Browser Uniqueness

This is going to be more of an educational lesson, so sit back, and relax. Browser uniqueness, more commonly known as fingerprinting, is something very commonly overcomplicated. Luckily, this lesson will keep the topic easy to understand, so let's go ahead and take care of it!

But it won't be as easy to understand as this message...

Promotional Spot

Browser uniqueness is exactly what it sounds like, how unique you are on the internet. *The idea here is the more you stick out from normal web traffic, the easier it is to track you, since you're the only person with a specific configuration. It's like being the only person in class with a 17.3 inch Alienware laptop.*

Something you have to realize about the configuration I've given you in the previous three lessons, **** hold guy fawkes mask **** is that it's not anonymity, or else you'd be blending in with everybody else, we'll talk about ways to do this in section 4. The configuration I've given you is created for personal safety and possible pseudonymisation. *Anonymization blends you in with people, essentially making you anonymous. Whereas pseudonymisation relies on you replacing any PI^2 with fake identities, or pseudonyms, which aren't tied to your real information, we'll discuss this more in section 6.* So even though you're unique, you're only using this browser for accounts that are inherently unprivate, like your personal banking and emails.

You can actually test your browser uniqueness using a service like *panopticlick, amiunique, or browserspy.dk. What you'll find if you followed the last few lessons is you are extremely unique.* We have made ourselves so private and secure that we stand out enough for websites to track us and continue to build a profile, just because we are unique—the irony is real. Does this mean everything we did was wasted? Well no, there are still lots of benefits from everything we've done. Being able to force HTTPS requests is enormously important, blocking invasive trackers that track you across websites are also important, and don't forget the ethical reasons to stop companies from tracking you nonstop.

On top of this, the hacker *Kevin Mitnick brings a different argument to the table: He says the less unique you are, the less he has to work to target you since you're using a more common, less private and secure configuration.* So even though a common fingerprint may benefit your anonymity, from a technical perspective, this opens you up to malicious activities.

Luckily, even with uniqueness concerns, there are a few things we can do to improve the problem, but keep in mind there's no fool-proof way of fixing this. The first thing is to make sure your scripts are being blocked with something like *NoScript, since scripts reveal so much about your configuration. Run panopticlick and view the revealing information with your script blocker on versus off to see why this is so important.* The second thing is to install an extension that periodically spoofs your user agent, making it look like you're using a different operating system in a different browser to confuse trackers. *User-Agent Switcher for Firefox has been working amazingly for me.* The last thing you should do is implement pseudonyms so there's as little information to tie to you as possible. This is not a pseudonym tutorial, and I'll be getting into that later on in the course. Using these three tips I've given you will help a lot, and they are as close as we can get you to full privacy and security without *touching the Tor browser—which we will do in section 4.*

Queue Outro Promos

That's going to wrap up our browser quadrilogy for section 3 of the course. I doubt this was more exciting than the *star wars trilogy,* but I hope it was still interesting and valuable nonetheless. I'll see you all in the next lesson, which will talk about *VPNs and proxies.* Thank you for watching, and see you soon!