany@gmail.com** and that source of spam would be cut off, but all of your other account emails would keep coming through just fine.

Other email services may or may not include this type of aliasing, but Gmail does it best. If you don’t have a Gmail account, they’re free, and I strongly recommend that you sign up for one and use it for this type of thing. If you have a privately hosted email service, you can also ask your administrator to set up a ‘catch-all’ email address, that will forward anything sent to your email domain directly to your inbox. I use private email for most of my accounts, so whenever I sign up for an account I use the format of **websitename@mydomain.com** for my accounts. I can quickly filter, delete and organize all of my different Internet account emails this way and cut down on the amount of spam and fluff that I get all at the same time.

Two-Factor Authentication

Two-factor authentication is an advanced security technique that is incredibly powerful in helping to protect users' accounts from being individually compromised. One-factor authentication typically relies upon something a person knows, such as their username and password. Two-factor authentication relies upon both something a user knows *and* something the users possesses. In two-factor authentication, a user typically uses a username and password to begin their login process, then inputs a security code provided to them by the website they are logging in to.

For example, if you set up two-factor authentication in Gmail, you will no longer be able to log in to your account with just your email address and password. Instead, you'll need your email and password along with a special code that will be sent to you over the phone (voice call or text message). This helps to protect your account by ensuring that even if someone obtains your password, they wouldn't be able to log into your account without also having access to your phone as well.

Two-factor authentication is available in many different areas, though it's typically only available from larger companies or websites that can afford the advanced infrastructure required to support it. The website TwoFactorAuth.org has a list of companies that support two-factor authentication, including what types they support. Many companies offer two-factor authentication support through phone calls, text messages or apps on your smartphone or tablet, while some offer dedicated hardware tokens.

Two-factor authentication adds a layer of complexity to your Internet browsing that may seem daunting, annoying or unnecessary. However, the level of security it adds is incredible, especially for any websites or accounts that have interactions with something valuable, such as sensitive data or money. I use two-factor authentication for all of my email accounts that support it along with my bank, and you should as well.

VI – Data Backups

At first glance, the idea of backing up your data may not sound like it’s related to your privacy and security on the Internet. Properly done, however, data backups are an essential part of ensuring your security and keeping your information safe. They function as a partner to other data protection techniques, and are a crucial part of any serious data security and privacy plan.

Protection Against Disasters

If you’re like an increasing number of people today, your entire life is contained in your computer. Pictures, emails, documents, financial records and more are all stored on our computers, and the amount of personal information we keep both in our computers and with third-parties is only growing with each passing day. For this reason it’s important to keep backups of your data on an external location from your computer, such as an external drive or another computer. If something tragic occurs and your computer’s hard disk is damaged or destroyed in a fire, flood or even something as simple as a hardware failure, having a recent backup of your data will allow you to quickly recover and get back to normal.

Local or Cloud Backups

Cloud backup services offer a *lot* of advantages over traditional local backups. With traditional local backups, you can perform them manually by copying files over to an external drive, or you can set up an automated piece of software that backs up your data to an external drive or location. Cloud backups, on the other hand, usually involved an automated process that backs up your data not to a private computer, but to a server owned by the backup company. Your data is compressed and stored online, ready for you to access and download whenever you want, wherever you want.

If this sounds like a fantastic idea, then I completely agree with you! However, there is a problem with these types of cloud backup solutions: privacy and security. As we've learned over the years, no one is completely safe from having their data compromised, including large companies. There have been a large number of companies both big and small in the news because their data has been compromised. Everything from customer lists to internal employee emails to names, emails, social security numbers and more has been exposed by malicious hackers.

For this reason, I prefer to manage my backups on my own instead of entrusting my data to a third party. Of course there is some data that you have to trust to some companies, but I take care of my computer backups myself. Using external hard drives, manual backups and automated backup software, I can create weekly backups of my data along with daily and hourly backups. With three separate drives that I rotate through, I ensure that two of them are always at a different location (one at my office and one in a bank safety deposit box, and both are encrypted using the techniques described in chapter seven). That way, if something were to happen to my computer, I would only lose a week's worth of data at worst, and in general I can expect to lose only a day or hour's worth of data. This method also ensures that I don't have to worry about my data being exposed should a cloud backup company be compromised.

But what about companies that encrypt your data before backing it up, you might ask. If you've already read the next chapter, you'll know what a great tool encryption is. The problem I have with cloud backup companies, even those that claim to encrypt your data before it's stored on their servers, is that I have to trust them with a huge portion of my life. I have to trust that their encryption methods are secure, I have to trust that there are no flaws in their procedure and I have to trust that they never get hacked and that the encryption scheme they use is never hacked, either. For me, personally, that doesn't sit well. I like to be in control of my information and I like to take charge of my privacy and security.

If you wanted to make use of a cloud backup system, my advice would be to use the encryption techniques from the next chapter to make encrypted folders that you periodically back your data up into. Then, instead of uploading your individual folders and files to a backup service, only upload your encrypted file containers. That way, everything you upload and store with the third party was encrypted by *you*, and you can therefore be confident that it’s safe.

Good Backup Strategies

If you decide to implement a backup strategy, you should spend some time thinking about what type of strategy to take. Some people prefer a monthly strategy, where they back up their data once every month. Some prefer to make weekly backups, some prefer daily backups and there are those that make backups multiple times per day.

How often you back up your data will depend on two factors: how many changes to your data occur in a given timeframe and how much data you're willing to lose if your computer were to go through a catastrophic event (theft, destruction, hardware failure, etc.).

For the first factor, consider how much information you create and how much of your current data you modify on a daily or weekly basis. If you only get a few emails every day and create a new document every few days, hourly or even daily backups are almost certainly too frequent to matter to you. If, however, you create or edit many files every day, then daily or perhaps even hourly backups are the way you should go.

Secondly, consider what you would do if your computer were to vanish right now, and all you had left was your last backup. If that backup was made a month ago, would you be comfortable with losing the last months' worth of data? What if your last backup was a week ago or yesterday? If your computer's hard drive is destroyed or stolen, the fact of the matter is that you will lose *something*. The question then becomes how much are you comfortable with losing? Once you've identified the answer to this question and the previous one you now know how often your backups should be made.

Don't be afraid to back up different segments of your data in different frequencies. If you have a chunk of data in a folder that doesn't change often, consider backing that folder up once per month. If you have another chunk that changes quite often, perhaps an hourly backup would be best for that. I use this strategy to segregate my backups into weekly, daily and hourly ones and it works very well.

Backup Software

Explaining the intricacies of setting up even one piece of backup software is beyond the scope of this book, and an entire book could be written about each different piece of backup software I'm going to suggest to you here. Some backup software is more complicated to set up than others, but as long as the solution you choose successfully creates backups of your data the way that you want, that's all that matters.

Acronis True Image is the non-cloud backup solution from Acronis. It supports Windows XP, 7, 8 and 10, along with recent Mac OS X versions. It lets you back up everything from individual files to your entire computer, all to an external hard drive or network-attached storage device. Acronis is easy to use and simple to set up, and guides you through the entire backup setup process.

My personal backup software choice is an open-source piece of software called Areca, which runs on the Windows operating system. Areca is not simple to set up, but it is powerful. You can schedule backups on the frequency that you want, and you can back up files to hard disks, external hard drives or even remote computers if you wish to make remote backups of your data. If you choose to go with Areca, I suggest that you read through the tutorials for it to get a sense of how to best operate the software.

Mac OS X has a built-in option called Time Machine that lets you make backups of your data. Likewise, Windows Backup is a built-in option for Windows 7 and above that will let you make backups of your data.

VII – Advanced Data Protection Procedures

While what we've discussed so far in this book will help anyone become safer and more secure both online and offline, there are many more advanced techniques that you can take advantage of as well. These techniques may not be something that casual users want to implement, but regardless of whether you do or not, it's good to familiarize yourself with them anyway. The more informed you are, the better decisions you can make, and you'll be aware of what risks you are and aren't taking.

Encryption

Simply put, encryption is the be-all and end-all security precaution. When implemented properly, encrypted files cannot be accessed through any method except through a password (called the *encryption key*) that unlocks the data. Think of encryption as an unbreakable box with a lock on it. Anything you put in that box will be completely secure and inaccessible to anyone except those who have the key to the lock. You can encrypt virtually whatever data you want, including your emails, your files and even the entire contents of your computer hard disk.

There are a few reasons why more people don't use encryption. One of the largest reasons is that it's somewhat inconvenient and uncomfortable to implement and deal with on a daily basis. I keep my computers encrypted at the disk-level, which means that I can't even get my operating system to boot up until the proper password is entered. This ensures that *everything* on my computer is protected and kept safe from anyone who might, for example, break in and steal my computer's hard drive. Without the password, all of the data on the drive will stay locked up *forever* and be inaccessible to the thief.

Another reason people don't use encryption is because there are some groups who strongly dislike encryption and what it represents. There are strong political lobbies in various regions (including the USA, UK and beyond) that are fighting strongly against allowing encryption to continue to be available to the general public. The reason for this is simple: if everyone encrypted their data, then it would be *much* more difficult for governments to spy on that data.

Encryption is also potentially dangerous, due to the fact that the encryption key is the only way to access the data. If you forget the encryption key for something you've encrypted, there's no way to access that data. In fact, until *huge* advances are made in computing technology, it would take *longer than the life of the universe* to break encryption that is implemented today. If you decide to implement encryption at any level, be aware of this fact, and know that if you forget your encryption key, there's nothing that anyone can do to break the encryption.

Note that this discussion about 'unbreakable' encryption assumes that when you encrypt something, you choose a complex password, like we discussed in an earlier chapter when talking about password managers. If you use a simple password, such as your name, a variation of the word 'password' or something

similar, then it's possible to quickly *brute force* the password. This involves using a piece of software to quickly try millions of combinations of different letters, words and numbers to guess what weak passwords are being used to secure the encrypted data. (Side note: this *brute force* method is also how many online accounts are compromised, which is another great reason for why you should always choose a strong password for your online accounts.)

There are several different encryption software packages, but before we go through a short list, I want to reiterate the dangers of file encryption one last time. **If you encrypt your data improperly or you forget your encryption key, your data will be lost *forever*. Make sure you have a full backup of your data somewhere else before you encrypt files or your entire disk on your computer. That way, if something goes wrong, you still have your data. After you finish the encryption and are comfortable with it, you can delete this backup, but until then I strongly recommend that you keep it**.

Okay, with that disclaimer out of the way, here are my suggestions for encryption software packages that you can try. My top pick and the one I use personally is VeraCrypt, which is open source and came out of the TrueCrypt project. It supports both full-disk and file container encryption, meaning that you can either encrypt your entire computer, or you can create a virtual hard drive that acts as a container to hold files. When the container is locked, it's encrypted and appears like a file on your computer. When unlocked, it appears as a hard disk on your machine and can be accessed like one.

Bitlocker is another choice that is included with modern Windows operating systems, and is baked into the Windows operating system itself. There is no small amount of controversy regarding Bitlocker due to allegations that it's not as secure as other encryption software suites. In my personal opinion it's a much better solution than no encryption, at least for the average user who doesn't want to have to deal with the nitty gritty aspects of encryption and just wants their data to be secured.

Symantec also makes some pretty good encryption software, though it's targeted more towards businesses than individuals. Their software encryption suites don't just cover file and disk encryption, but also email encryption as well. If you work in a business that deals with sensitive information, Symantec is a great place to start.

VPNs

A VPN (Virtual Private Network) is a great tool for helping you to protect your privacy on the web by hiding your IP address from websites that you visit and other services you use. Here's how.

When you connect to a website, the connection goes from your computer through your ISP (Comcast, Time Warner, Verizon, etc.), through a few intermediate steps until it reaches the website you want to reach. This is a direct connection to the Internet, and is what most people have. It allows the website you're connecting to (along with every other location that your connection jumps through) to see your personal IP address. If a website, service or other entity wants to track your actions on the web, it's very easy to do so by using this address.

If, however, you use a VPN, then the connection out to the web is much different. Once your connection reaches your ISP, it routes to the VPN before traveling out to the website that you want to visit. The website or service that you're connecting to sees the connection as coming from the VPN, not your personal computer, and thus can't associate the visit with your computer's IP address. Many public VPN services use what are called *shared IP addresses*, which means that everyone who uses the VPN appears to be using the same IP address when they connect out to the web. With so many different connections coming from the same IP it becomes nearly impossible to track people as they browse across the web, since all of the connections appear to be coming from the same location.

VPNs have another benefit related to where in the world you're physically located. Many services use geolocation (where you are in the world) to restrict what content you can read, watch and listen to. Some videos on Youtube, for example, can only be viewed by people inside the USA. These types of restrictions are done in real time based on the IP address of the visitor, which can be used to tell what country, state and city you're in. Because a VPN effectively hides your home IP and makes it appear as though you're accessing the Internet from the IP address of the VPN, you can access geography-restricted content by accessing the content through a VPN that has an IP address in the appropriate country. For example, if you live in Mexico and wanted to view a video that's restricted to USA residents, you could connect to a USA VPN and then view the video, because as far as the video service is concerned, you *are* a USA resident due to your IP address being that of the VPN.

My two favorite VPN providers that have IP addresses in multiple countries across the world are SaferVPN and StrongVPN. I use both services and have had a great

experience with both, so it’s up to you to decide which one you want to use based on what each service provides and the differently-priced packages they offer. If a VPN sounds like something that would be useful to you, I would encourage you to check out these and other VPN services on your own to see what they have to offer.

VIII – Wrapping it All Up

We've covered a lot in this book, and I'm hopeful that it was both educational and useful! We've talked about how to keep yourself and your data safe from all types of attacks, as well as basic and advanced methods you can use to keep your data safe, secure and protected. Armed with this new knowledge, you should feel confident and well-equipped to start securing yourself when you go online. Don't forget, though, security is an ever-evolving art form. I encourage you to spend some time every week reading about new security breaches that have taken place, researching new browser plugins to further secure your data and putting into practice what you've read in this book.

If you enjoyed this book and found it helpful, please do consider leaving a review for it at Amazon. Reviews are one of the best ways readers find new books, and sharing your experience with other potential readers would be of great value to me.

If you'd like to stay up to date with some great free tech books, I encourage you to sign up for the AppSna.gr newsletter right here. I've partnered with them to offer my books for free through their book giveaway program, so each time I write a new book, review copies are randomly given out to dozens of folks who are subscribed to the newsletter.