Your Browser

Your browser is your entry to the world of the internet, without it...you wouldn't really be able to do anything. Since your browser plays such an important role in how we interact with our devices, it's important that you, the user, configures it in a way that will increase your privacy and security, limit website tracking, and give you a much cleaner web experience. Let's pick our knight!

Almost as clean as the premium version of the course with no promo messages like this one:

Promotional Spot

To start off simple, what knight, or browser should you be using? *All of them claim to be either the best, the fastest, or offer the best battery life.* So here are the browsers I recommend you use with a focus on either security, privacy, or both. If something isn't mentioned, it's because it's too new, or it's not recommended enough in the community for me to mention.

Let's start with the browser that over half of you watching this lesson are using: *Google Chrome. Yes, Chrome is the fastest browser in a great deal of tasks,* and it's (for the most part) very secure, but it is terrible for your privacy, since it's run by Google, and they're collecting data.

Google tracks your *emails, location, search history, web history and much more, you guys know this because I took you to your activity page in section 2.* Even If you're using chrome without a Google account, they are still collecting the same information and building a profile within your browser. They even came under fire for *scanning files on your computer for "improved security".* Because of this mistrust, I advise you avoid Chrome, and even avoid *chromium, the open source version of Chrome, since there is still Google tracking going on.* There are tools like *ungoogled chromium that attempt to cut out background data collection, but I'd still be wary with them.*

The next popular option is *Firefox. Firefox is a very good standard for privacy and security,* and is commonly the recommended way to go. *There is a very small amount of tracking down by the browser itself, and most of that can be disabled.* It also has some of the best support for extensions and settings used to harden the browser for the best protection, even on mobile devices, something we'll talk about in the next lesson.

Some other honorable mentions are *Waterfox, a version of Firefox with some tracking disabled by default*, although I'd still recommend using Firefox if you're willing to take the time to configure it properly.

Brave is another option. I'd argue Brave is more private than Firefox out of the box. But, it won't beat a properly configured Firefox, since Firefox will give you much more control over what's being tracked, especially related to scripts. So Brave is a great option for users who don't want to take the time to do the hardening themselves, and it's quite honestly a very promising project with high ambitions for improving privacy and security on the internet. If you go with Brave, you don't have to worry too much about the extension-oriented type of hardening we will be doing in the next few lessons.

The very last browser is the *Tor browser, which most of you have heard of.* Tor deserves its own lesson, which will be in section 4 of the course. Even if you end up using Tor, I'm going to recommend having a secondary browser as well, which should be a fully hardened browser--so make sure to configure one of the other browsers in the following lessons.

--t there is a lot more you need to do, mostly related to extensions and browsing habits. For most of you watching this lesson, I would recommend you go with Firefox because it offers such good support for extensions that we need to use. The instructions in the next few lessons will be aimed at Firefox.

Queue Outro Promos

Thank you for watching this lesson, it was straightforward because there are three more lessons which will get into the more technical side of things. I hope you've made your browser choice, and I'll see you in the *next lesson: Hardening Your Browser.*