Proxies & VPNs

Welcome back to the course! If you follow or keep up with any security or privacy news, I'm sure you've heard of one of the following terms: *Proxies and/or VPNs.* What are these tools? Do they make you anonymous? Are they different from one another? In this lesson, we're going to cover all of those questions, and much much more!

Promotional Spot

Let's start with proxies. A proxy's main goal is to hide your real IP address. *An IP address is a unique code used to identify you on the internet. Proxies spoof this by acting as a middleman between you and the websites you visit, so that the website thinks you're visiting from the proxy server. They are typically programs you download, or they can be configured directly in the settings of applications.*

The main downsides to proxies is they don't typically encrypt your traffic between your computer and the proxy server, they don't tend to strip identifying information outside your IP address, and there are no additional privacy or security considerations built in. so when it comes to protecting your data from internet service providers, governments, or network attacks—proxies won't really help you. What they will help with is simply making your IP address.

Let's move to VPNs...VPN stands for *Virtual Private Network;* they're going to hide your IP address and allow you to connect to servers around the world--like proxies; except there's one major difference--your traffic is encrypted. *So now, no one except the VPN company and you have the direct ability to view and see what you're doing online. If your VPN is a good one, they themselves shouldn't know what you're doing either.* Because VPNs are encrypted, any people who could potentially be between you and your final destination will have a difficult time figuring out what's happening inside the VPN, meaning people like internet service providers won't be able to snoop, collect, and sell your browsing data, *which they DO do. (doodoo) In fact they lobbied congress to make this legal in 2017.*

Another benefit to VPN encryption is if you're on public wifi, there's a possibility the shady guy in the corner is using a *free tool like wireshark to view every connected device on the network to view its contents, including yours. He could just be watching, or he could be redirecting your connection to a javascript keylogger that logs all of your keystrokes to steal your passwords. This is called a man-in-the-middle attack. If you're using a VPN, the creepy man can only see that you're connected to a VPN, nothing else.*

This is all great, but, there are downsides to VPNs. First, they use processing power to encrypt traffic, which may be tougher on older hardware. Second, they tend to **** show money **** cost more than proxies since they offer more functionality. Third, some *sites like Google will give you a CAPTCHA request to ensure you're a human, since your IP address is likely being used by a great number of people, this is extremely annoying. Fourth, some websites will block VPNs because of the large amount of people using the same IP address, Amazon is a big fan of this*. The last downside to VPNs is they're typically slower than proxies, which could be a problem for people looking to stream or download content.

Whether you go for a proxy or VPN, I will typically push you away from free services. It costs money to run them, so if you're not paying with your cash, you're most likely paying with your data. There are exceptions to this rule, like if a quality VPN service offers a *free tier, like ProtonVPN or Windscribe.* This can be okay, just avoid services that are only free with no paid variants, and no clear business model. *Security expert Chema Alonso demonstrated at DEFCON how he setup a free 'anonymous proxy' to attract bad guys to the service. After just a few days of the creation of xroxy.com, he had over 5,000 people using the service.* Alonso could have used this opportunity to push malware into people's browsers, tracking everything they do. He could harvest and sell their data, or he could turn everyone over to law enforcement. Let this demonstrate how easy it is for someone to put up fake services, and why free services should be treated with caution.

Outside of not being free, what are some other considerations you should take when picking a VPN?

- Check the encryption and make sure they offer *AES-256 bit data encryption and at least 2048 bit handshake encryption utilizing OpenVPN or WireGuard—we'll talk about WireGuard soon.*
- Check their jurisdiction if you believe the location of the company impacts its ability to be private. Avoiding US companies tends to be a common pattern.
- *Do they implement Perfect Forward Secrecy, meaning they continually cycle encryption keys so that if one key is compromised, the others will still be safe?*
- *Investigate their history to see their background and if they've ever given up user information.*
- Check their privacy policy to see their stance on how they work with law enforcement. If they publicly state they do, then you should assume they keep or will keep logs.

- *Some extra things to look for are system-wide kill switches, a setting where if the VPN disconnects, all internet traffic from your computer will be stopped--never exposing your true IP address.*
- *If you want a quick list of good services, privacytools.io has a good basic list, or we evaluate VPN services on our website and YouTube channel, utilizing a systematic, public, review protocol.*

It's important to mention that VPNs are NOT all-in-one anonymization tools. If you want your VPN to be private, not just secure, you're going to have to open an account anonymously. This means utilizing techniques you'll learn throughout the course, like setting up an account with a fake name and email on an open wireless network using something like Tor, we'll discuss how to do all of this later on. Next, you have to find a way to pay for the VPN anonymously. In short, you have to find a service that takes *cash like Mullvad or IVPN, anonymous cryptocurrencies like NordVPN, gift cards like PIA, or you can buy prepaid debit cards anonymously and use those--I'll discuss anonymous transactions later on in section 6.*

Even if you take proper precautions, you should not fully trust your VPN to handle your data--they can be a single point of failure. *IPVanish, Hidemyass, and PureVPN are just a few services who handed over user data.* All vital information should be encrypted before it reaches the VPN's encrypted tunnel. Use HTTPS everywhere in your browser, use encryption for your emails, and anything else you can do to encrypt yourself, before it leaves your computer. We'll discuss how to do all of this later on.

All of this mistrust with VPNs brings up a valid question, should you host your own VPN server? It's difficult to self-host a VPN anonymously, because you're self hosting it. There are some configurations I've seen to mitigate this issue, but they're pretty complex to implement. Self-hosting vs commercial VPNs will come down to what your priorities are, and what works best for your use-case.

The very last thing I want to bring up is *WireGuard, a new protocol designed to replace the current VPN standard--OpenVPN.* As of today, they have recently left beta, and are becoming a more standard offering across both operating systems and VPN providers. I'm still wary since it's relatively new to the scene, but *definitely keep an eye on Wireguard, it's a very promising project that may one day be the new recommended protocol, over OpenVPN.*

Queue Outro Promos

That's going to wrap up everything! I hope you understand the differences between proxies and VPNs. I hope you enjoyed the lesson, and I will see you in the next one, where we talk *about antiviruses and malware.* Thanks for watching.