# Welcome to Securing Your Digital Footprint

## VPN

In the last seven articles, we have covered general security, passwords, 2-form authentication (2FA), emails, pretty good privacy (PGP), browsers, mobile devices and free wifi. Hopefully, you've been implementing all of the information you've learned, and are feeling pretty good about security your world.

Put simply, a VPN or Virtual Private Network, is a group of computers (or discrete networks) networked together over a public network- namely, the Internet.

When you connect to a VPN, a VPN client is launched on your computer (or click a link on a special website), log in with your credentials, and your computer exchanges trusted keys with a far-away server. Once both computers have verified each other as authentic, all of your internet communications are encrypted and secured from eavesdropping. The most important thing you need to know about a VPN: it secures your computer's Internet connection to guarantee that all of the data you're sending and receiving is encrypted from prying eyes. Source.

What to use a VPN for:

- **Making your IP address invisible** - Your IP address is monitored all the time you browse the net for marketing purposes. With a VPN you can hide from bots roaming the net for your information.
- **Securing your data** - Connecting to a public WiFi can be risky, because public WiFis can eavesdrop on your data. In the worst case scenario this could lead to your passwords getting in the wrong hands. With VPN's encryption all the data you send and receive through the Internet is secured.
- **Seeing blocked or limited content** - Some websites are limited to certain countries only. With a VPN you can change your location and use the websites normally.
- **Avoid throttling** - Some Internet service providers (ISP) slow down your connection while streaming video or gaming to save their bandwidth. With VPN you can avoid this, because the ISP can't analyze your data. Source:
- **Internet Kill Switch** - This allows that you don't have DNS (Dynamic Name System) leak - if you loose connection with your VPN, it shuts down all of the programs that access the Internet, to stop you from publicly broadcasting over the web.

The network maybe safe from gov't spying, but it is still a network, practicing safe computing with virus and malware scans for PC's and Androids and verifying browser(s) are set to hide your fingerprints. Remember you can block tracking but its very hard to stop it completely.

© Copyright Diversity Computers 2017 Not to be used without permission.
© 2025 Janet Redhawk / Plain Text Studios / All rights reserved.

Plain Text Studios

When considering a VPN you should ask these two questions:

1. Do they keep ANY logs which would allow them or a 3rd party to match an IP address and a time stamp to a user of their service? If so, exactly what information do they hold?

2. Under what jurisdictions does their company operate and under what exact circumstances will they share the information they hold with a 3rd party? Source:

VPN's come in two different types, free and paid.

Remember the golden rule of the web: "If You're Not Paying For It, You Become The Product." Free VPNs aren't trustworthy nowadays and many of them are even malware or adware. They tend to compromise on speed, performance, and also keep logs of each user's activities.

If you are tech savvy, a free option that works well is OpenVPN, an open source program that allows you to install and run your own VPN.

Paid options are available in cheap and not.

Cheap options will run you one to two dollars a month. That might sound like something that has limited or sketchy services, but believe it or not the opposite is true. Be sure to do your homework, we gave Ivacy a try. In their list of services, there was nothing that said that OS X (mac), and iOS could not access several of their services. Their interface had problems installing, and tech support was next to useless.

We did end up going with NordVPN. After several weeks the product has been performing great. We got a deal for two years, $80. The Kill Switch, takes a bit of getting used to. Every time your machine goes to sleep or you lose connection with your Internet connection, all of the program you have listed close. Make sure you set your browser(s) to "start where they left off," that way all the sites you were working with will be there when you open the browser again.

Other paid options can run ten dollars or more a month, you get a lot of the same services as the cheap options.

To help you make a decision, here's a dated article, from 2011. This article http://lifehacker.com/5935863/five-best-vpn-service-providers is a more current. For the most up to date information read this one.

Once again Apple has provided for its users and included a tool. You won't need a 'VPN program' to run on your devices. All you need is the connection info from the VPN provider. However, the Apple VPN does not have options like the Kill Switch.

Plain Text Studios

© Copyright Diversity Computers 2017 Not to be used without permission.
© 2025 Janet Redhawk / Plain Text Studios / All rights reserved.

One last comment, the whole point of using a VPN is securely connecting to the Internet. Even if the VPN company you choose says that they don't log, we only have their word for that. There is a group that would like to put together a decentralized VPN. That way everyone would know what was going on behind the scenes.

Conquering this in-depth step, you are well on your way to living in a more secure digital world. With just one more article we are coming to the end of our class. Tomorrow we tackle system Encryption.

Plain Text Studios

© Copyright Diversity Computers 2017 Not to be used without permission.
© 2025 Janet Redhawk / Plain Text Studios / All rights reserved.