

# How to Fix Your Privacy

v1.1, last updated April 29th, 2021.

*Keep in mind that I'm an enthusiast putting together the information I've come across. I'm not an expert. Always double-check your information.*

The modern internet is a privacy nightmare.

You might have some idea of how bad the internet's privacy is by default if you're taking the time to read this- privacy guides don't tend to fall into people's laps, and you got here somehow. If you aren't familiar, here's a quick rundown of some of the bigger issues:

- Your web browser and search engine are both spying on you and sending data to various third parties; by default, most have very bad privacy policies and settings. If you use Chrome, [your browser is pretty much blatant spyware](#). If you use Firefox, the situation is better but still not great- Mozilla does collect usage data, meaning that they see what sites you visit, what you do on them, and [otherwise have access to your activities](#) if you haven't taken steps to stop that. If you use another browser, it's generally not going to be good for your privacy unless you've taken particular care selecting it with privacy in mind.
- Google is a [privacy hellhole](#) (of particular note in that link: "Your identity is used in ads that are shown to other users" and "They store data on you even if you did not interact with the service"). [Bing is just as bad](#). Most large companies are horrible at respecting your privacy, and this is a common problem. [Even "privacy-friendly" services track you decently often](#).
- If you're using Windows or MacOS and have accepted the terms and conditions, your computer sends information about what you do on it back to [Microsoft](#) or [Apple](#) respectively.
- If you use Windows 10, your computer [also has built-in advertisements](#).
- Most websites can see where you're coming from and where you're leaving to, and most use cookies and trackers to collect data on you. It's entirely possible that Twitter knows you use Tumblr, and it will use that information to send you targeted advertisements. It doesn't help that many major websites [have horrible privacy policies](#).

Without doing anything to protect your privacy, your data is fully exposed to the internet- but why should you care? Surely you have nothing to hide.

Think of it like this. You don't want strangers to know all of your logins. You don't want to let them tweet whatever they want from your account, or hand them your bank account's login details. You don't want a total stranger knowing where you live, where you work, and when you're not home. You need privacy to protect all that information, even if you have nothing else to hide.

Even if you can't completely escape the privacy hell that is the internet, you can improve your privacy barriers and make your browsing harder to track. If Google wants your information, they're going to have to fight you for it.

## Table of Contents

- [Operating Systems](#)
- [Web Browsers](#)
  - o [Neutering Firefox](#)
  - o [Extensions and Plugins](#)
- [Search Engines](#)
- [Passwords](#)
- [VPNs](#)
- [De-Googleing](#)
- [Other Privacy Tips](#)
- [Security](#)
  - o [General Security Advice](#)
  - o [Encryption](#)
  - o [Virus Protection](#)
  - o [Jailing and Sandboxing Programs](#)
  - o [Other Resources](#)

## Operating Systems

First things first: if it's at all possible for you, give Linux or BSD a try and get away from Microsoft and Apple. There are plenty of other free options out there that will respect your privacy, and personal data collection really shouldn't be baked into your OS.

That said, not everyone can get away from Windows or MacOS. Unfortunately, software support for Linux and BSD isn't quite there yet, though it's certainly improving, and some programs can still only be run on Windows (Mac-specific software tends to be more compatible with Linux as far as I'm aware). If you have hardware compatibility issues, that's another problem- while most hardware is compatible with Linux, a few parts might have problems or need you to track down drivers for them (looking at you, NVIDIA). Luckily, odds are that someone else has already done the legwork, and a quick search will turn up results on how to get things working. There are ways around software compatibility issues as well in many cases (e.g. running Windows/MacOS in a virtual machine on a Linux host, or using Wine to run Windows programs on Linux), but there are a few things that just won't work on Linux.

If you have to use Windows, you can find a guide to disabling telemetry (data collection) [here](#). If you have to use MacOS, look into disabling .NET telemetry and look for other forms of data collection.

At the end of the day it's up to you whether your privacy or your OS matters most if you're in this situation- sometimes the operating system wins out. That doesn't mean you can't still improve your privacy! The rest of the advice in this guide will usually still apply on other operating systems, and what operating system you use should be entirely your choice.

Unfortunately, I don't know enough about BSD operating systems to make any recommendations, though [OpenBSD](#) and [FreeBSD](#) seem popular. If you decide to switch to Linux, I can recommend a few different Linux distributions. In no particular order:

- [Pop\\_OS!](#): Great for beginners and maintained by System76, who are making some excellent decisions about privacy in their products. Pop is a great introduction to Linux and works brilliantly right after install- even NVIDIA drivers have built-in support. It also has great support for gaming and most applications, and its GUI tools make installing programs a breeze if you're not used to the command line.

- [Fedora](#) is a popular rolling-release distribution developed by Red Hat. By default, it only uses open source repositories, though you can add proprietary repositories if you want. It has built-in containers and virtualization, and it's particularly popular with developers.
- [Debian](#) is a rock-solid distribution known for its stability and excellent support for different packages. It's secure and is used for servers as well as desktops, making it rather versatile. It's also community-run, so Debian is a good option if you don't want a distribution linked to a commercial entity. Debian is commonly said to "just work."
- [Arch Linux](#): A community-run rolling release distribution known for its minimalist philosophy. If you want a lot of control over your computer and don't mind doing some serious reading, give Arch a go. The installation can be intimidating, but there's a [detailed guide](#) on the wiki and you'll be just fine if you take your time and read carefully (don't forget to install a networking tool!). You will have to do more things manually, but you'll learn quite a lot about your computer in the process and odds are you'll become an expert on your device. Arch also has an excellent package manager, [wiki](#), and access to the [AUR](#), both of which are major draws to the distribution. If you don't like systemd, [Artix](#) is Arch but with other inits.
- [Manjaro](#): A beginner's introduction to Arch Linux that makes the installation relatively easy. It has Arch's excellent package manager and access to the AUR (though use it with care on Manjaro, as support isn't great for the AUR and packages may break). In my experience, it breaks more often than Arch itself does, but it's also much faster and easier to install. [EndeavorOS](#) is also a good option if you want a pre-built Arch derivative.
- [Tails](#): If you really, really care about security and privacy and are willing to make some sacrifices, Tails might be what you're looking for. It runs off a USB and performs all networking through the TOR network, which anonymizes you quite effectively. It also comes with tools for online security. If you want a version without systemd that doesn't use any proprietary software, [Heads](#) might be a good option for you.

## Web Browsers

Stop using Chrome.

No, really. Drop Chrome immediately. Drop Chromium as well. Chrome itself is by far the worst privacy offender when it comes to web browsers, and using something different will already be a substantial improvement. [Chromium is also still connected to Google](#), though less overtly. If you *have* to use a Chromium-based browser, use [Ungoogled-Chromium](#), but ideally you should migrate to a different family of browsers entirely.

Before you ask, [incognito mode won't protect you much at all](#) and isn't a viable alternative to finding a better browser. It's better than nothing, but your data is still making its way back to Google as you browse the web.

If you don't mind [doing some work](#) to fix the privacy defaults, [Firefox](#) isn't a bad option. By default, it sends data back to Mozilla, but you can disable that with a little effort. Unfortunately, there's no guarantee that your settings won't be overwritten or worked around with a new update, so you might want to check on your changes now and then and see if anything new needs tweaking. You also have to be willing to trust that Mozilla isn't horrible if they do get your data, but there's [plenty of information out there on various privacy issues they've had](#) (link is highly opinionated but well-documented).

You could also go with a Firefox derivative- [GNU Icecat](#) is a good option, but binaries aren't distributed for Windows or MacOS. [Librewolf](#) is another good derivative, and it's essentially the Ungoogled-Chromium of Firefox. It comes pre-built for Linux, but [experimental binaries](#) are available for Windows users. [Mac users can still download it](#), but it has to be compiled or installed from disk. [Don't use Waterfox](#). It spies on you just as much as Firefox does, if not more.

If you're willing to sacrifice a little convenience or speed, there are a few niche browsers that have much better privacy settings with much less work. [Tor](#) is as secure as it gets- your data is encrypted, routed through several other computers to anonymize it, and then decrypted when it reaches its destination. Unfortunately, this also makes Tor extremely slow and not suitable for casual browsing; it's better for visiting particularly privacy-disrespecting websites or doing anything sensitive. [Qutebrowser](#) comes with no telemetry and I've seen it recommended many

times, but it has a very minimal GUI and is keyboard-focused rather than mouse-focused, so it may take some adjustment. [WebBrowser](#) is very similar to Firefox visually and comes with no telemetry, but it has to be compiled (which isn't too difficult but does take time; it took about an hour on a low-mid laptop). [Lynx](#) is as minimal as it gets and respects privacy very well, but it's text-only and runs in the terminal.

For the average user, going to the effort to make Firefox or a derivative respect your privacy is probably the best bet, followed by learning Qutebrowser or compiling WebBrowser. I personally use WebBrowser with a few plugins that further enhance privacy: more on that later.

Want to test how much web trackers can see? [Here's](#) a site that tests exactly that.

## Neutering Firefox

If you're going to use Firefox, you're going to want to change quite a few settings. Start in the regular settings menu and go through all the options, turning off anything that could send data back to Mozilla. Once you've done that, you need to change the settings that aren't so easy to get to. You won't find these settings in the settings menu; instead, you can get to them by typing `about:config` into your url bar. Firefox will warn you that it may be dangerous to access these settings, and it's right in that you can break the browser if you mess with the wrong ones, but you won't be doing anything that will break it. All you're doing is disabling telemetry and shoring up your privacy.

Before you go in and change settings by hand, you might want to make use of a web tool called [Firefox Profilemaker](#) that makes this process much easier. You'll still need to check settings, but this will do most of the work for you and should save you some time. The tool helps you to create a Firefox profile file with the settings you want, and then provides instructions on where to put that file. You could also download [arkenfox.js](#), a premade profile designed to harden and secure Firefox as much as possible.

It's worth checking these `about:config` settings on browsers other than Firefox as well; many of them share the same or similar options, and it's a good way to see how much the browser actually respects your privacy by default.

Here are the key settings you'll want to check/change, what they do, and what you're going to change them to:

- **beacon.enabled = false**
  - Disables sending extra analytics and information to web servers.
- **browser.safebrowsing.downloads.remote.enabled = false**
  - Stops your browser from sending information about .exe files you download to Google to scan them for viruses; while disabling this stops Google from seeing what you download, it does raise your risk of downloading an infected file. Basic web safety practices should be keeping you safe from risky files anyway, but think this setting through and decide whether you care more about keeping data away from Google or having one extra layer of virus protection.
- **browser.send\_pings = false**
  - This attribute is often used to track clicks on a website, which can be used to reconstruct what you were doing while you were there.
- **browser.sessionstore.privacy\_level = 2**
  - This tells your browser when to store extra information about a session: things like what was entered into a form and where your scroll bar is. Should be turned off because form entry information includes your passwords, making this a security risk. A 2 turns this off completely, while a 0 tells the browser to always store this information, and a 1 tells it to only store this information for unencrypted (HTTP) sites.
- **browser.urlbar.speculativeConnect.enabled = false**
  - Normally, Firefox connects to all of the websites it suggests to you in the search bar even if you don't end up visiting them. This is a bad thing because those websites come with all of their tracking, cookies, and surveillance. It doesn't save much time to pre-connect like this, just a few milliseconds, so you shouldn't miss it.
- **dom.event.clipboardevents.enabled = false**
  - Stops websites from seeing what you copy and paste on them, which also stops them from adding onto what you copy. This may break features of some websites (Neocities, for example, wouldn't copy anything properly), but on most sites you won't miss it.

- **media.eme.enabled = false**
  - Stops DRM-controlled media from playing. Why turn it off? That media automatically downloads a module from Google, and Google has a track record of being horrible for your privacy. I've yet to see this setting break anything.
- **media.gmp-widevinecdm.enabled = false**
  - Disables the Google DRM module.
- **media.navigator.enabled = false**
  - Stops websites from seeing whether your camera and microphone are enabled.
- **network.cookie.cookieBehavior = 1**
  - Disables third-party cookies! Setting this to 2 blocks all cookies by default, and setting it to 0 allows all cookies by default. If you want to be extra-private, set this to 2, but be aware that some websites may break. Using [extensions](#) to block first-party cookies unless you allow them can be a better option.
- **network.dns.disablePrefetch = true , network.dns.disablePrefetchFromHTTPS = true , network.predictor.enabled = false , network.predictor.enable-prefetch = false , network.prefetch-next = false**
  - All of these together disable prefetching, which lets your browser download the contents of a website before you visit it (including cookies and trackers). It doesn't speed things up much to leave prefetching on, so it's better to turn it off for the privacy improvements.
- **network.http.referer.XOriginPolicy = 2**
  - Stops websites from knowing where you came from before getting there if it comes from somewhere outside of that website. A 0 always lets them know, and a 1 lets them know only if they have the same [eTLD](#).
- **network.http.referer.XOriginTrimmingPolicy = 2**
  - Limits what information a website gets about where you came from.
- **network.IDN\_show\_punycode = true**
  - Makes it easier to notice phishing attacks.
- **privacy.firstparty.isolate = true**
  - Isolates a website so that other websites' cookies and trackers will have a much harder time reaching it; in short, it helps prevent tracking between websites.
- **privacy.resistFingerprinting = true**



- Makes it harder for websites to figure out the details of what kind of browser and computer you're using (this is called fingerprinting).
- **privacy.trackingprotection.fingerprinting.enabled = true**
  - Helps block fingerprinting.
- **privacy.trackingprotection.cryptomining.enabled = true**
  - Blocks cryptomining so that other people can't use your computer to mine bitcoin.
- **privacy.trackingprotection.enabled = true**
  - Helps to block tracking; it's not perfect, but every bit counts.
- **webgl.disabled = true**
  - Disables WebGL, which is a known security risk.
- Even more settings that you may want to consider can be found [here](#), but be aware that some of these will break certain websites and functionality. As always, think about what you need, do your own research, and weigh the risks against the benefits.

## Extensions and Plugins

Even after changing all of those settings, you're not done. While Firefox can't track you and websites will have a much harder time getting detailed information, you can and will be tracked by quite a few websites. Luckily, there are quite a few privacy extensions out there, and using these alongside your `about:config` tweaks should help further shore up the privacy of your browser. You don't want to install every single extension on the web, though- oddly enough, that makes it *easier* for you to be tracked by making your "fingerprint" more unique, so any extension you install needs to be worthwhile.

There are a few different plugins that I would recommend installing together:

- [uMatrix](#) is possibly the most powerful privacy protector on this list, but it takes a bit of learning to use well. It allows you to forbid *any* requests your browser makes to servers, letting you have complete control over what your browser downloads. You can block cookies and trackers, stop Javascript scripts, get rid of media and images, and more. The tradeoff is that you do have to work with it to get some sites working, since by default it forbids most requests, but that's not an impossible task. It's not too hard to learn and is absolutely worth the effort- if you install no other extensions, at least install this one. On WebBrowser, you're looking for [nMatrix](#).

- [uBlock Origin](#) is a fantastic adblocker that can also block other elements of a webpage if you rightclick on them. With this installed, you can say goodbye to ads! You'll also want to add the [EasyList and EasyPrivacy](#) lists to uBlock to further improve your adblocking. If you're using WebBrowser, you'll want to install [uBlock Legacy](#). If you use uMatrix, this extension is not required.
- [HTTPS Everywhere](#) upgrades most HTTP websites to HTTPS, making the connection much more secure. On WebBrowser, you'll want [HTTPS Always](#).
- [Decentraleyes](#) helps protect your privacy by replacing outsourced files with local ones. It stops requests to Google and similar companies, then provides substitute files to keep websites from breaking. As a bonus, it speeds up those requests!
- [ClearURLs](#) removes all the tracking junk from redirect URLs. On WebBrowser, [PureURL](#) does the same thing.
- [Cookie AutoDelete](#) deletes your browser's cookies, cache, local storage, and other stored data when you close the browser so that you leave no trace of where you've been. This may break a few websites, but it comes with whitelisting functionality that allows you to fix any problem sites. [Crush Those Cookies](#) is the closest option for WebBrowser. If you use uMatrix, you don't *need* this if you're managing cookies properly, but it may still be a good idea depending on your use case.

## Search Engines

[Google sucks](#)- hopefully we've established that by now. If you're still using Google for web searches, it's time to look for an alternative. Bing isn't much better, nor is Yahoo, or most of the other major search engines. If you care about your privacy, you're going to need to try something more unfamiliar.

The best-known privacy-respecting search engine is DuckDuckGo. DDG isn't bad- its privacy policy is leagues better than Google's or Bing's- [but it is slightly suspect](#). Its founder used to run a website called the Names Database that was supposed to help you connect with old friends, but it had a horrible privacy policy and terms of use. If there's anything I've learned, it's that the habits of the developer tend to translate to the habits of the program, and a history of disrespecting privacy doesn't bode well. If that isn't suspicious enough, DDG's privacy policy

leaves plenty of room for data collection, and I've noticed they have a tendency to use tracking links. They're still much better than Google and co., but they're not perfect by a long shot.

Unfortunately, other options aren't much better. Startpage feeds you Google advertisements, relies on Google for results, and may share your computer's information with a third party. Swisscows redirects your browsing history to a third party, censors you, and will freely give your information to the government if asked. Searx actually respects your privacy, but the results are often lacking and it relies on the big offenders to work in the first place (still the most private option here if you pick a good instance). Qwant may record your IP and censor content. MetaGer stores and shares your IP. Ecosia records your IP and relies on Bing. The list goes on. At present, there just aren't any good search engines that both get results and actually respect your privacy.

If you need a search engine, DuckDuckGo, Searx, and Startpage are the least bad.

## Passwords

Passwords are one of the most essential aspects of online (and offline) security for your computer. They're what stops the average stranger from tweeting something embarrassing on your Twitter account- or more importantly, logging into your lost laptop. Using secure and varied passwords is absolutely essential to good online security.

Unfortunately, human memories suck. Computers can crack short and/or uncomplicated passwords easily, which is a shame; that sort of password is what the average person can remember. Even if you can remember a complex password, you can't just memorize *one* very secure password- if an attacker knows one of your passwords and you use the same password for all of your accounts, all of your accounts using that password are compromised. It's even worse if you use that same password to log into your computer! To secure all of your accounts, you need to use a different complex password for every single account.

Luckily, other people have bad memories too and have created tools to make this much easier. Password managers allow you to keep your passwords in a secure, encrypted database protected by one master password, allowing you to store and use very complicated passwords without having to remember all of them. All you need to remember is your one master

password. That password should be reasonably secure while still being memorable- more on how to do that in a moment.

Don't use your web browser's built-in password manager. Those password managers tend to be unencrypted, making them insecure. Instead, I'd recommend [KeyPassXC](#). It's cross-platform, free, stores your passwords locally on your computer, and works offline (great for local programs). Storing your passwords locally instead of on the cloud matters because cloud servers are both accessible to the host company and can be attacked, compromising your password. Locally-stored passwords never leave your computer, keeping them safe unless your computer is directly attacked.

Make sure to back up your password database somewhere, and make sure that you can remember your master password. You don't want to lose your logins if your computer becomes inaccessible.

Speaking of master passwords: how do you make a good password that's memorable but hard to guess? You *could* generate a completely random password and memorize it with muscle memory or repetition, but it's likely to be difficult to really memorize anything long enough to be secure. A commonly recommended password length is at least 20 characters!

A far better option is to randomly select at least four words from the dictionary (more if you can remember them), put them together, and use a simple set of rules to transform them and make the password harder to crack.

For example, I used a random word generator and got "pardon waterfall jockey whisper." I put those together, then came up with a simple ruleset to transform them:

- Every other word is capitalized, starting with the first word.
- The second letter of each word is dropped.
- The last vowel in the word is changed into a number or symbol.
- The first three symbols on my keyboard are used one after another instead of spaces.

Following those rules, my password is "Prd0n!wterf@ll@Jck3y#wisp3r", which is hard to guess but relatively easy to memorize using the ruleset I used to make it. According to a password checker on [security.org](#) (please don't enter your passwords into a password checker), this

particular password would take *600 nonillion years* to crack, but I can memorize this in the span of a day or two.

Don't use this exact password (if it's in public like this, it's compromised!), but feel free to use the ideas behind it to construct your own ruleset.

A few more notes on password rules:

- Have at least one rule that adds or removes a letter from every word. Computers are very good at guessing dictionary words if they're not altered, even if you substitute a letter for a symbol. Adding or removing a letter fixes this problem.
- Using a typing quirk is a great rule- it's a memorable pattern! The more complex the quirk, the better it is for password creation.
- Make sure the words are truly random. It's much easier to crack a password that forms a phrase than it is to crack unrelated words.
- Try to make rules so that you wind up with a mixture of numbers, letters, and symbols. Mixing up capitalization helps as well.
- Take care not to make a password that includes commands that typically delete things! Check that your password would be safe to enter onto any computer. You never know who hasn't accounted for that sort of issue, and [you don't want to wipe someone's server database.](#)
- [Relevant XKCD that inspired this approach.](#)

## VPNs

Like it or not, it's incredibly hard to evade all tracking and data collection if you use the internet. Websites can see your IP address even if you don't let them see your physical location, and your IP address can be used to identify where you live quite easily even if you've taken every single precaution thus far. Think I'm kidding? [This website](#) will try to tell you all sorts of information about your browser, and your IP and geographic location are included.

Your internet service provider (ISP) can also keep tabs on what you're doing- everything you do online goes through them, and they can see and save that data. Depending on your provider and locale, this might be a serious privacy issue; for example, in the USA, the government can

demand this data from your ISP. It's also possible that your ISP's servers could be broken into in other ways, leaving your data vulnerable.

Enter the VPN. VPN stands for Virtual Private Network, and VPNs are one of your best tools when it comes to hiding your IP and network traffic. They act as a middleman between your computer and the world wide web; your web traffic is encrypted and sent through your VPN provider before reaching the internet, masking your IP and making it harder for any attackers to intercept your data.

Not all VPN services are made equal. There's a saying that if you're not paying for a service then you must be the product, and this holds true here. A VPN provider has access to your data in one form or another. You're trusting that they don't snoop and keep it private, but not every provider actually protects your data. Heck, some harvest and sell it! They have to make enough money to sustain their service somehow, so a "free" VPN must be making that money in some other way. Be wary of them.

You'll want a paid VPN that doesn't log your data and isn't located in a 5-eyes, 9-eyes, or 14-eyes country (those have public surveillance agreements). There are a lot of different VPNs, and it's hard to do the legwork yourself to find a good one, but luckily someone else has done the work for you. [This website](#) is about to become your best friend. There's a detailed chart comparing and rating 185 different VPN providers on many different criteria, making it a wonderful resource for choosing a VPN. Refer to it and think the choice through carefully- whatever provider you use will have access to all of the data you send its way, so you want to be sure they'll protect it and your privacy.

A quick note- thus far, the only good free VPN I've seen has been [Riseup's Bitmask VPN](#). It's free to download for all common operating systems and runs off donations- if you choose to use this, donate when you have the chance. They rely on that money to keep the VPN service running.

## De-Googleing

So you want to get the hell away from Google? Don't worry, I've got some alternatives.

First things first, make the easiest changes: use a [web browser](#) and [search engine](#) that aren't Chrome or Google. If you desperately need Chrome for some reason, Ungogled-Chromium is your best bet, but ideally you should abandon Chrome altogether. Even Ungogled-Chromium is working off of Google's code base for Chrome, and the developers have to keep up with changes to that code. You're best off picking another browser and a new search engine while you're at it.

Once you're on a new browser, you're going to want a new email provider. There are quite a few options that respect your privacy- [ProtonMail](#), [Tutanota](#), and [Riseup](#) are some of the best options as of now, but there are plenty of others out there. If at all possible, you should choose a provider that supports OpenPGP or another form of encryption to keep your emails safe from prying eyes.

Consider whether you only want email from your email provider. If you want that same email provider to give you a calendar, messaging service, and other utilities, that limits your options. If you want that provider to give you an app or other utility specifically for their email service, that also limits your options; that said, there are quite a few apps that can work with any email provider. [Sylpheed](#) is a very good option on desktop, and [Thunderbird](#) is another popular choice. On mobile, [Delta Chat](#) (also for desktop!) is one of the best options, as is [K-9 Mail](#).

Speaking of calendars and messaging services, you're going to want to get off of Google Calendar, Hangouts, and Messages. This is probably going to be easier than leaving Gmail and Chrome was; a calendar is a calendar, and as long as a given provider can handle your messages securely, you're fine. [Signal](#), [Element](#), [Briar](#), and [Jami](#) are all good options for personal communication. For voice calls, [Mumble](#) and [Linphone](#) both work well.

Google Drive also needs to be replaced. [Nextcloud](#) is the most prominent alternative here when it comes to general storage- not many other options are able to compete with it. [EteSync](#) can be used to synchronize contacts, calendars, tasks, and notes across different devices- while it's paid if you use their servers, it's free to host a server yourself if you have the hardware ([a cheap option there is a Raspberry Pi!](#)). When it comes to backing up your computer or moving files, an external hard drive or SSD is the most private solution, [especially if you encrypt it](#). Seagate makes some excellent storage devices that have more space than you'll likely ever need.

Google Docs is easy to replace when it comes to document editing, but difficult when it comes to collaboration. [Framasoft](#) is an up-and-coming option for collaborative document editing. [Cryptpad](#) seems to be good and is browser-based much like Google Docs is. If you only need a document editor, [LibreOffice](#) and [OnlyOffice](#) are both fantastic and free. OnlyOffice could potentially be used collaboratively through their [connectors](#), but I've never tried doing that myself and am unsure how well that would work.

Odds are that there are more services and software that you need to switch away from- Google is everywhere. This guide is long enough as it is, and other people have already covered this issue much better than I can. A list of alternatives to various Google services can be found [here](#) and [here](#), and there are many more sites out there providing similar lists.

De-Googleing is a process that will likely take some time and may not be entirely possible for you, but even partial de-Googleing is worth it for the privacy improvements. Google is surveillance hell and the less information they get, the better. Go through every Google service you use one at a time and look for alternatives. Even if you don't think a service belongs to Google, check- [you might be surprised](#).

## Other Privacy Tips

I can give you all of the advice in the world and there will still be gaps in your privacy; I don't know anything about your computer, and you likely have your own privacy issues not mentioned here. To keep your privacy solid, you'll need to keep an eye on who has your information and where it's going, and you'll probably need to relearn a few habits. After a while, maintaining digital privacy becomes second nature and you'll learn how best to control where your data winds up.

There are a few additional concerns you may want to address while working to improve your privacy:

- Review the privacy policies of your programs and services, then either use a screening tool ([here's one for testing web browsers](#)) or do some research to see if they actually follow those policies. Be mindful of tricky phrasing, and know that even anonymous data collection can be potentially traced back to you. Do you trust that program's provider to keep that data secure? Do you trust them with your data at all?



- Research the companies or people responsible for your programs. If someone turns out to have a known track record of disrespecting privacy, research their programs further and keep an eye on their behavior. A suspect developer means a suspect program.
- Don't neglect your [computer's security](#) in the pursuit of privacy. Both security and privacy are important when it comes to protecting your information, and you'll want to put some effort into improving both.
- Consider what you're willing to give up to improve your privacy. Some programs just can't be stopped from sending your data elsewhere, and it's up to you to weigh how important that privacy-disrespecting program really is. If you have to keep it, do your best to [reduce how much access that program has to the rest of your computer](#).
- Get a webcam cover. They can be bought for dirt-cheap and ensure that your computer's camera can't snoop on you. Given how many scandals have happened where a company was secretly using the webcam to spy on users, this is almost a required precaution.
- Be watchful, but don't let yourself get caught up in paranoia or conspiracy theories. If you find yourself getting paranoid or obsessing over unproven ideas, take a break and do something else for a while. Your privacy isn't worth your mental health.

## Security

Security matters just as much as privacy when it comes to protecting your data. While good privacy practices prevent more mundane harvesting of your data, good security practices protect you from dedicated attacks, malware, and other threats to your device or information. Without security, anyone could log into your computer and do whatever they wanted with the information they found there, rendering all of your privacy efforts pointless. It's worth taking the time to shore up your defenses.

### General Security Advice

- Come up with a threat model. Who are you trying to defend your computer from? Casual attackers? A professional hacker? The government? Your mom? Yourself? Tailor your defenses to best match your threat model.
- Use [secure passwords](#) and common sense. All of the security in the world won't mean anything if you enter your password into a phishing site and compromise it.
- Use a firewall, both on your router and on your computer. The best metaphor I've seen for a firewall is that it's a traffic monitor with an AK-47; it stops unwanted traffic before it gets into your computer, preventing quite a few casual attacks.
- Security needs to be balanced with convenience and usability. Oftentimes, the most secure practices will be inconvenient or reduce how many things you can do. Consider what you're willing to give up and what you absolutely need, and remember that the only perfectly secure computer is one that can't be accessed at all.
- If you don't need a program or file on your computer, don't put it on your computer. If you never use something, uninstall it. Any software can potentially become an access point for an attacker if not properly secured, so fewer files are going to be more secure and easier to defend.
- Keep all of your programs up to date. An outdated program is a vulnerable program.
- Don't connect to the internet if you're not actively using it. An internet connection is one of the greatest threats to your computer's security; if you're not connected, it becomes much more difficult for an attacker to gain access.
- Be mindful of your physical surroundings. People can always look over your shoulder and see what you're typing, and that could compromise your account information if

they're trying to see you type that. If you think someone has learned your passwords or information, change them as soon as possible.

- Don't run something as administrator or root unless you have no other choice, and avoid logging in as root. Have and use an unprivileged user for your daily activities. If that user is compromised, it will be much less problematic than if your root user is compromised. If possible, disable the password for your root user so that it can't be logged into at all. Use `sudo`, `doas`, or equivalents if you have to do something as root.
- Always think before you download, open, or run a file. Make sure it came from a reliable source, and if possible screen it for malware first. It only takes one "safe" file to compromise a computer and possibly every other computer connected to it.
- Pay attention to file permissions. Managing these is a great way to limit who can see your files and is rudimentary protection against an average user's snooping (though permissions can be bypassed by an attacker).
- Check your task manager / run `top` (or `htop`, or another alternative) every now and then and look for any unusual or suspicious processes. If you don't know what something is, look it up. This is a great way to spot problems and may help you detect any attacks. A monitor for network uploads and downloads is also quite useful.
- Use [SSHGuard](#) (Linux/Mac/Unix only) or an equivalent if brute-force attacks are in your threat model.
- Never run a command if you don't know exactly what it does. If you don't know, look it up and learn it. Man pages and help pages are a good place to start.
- Do not leave your computer alone if you're worried about someone accessing it physically. Keep it with you. Use Secure Boot if possible, set a BIOS password, secure your bootloader, and encrypt your drives to further improve physical security. If you're really paranoid, use an OS that runs off a USB stick and keep that with you at all times and/or use a keyfile on a USB to supplement your computer's password.
- Don't plug random USB sticks and CDs into your computer. USBs and CDs can be very easily used to gain remotely access to and/or modify your OS, bootloader, personal files, or anything else on your computer, and some attackers intentionally leave these lying around as bait. Even if it's not an intentional attack, you have no idea whether that lost USB or CD is carrying malware from its previous owner. Don't use a USB or CD unless you're sure it's safe.

- [Encrypt your hard drive or SSD](#) if at all possible. This ideally should be done at installation, but it can be done later if you don't mind putting in more work. If you want to secure your information on an unencrypted drive, [VeraCrypt](#) is an excellent free tool for creating encrypted file containers that can also encrypt the whole drive if you so choose.
- Encrypt your messages and emails ([OpenPGP](#) is a great option for emails). Without encryption, anyone could intercept your messages and read them. If you encrypt them, they'll only be able to read gibberish.
- [Use your hosts file to block malicious sites](#). Information on how to modify this file can be found near the bottom of the linked page.
- The only truly safe computer is a completely unusable one- you will never have perfect security. Secure what you can and keep an eye on what you can't.

## Virus Protection

Malware is pretty common online, unfortunately. Basic internet safety can protect you from the worst of it, but even an apparently benign and helpful program can sneak in a virus. Just look at Bonsai Buddy- [it turned out to be adware and spyware](#).

If you're on Windows or Mac, you should probably get an antivirus. Viruses and malware are uncomfortably common on both platforms, and Windows in particular is vulnerable to some nasty attacks that range from stealing personal information to frying your hardware. Considering how common malware is, it's best to get an antivirus program to protect you.

There are quite a lot of options here, but I'll save you time by saying that the vast majority of the free options are either garbage or actually malware themselves. Avast is spyware and annoying as hell, Avira is heavy and not effective enough, and other providers similarly fall through.

There's also the issue of free commercial software not being truly free: funding has to come from somewhere, and if you're not paying, then you're the product. All in all, avoid free antiviruses if at all possible. If you *have* to use one, go for Kaspersky (there *is* a free version, but it's annoyingly hard to find- good luck).

If you can, you should go for a paid antivirus. Vet them carefully and review their privacy policy and terms of service. BitDefender is apparently quite good and I've seen it recommended decently often. Kaspersky does the job well enough while being pleasantly lightweight, and has

significantly improved its privacy practices after a big scandal years ago. McAfee works, but it's very heavy and I have doubts as to whether it's as good as it claims to be, so I can't say I recommend it when there are better options available.

If you're on Linux, use common sense and vet your repositories and their sources. Wait a little while after an update before downloading it if your distribution isn't rolling release; if any malware somehow made it into an official repository, it'll be caught. Verify that you know where your packages are coming from and you'll likely be fine- there aren't many Linux viruses, and official package repositories help lower the risk. You're not invulnerable, but malware isn't as big of a worry as it is on Windows as long as you follow basic internet safety practices. If you're really worried *or if you regularly send files to a Windows computer*, you can download [ClamAV](#) and use that to scan your files. Ironically, one of the biggest uses of an antivirus on Linux desktops is to keep Windows computers safe.

One more note on Linux virus safety: be careful using Wine. Any program run with Wine can access all of your files, root directory included, and viruses can run with Wine. Make sure that you know what you're running is safe, and [sandbox](#) Wine if possible.

## Jailing and Sandboxing Programs

Most programs can access all of the files on your computer by default. Some Linux distributions prevent this, and Windows or MacOS might also prevent this (as they should!), but a fair number of computers give programs full access to all of the files within. Want to test it? Type / into the address bar of your browser (yes, just a single forward slash) and see what comes up. You might be surprised. If you're on Windows, [try file:///C: and see what happens](#).

Aside from all of the issues inherent in exposing your personal files to something like your web browser, this is a potential security risk. It's not just your essays and photos that are exposed; it's *everything*, including the files that let your computer boot into your OS so you can use it. You don't want anyone to mess with those files, but if someone were to hack your browser, they could potentially use it to do just that.

It's not just your browser, either. Every program on your computer can access all of your files by default, opening you up to a whole host of potential exploits and security hazards. The good news is that there are ways to limit what files a program can access and keep them contained.

On the extreme end of containerization, Virtual Machines are like computers within your computer. They have their own file systems, programs, and are self-contained. Running a program in a virtual machine usually protects the rest of your computer from what happens inside that virtual machine; a few viruses can get out in rare cases, but the average program won't be going anywhere. If you want to completely isolate something from the rest of your machine, a virtual machine might be a good solution. [VirtualBox](#) is excellent for creating and managing virtual machines on Windows, Linux, and Mac alike. On Linux, [Linux Containers](#) is another good option that uses fewer resources to achieve a similar effect.

Perhaps more practical for daily use is something called sandboxing. When you sandbox an application, you limit what files it's allowed to see and change without running a virtual machine. There are quite a few tools for doing this. On Linux, [Firejail](#) and [bubblewrap](#) make it relatively painless to sandbox applications (you only need one- I'd recommend Firejail). If you're feeling adventurous, you can manually create a [chroot jail](#) (good explanation of what that means [here](#)).

On Windows, [you may have a sandbox feature built-in](#) if you have particular versions of Windows, but otherwise you'll need to look for [third-party software](#). [Sandboxie](#) looks very promising (but definitely unfamiliar to most Windows users).

On Mac, you have a [built-in sandboxing tool](#), but not much else that I could find outside of a virtual machine or chroot jail (though I did find [two scripts](#) to make chroot jails easier!).

Regardless of the tool you use, you'll want to restrict the program as much as possible while keeping it usable. You should only allow it access to the minimum of what it needs to function. It may take some trial and error, but you'll figure out what it needs and build a secure container for it.

## Other Resources

As of April 29th, 2021, these sites were all working and had some useful additional information and tools on digital privacy and security.

- [PrivacyTools.io](https://www.privacytools.io)
- [Cyberpunk Links and Privacy/Security Guide](#)
- [Dig Deeper](#)
- [The Paranoid #! Security Guide](#)
- [Spyware Watchdog](#)
- [How to Live Without Google and Other Evil Tech Giants](#)
- [Firefox Profilemaker](#)
- [Arch Linux's Security Wiki Page](#)
- [StevenBlack's Hosts File](#)
- [Safely Creating and Using Temporary Files](#)
- [Riseup's Security Information](#)
- [Surveillance Self-Defense](#)
- [Security in a Box](#)
- [Digital First-Aid Kit](#)