Your Browsing Habits

Alright, welcome back! The last two lessons have taught you not only what browser to be using, but how to harden your browser to make it as safe as possible. The problem is that your decisions when you're browsing can be your downfall, so it's equally important for you to understand risks on the internet and how to get around them. Let's dive right into it...

Promotional Spot

First, only visit trusted, non-suspicious websites. *If you go to a website and it seems sketchy, just leave.* The more you browse the internet and get exposed to different websites, the better your BS radar's going to be. Here's a few things you should watch out for:

- Any website that hosts program downloads like *download.com should be avoided. Only get programs from the original source to minimize the risk of someone tampering with the file.*
- *Any website or ad that says your system is infected with malware is always fake.*
- *Check for typos, since professional websites will typically not have mistakes. Outside of that, you'll need to learn mostly through experience.*

Next up...if your antivirus, operating system, or browser warns you that a *website is unsafe, don't ignore the warning. Leave!*

Piracy can also be a problem. This isn't an ethics lesson, I'm not going to tell you whether or not to do it, the reality is it's happening. If you're a person who's pirating anything, you need to be aware of the risks that come along with downloading files from random people on the internet. The content is not coming from the original source and people can modify it in any way possible. Avoid pirating for the sake of your security.

In other news, if you're speaking to random people on the internet, scams are everywhere and you need to assume that everything is a scam, until otherwise proven legitimate.

A common scam is phishing attacks, which are website and/or other digital impersonations, *like you visit Google, but it's not actually google.com, maybe it's yoogle.com, a website owned by the attacker. When you type in your Google username and password, this information is sent to the hacker and they now have your information.* To avoid this:

- *Check the URL when you visit sensitive websites*
- *Check the site owner and certificate, browsers make this very easy to verify.*
- Make sure to setup two-factor authentication as discussed earlier in the course.

Another form of phishing attacks is through communication, so maybe someone will impersonate your bank through email and ask for your details. To combat this:

- *Always check the email domain and make sure it is the correct domain for the service.*
- Watch for poor grammar, misspellings, urgent messages, pleas for money, or pleas for information. Keep in mind that your friend may get their email hacked, causing you to receive a malicious email from your friend. If anything seems suspicious, double check with them to make sure they sent you the message.

Okay, that's all covered. Here are some more random tips, let's just rip through them!

- *Try to log out of websites when you're done using them.* Google and Facebook can track your browsing habits and tie it to the account you're logged in to.
- Within your browser, make sure to implement minimalism with permissions like we discussed earlier in the "Permissions & Settings" lesson. *Don't hand over your location, webcam, audio, or other any information to a website that doesn't need it.*
- At this point you'd think it's difficult for websites to track you, and...don't get me wrong it is. But behavioural analysis can still leave you exposed. *The way you type is something extremely unique to you as a user, meaning it can be used to track you.* This is concerning because Google and other firms can tie different types of data to an individual based on their typing habits. Luckily, there's a plug-in called '*Keyboard Privacy' for Chrome which plays your keystrokes at random cadences to reduce behavioural tracking. Unfortunately, there's no official version of this for Firefox, but 'behavioural keyboard privacy' attempts to do the same thing. You can take this to the extreme by never typing anything directly into your browser--type things in a text editor and copy and paste the data to your browser.*
- On an unrelated note, when you're installing programs on your computer, it's not uncommon for them to try to sneak *PUPs, or Potentially Unwanted Programs,* onto your system. *To avoid this, read all the checks within programs during the installation process, since some of them are not related to terms and conditions, it's just asking to install PUPs.*

To finish everything off, try to use common sense on the internet. If a random stranger is asking for your personal details, you probably shouldn't give it to them. If there's an ad for a ***show pill*** penis enlargement pill, it's most likely a scam and doesn't work, just be aware.

Queue Outro Promos

In reality, you're probably going to mess up here and there, we all do, but that's why we've discussed different precautions, and we will have many more safety nets throughout the rest of the course. The next lesson will be the final lesson of our browser quadrilogy, and *it's titled: browser uniqueness.* It's super interesting actually. Thank you for watching, and see you then!