thetoolsweneed.com

A Few Simple Steps to Vastly Increase Your Privacy Online

Keith Axline Portland, OR Twitter

9-11 minutes

Update: *Since first publishing this post, many people have pointed out that changing your DNS isn't a huge privacy add since your ISP can still see a lot of your traffic. The real solution here is a Virtual Private Network (VPN), which I felt went beyond the "simple" scope of these steps.* ***Read about VPNs here****.*

Update 2: *People have pointed out that HTTPS Everywhere is not a good recommendation. I'm now using* ***Smart HTTPS*** *instead.*

Online privacy is important for everyone, not just tinfoil hat wearers. First, it's more in line with what a user's expectation is when they browse the internet. Not many people understand all the tracking that happens by default.

Second, it's more how we operate in real life. You don't have someone following you around from store to store writing down every product you touch or look at, and then block you from entering other stores until you watch an ad.

Third, the principled view of not giving away valuable data to companies for them to sell is beneficial for everyone. Yes, in some cases you happily give up your data to sites that you enjoy so that

they can stay in business. But you can't opt-in to the sites you choose until you put the tools in place to block every site.

By the end of this post, you'll be leaving much lighter footprints in the internet forest. Certainly more so than your average web surfer. We'll switch up your browser and search engine, add some plugins to block surveillance, and get a little technical with DNS servers.

Don't worry, the faster browsing and smug satisfaction of being a savvy internet user will make up for the discomfort of changing your routines.

Switch to Firefox as your browser on all devices

I'm not a Chrome or Edge hater, I'm just lazy. I don't want to parse whether each new update contains a privacy regression or new settings I need to worry about. I just want a browser that has more of my best interests in mind.

Firefox is developed by a non-profit company, Mozilla, explicitly dedicated to users' needs. Google and Microsoft make money off of users in different ways and we can never be sure that their business decisions are going to align with what we would want as users.

> A non-profit giving away free software makes sense. Some of the biggest companies in the world giving away free software is suspicious.

I don't doubt that the engineers and product people are developing Edge and Chrome for the right reasons, but they are allowed to do so only so far as it is beneficial to the money-making efforts of the company they work for.

Honestly, I just really don't want to worry about it. If I have to trust someone, it's going to be Mozilla. Firefox makes it pretty easy to port over your bookmarks and preferences from Chrome as well.

Switch from Chrome to Firefox in just a few minutes

Even if you don't want to switch, you can still get a lot of benefit from the extensions I mention in the next section, which are all also available for Chrome.

Install these browser extensions

There are a few set-it-and-forget-it browser extensions I use that really only improve my browsing experience and take zero configuration. These are all available for Chrome and Firefox, except for CanvasBlocker and Smart Referer (alternatives suggested).

Privacy Badger: Developed by the Electronic Frontier Foundation (EFF) to stop invisible trackers from following you around the web.

Smart HTTPS: Enforces encrypted connections with websites whenever possible. Keeps you from accidentally using unencrypted versions of sites.

uBlock Origin: A very efficient ad-blocker that will significantly speed up page load times if you aren't using a blocker already.

Decentraleyes: When you load a page, many requests are made to sites other than the one you are visiting. Web developers find it easier to link to tools off-site rather than host those files themselves. This extension checks to see if it can use any of these files from your computer first rather than making the external request. This means faster loading pages and less of a browsing

trail for companies to follow.

CanvasBlocker: Canvas Fingerprinting is a sophisticated technique of identifying your computer across multiple sites. It can tell if you visited site A and site B just by knowing how your browser renders the pages you visit. This extension blocks the APIs in the browser that allow this to happen.

For Chrome you might checkout this other Canvas Blocker, but I' haven't used it so can't vouch for it.

Smart Referer: When you browse from google.com to nytimes.com, the nytimes.com request will tell The New York Times' servers that you came from google.com. This is called a referer. This extension removes that piece of information so that nytimes.com doesn't know where you came from. It's kind of a dick move to the sites you like since it removes valuable analytics for them, so you can (and should) whitelist domains that you want to keep sharing data with.

For Chrome there's Referer Control, but it looks like it takes more configuration and I haven't used it.

Use Startpage and set it as your default search engine

This might be the most important step listed here, since our search history is oddly personal and something I think most people are squeemish about being tracked.

I like Startpage better than DuckDuckGo as a Google Search alternative, but both are good. I believe Startpage purchases results from Google, so you get good results without one search being tied to another and then tied back to a personal dossier about you.

These search engines are still ad-driven, but they are generic ads around your search terms, not targeted to you in any way or aware of your information. It's a straightforward business model that I can trust, so I have no reason to think they are tracking me and lying about it.

Add Startpage as your default search engine in Firefox

Add Startpage as your default search engine in Chrome

Switch DNS to 1.1.1.1

Now we're getting a little more technical, but bear with me, you can do this. The first thing your computer does when you try to go to a website, like startpage.com, is it reaches out to a Domain Name Server (DNS) to get the computer-readable address of the page you asked for.

These DNS's have computer-readable addresses themselves, which are four numbers separated by periods, like 8.8.8.8 (Which is Google's DNS). All the ones I'm aware of have the same number repeated four times. The one we're switching to is 1.1.1.1.

So yeah, there's a server out there that knows every domain that you try to visit. This is definitely something we want to be secure. Your ISP will usually configure your device to use their own by default when you connect to your Wifi, but that's probably not going to get you what you want in terms of privacy and speed.

Fortunately, you can tell your computer which DNS to use.

The company Cloudflare has a publicly accessible DNS at the address 1.1.1.1 that they claim is encrypted and secure. They promise not to sell your browsing history or even log your IP

address in order to tie queries to a single person, let alone you.

And you know what? That's about the best you can ask for with a centralized infrastructure for the internet. A recurring theme in this quest for data ownership and privacy is that you can only take it so far before you have to ultimately trust a company or entity to do what they say they're doing.

In this case, Cloudflare is more of a trust-based business than most since they need most web operators to believe in their integrity to function. Their response to the Heartbleed vulnerability in 2014 was transparent, swift, and smart. Their public communication has bolstered my trust in them, as well as many other web developers.

The gist of how to set your DNS to 1.1.1.1 is to go into your computer's network settings and add those numbers in the right spot. But here's a few specific tutorials:

How to change DNS settings on a Windows 10 PC

How to change DNS Server Settings in Mac OS

How to change the DNS server used by your iPhone and iPad

How to make Android use the DNS server of your choice

Enable Private DNS with 1.1.1.1 on Android 9 Pie

If you have a different operating system, just search "change dns in XXX" where XXX is your operating system. When it gets to the actual numbers to enter, enter 1.1.1.1.

EXTRA CREDIT: If you successfully switched over to Firefox and 1.1.1.1, you should be able to turn on HTTPS over DNS, which means your request to 1.1.1.1 will be encrypted and private. Follow the numbered steps in this post to turn it on (skip the top part about nightly builds and go straight to the numbered steps):

Turn on HTTPS for DNS on Firefox

Let Me Know How It Goes

I'm happy to help you through any blockers and I'll update this post as I hear about issues that people are having. Get in touch @toolsweneed or email 'keith' at the domain of this website.

These steps should not only shrink your personal dossier that companies have on you, but will likely make your browsing much faster due to the DNS upgrade and ad-blocker.

Be a Good Netizen

Be sure to turn off uBlock Origin and Smart Referer for sites that you value, as those likely provide valuable revenue and analytics for them.

If you want to see more posts like this, subscribe below.

Cover image by Bernard Hermant on Unsplash