

Virtual Private Networks (VPN)

By Phil Davis

July 19, 2017 (updated January 12, 2019)

What is a VPN?

Virtual Private Networks (VPNs) have been in the news a lot recently so you may be wondering just what it is, how it works, and whether or not you should be using one. With the government allowing your internet service provider to sell your web history, It may be a good time to start looking for a good VPN product.

Normally, anything you send or retrieve from a website is sent in the clear. Anyone intercepting it can view or capture it – they can see exactly what you send or receive from a website. A VPN can make surfing on unsecured networks more secure by encrypting all of your traffic on that network and then decrypting it before sending it out – It's a middleman between you and the internet. Your ISP can only see a bunch of encrypted traffic that looks like random characters and it looks like you only visited one website, your VPN server.

Figure 1 shows what happens when you use a VPN. I used dnsleaktest.com to detect my IP address in three ways: with no VPN, a VPN server in the midwest, and a VPN server in New Zealand. The VPN service that I use has over 35 other choices for servers in many other countries. Although I have blanked out the IP address with no VPN, it is just the IP address that my ISP automatically assigns when I connect.

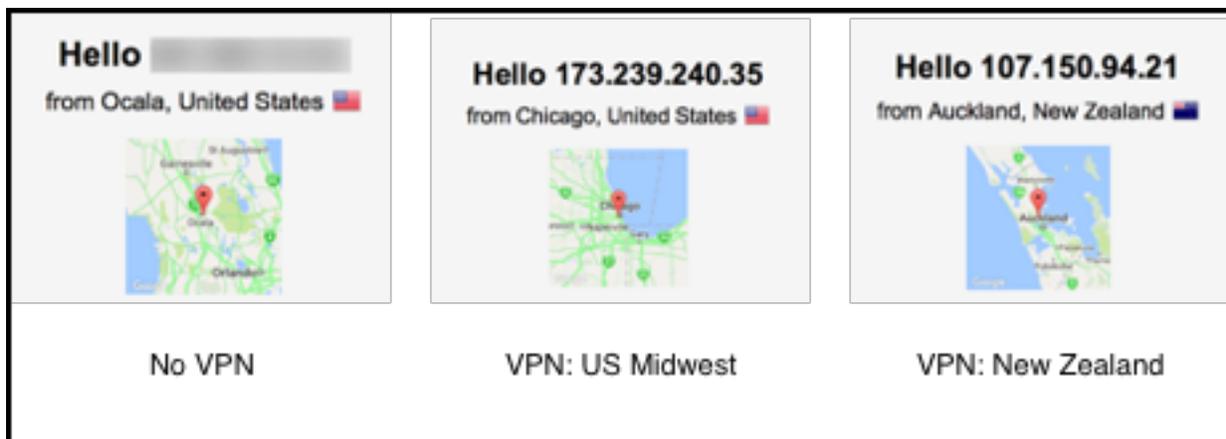


Figure 1. IP Cloaking

A VPN connection (Figure 2) is like having a really long ethernet cable from your computer to the server on the other end. VPNs are not new. Businesses have used them for many years to ensure the privacy of their communications and to allow employees to access their work network securely when they're away from the office.

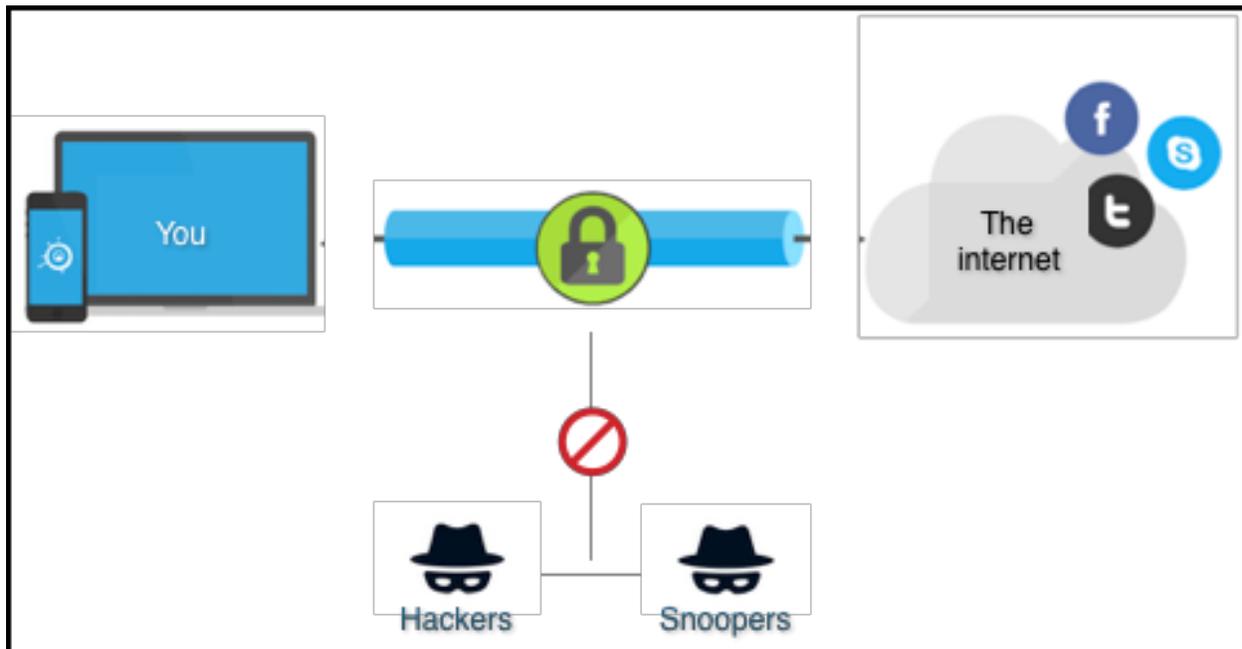


Figure 2. VPN Diagram

One misconception about VPNs is that they provide user anonymity. Jeremy Campbell, creator of DNSleaktest.com, has said that “Using public VPNs for anonymity is foolish and potentially dangerous, no matter how securely it’s configured, simply because the technology was not designed at all for anonymity. VPN services require that you trust them, which is a property that anonymity systems do not have.”

Using a VPN On Your Computer (or Mobile Device)

Choosing a trustworthy, reliable VPN service provider can be hard, but Reddit user *That One Privacy Guy* collected virtually everything there is to know about most large (and many small) VPNs and put them into a single color-coded chart that’s easy to read and understand. This [online chart](#) outlines VPN business practices, logging, service configuration, and other features, pinpointing contradictory policies and misleading claims by various services are 100 percent effective.

Tip: Be careful when selecting a VPN provider. Although the traffic is encrypted, be sure that you select a company with a good reputation, rather than one that looks a little too good to be true!

Although there are free VPN services available most experts caution against using them because they may not provide the best security. It is better to pay for your VPN service which can be as little as \$40/year.

Most VPN providers offer their own desktop clients that make it easy to connect to the service. Simply install the software that they provide and set some preferences. From there it is usually automatic. Most services let you pick a server location and set some networks to be trusted at all times.

I recommend using the [VPN Comparison chart](#) to select one or more product to test. Most of them will have a free trial so you can see how they work, see where their servers are located and test the impact on your internet connection speed (should be minimal).

Occasionally you will find a site that doesn't work well with your VPN. If this happens it is easy to turn the VPN off temporarily. I tried several services before I settled on the one I use now. Make sure you select one that allows you to use the service on several devices, including your iPhone, iPad, and Android device.

Here are several providers that have a reputation for being reliable and trustworthy: [Private Internet Access](#), [NordVPN](#), [Cloak](#), and [Tunnelbear](#), but do your own research before you make a decision.

Learn more about choosing a provider from [That One Privacy Site](#),