Hardening Your Browser

The last lesson talked about what browser to choose, and I hope many of you picked Firefox because it's going to make your life a lot easier. In this lesson, we're going to configure your browser to be as private and secure as possible, a process called "Hardening" your web browser. I will be demonstrating with Firefox, and most steps will apply to other browsers as well, like Chrome. The two browsers that can be hardened but shouldn't have extensions are Brave and Tor. Brave because it doesn't rely on extensions for hardening, and Tor has its own reasons which we'll discuss in section 4.

But first, a quick message!

Promotional Spot

To start off with standard settings, make sure you always check for updates and install them automatically for the newest security patches. Set your homepage to a privacy-oriented search engine like the ones we discussed earlier, set your default search engine to a privacy search engine, and I'd recommend disabling all forms of suggestions in your omnibar. Make sure to disable any password management done by your browser, use a password manager as previously discussed. Set your browser to never remember history, block as many cookies as possible, remove cookies and other data on browser exit, enable tracking protection at all times, send a Do Not Track signal, block pop-up windows, and make sure to limit as many permissions as possible. Lastly, make sure to disable any data collection done by Mozilla, and make sure you're not signed in to any Firefox account to sync your settings--keep it local. If you're somebody who uses Chrome or another browser, find these settings in those browsers and cover those settings. They all include more or less the same stuff.

Now something powerful Firefox has is an advanced settings menu, which you can access by typing *'about:config' into your search bar on top. Privacytools.io was nice enough to include a great list of tweaks that you should make inside of this menu to make your configuration inside of Firefox more private and secure. DO NOT skip this step.*

So now your settings are configured properly, but that's only half the story. Even then, most browsers still aren't configured to protect your information, so we need some third-party help. This is one of the few instances where we need to break the rules of minimalism in order to fully protect ourselves.

The first extension is HTTPS Everywhere. HTTP is a protocol that serves as a foundation for data communication on the internet. *Almost any website you visit utilizes HTTP or HTTPS. HTTPS is HTTP, but with a massive S at the end, which stands for security. HTTPS secures your connection and data by using an SSL certificate, encrypting your traffic.* HTTPS Everywhere forces HTTP requests to be HTTPS, making it an extremely important extension to be using.

Up next, we have Ublock Origin, an ad and tracker blocker. The reason you want to use Ublock Origin over other ad-blockers is because Ublock is open source, and Ublock doesn't whitelist websites who pay money to show ads, *which other extensions have done. Booo!*

The third extension you want is Privacy Badger, which blocks spy ads and invisible trackers. It sends a Do Not Track signal and if trackers ignore these wishes, the badger blocks them.

Both Ublock Origin and Privacy Badger *include options to prevent Webrtc leaks, which could potentially leak your real IP address when you're using a VPN or proxy, so make sure to enable it in one of these programs. Or, if you're a hands-on type of person, you can do this manually in the about:config menu, the instructions are on privacytools.io.*

Decentraleyes, clever name... Protects you against third-party tracking through large, centralized, content deliverers. It prevents a lot of requests from reaching networks like Google Hosted Libraries, and other non private libraries.

Cookie AutoDelete is an extension that deletes cookies automatically when you close a tab. So if you're on Facebook in one tab, Amazon in another, and Google in a third, closing one tab will delete all cookies associated with the traffic inside of that tab.

When you visit a website, *the basics of the website are programmed in a language called HTML, serving as the structure of the website. The second language is CSS, which styles the website and makes it look pretty. The third language is Javascript, a scripting language functioning as the brains of the website, allowing it to perform functions and features.* Javascript and other pieces of software like Flash and Java are utilized by a lot of websites. The problem is, they're *extremely easy to exploit, and typically reveal a lot about your information and browser configuration. In fact, the infamous "Spectre" and "Meltdown" exploits rely on the use of Javascript.*

Lucky for us, the newest version of HTML: *HTML5...has removed the need of one of these dangerous pieces of software: flash.* But, it's also brought its own tracking technology *called canvas fingerprinting.* Canvas fingerprinting uses the HTML5 canvas element to *draw an image on your browser that's not visible to you.* The idea is your hardware and software configuration will render the invisible image uniquely, and this is used to track you across different websites. To avoid this, *install 'canvasblocker' for Firefox, or 'canvas defender' for Chrome.*

Sadly though, HTML5 doesn't fix the problems with Javascript and other scripting languages. So this is where *NoScript comes into action. NoScript, as it sounds, disables all website scripts by default, which is fantastic!* However, it is disabling the brains of a website; so if the website relies on brains, it will severely break the site. Luckily, fixing the site is as simple as *clicking NoScript and enabling scripts for that website temporarily, or Noscript lets you load individual elements while continuing to block the others.* It is not as extreme as a plugin as people make it seem; if you need a site to work, add it as an exclusion and you never have to worry about it again. If you're using Chrome, *'scriptblock' replaces NoScript.*

The very last extension is *uMatrix, which lets you manage cross-website requests to stop tracking between websites.* I saved this for last because it's a more complex extension to use, geared more towards advanced users. I would recommend it if you are comfortable configuring it.

Queue Outro Promos

So that is how you harden Firefox and other web browsers to give you the safest browsing experience possible. We have implemented a ton of precautions on the technical side of things, but unfortunately this still isn't enough to protect you online, because there's still room for you to mess up--human error is a huge problem. The next lesson will *teach proper browsing habits, i*ncluding rules, tips, and tricks to keep you safer inside your browser. See you then!