SWCP Portal

May 2024

VPNs – Who Needs Them?

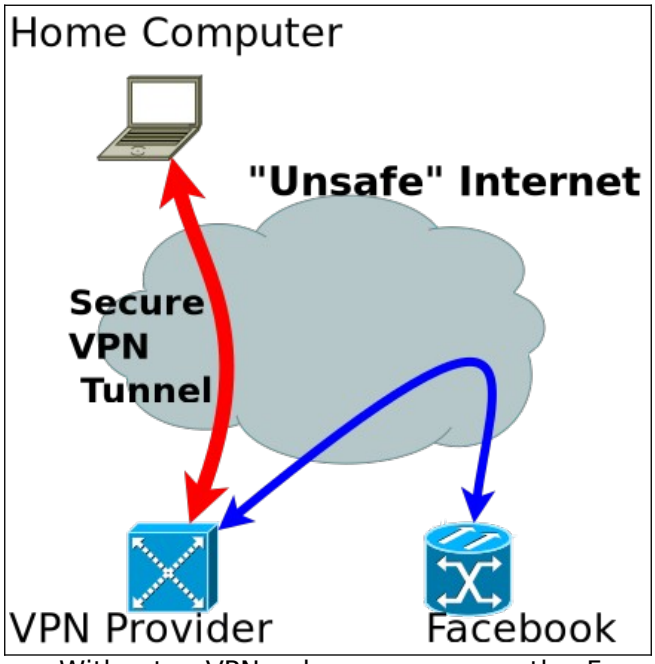
By Mark Costlow

If you listen to podcasts or watch Youtube videos, you've seen and heard a great number of VPN advertisements. Vendors promote them as vital security measures to keep you safe online. How vital are they really? Are you putting yourself at risk if you dare to google without protection? Or are VPNs just security snake oil designed to separate you from a few more sawbucks? Or is it a tool for evading the Internet's Intellectual Property police?

As usual, the answer is, "It depends". We're here to tell you what it depends on and demystify the murky world of "VPN".

What exactly is it?

Let's start by defining the term. VPN stands for Virtual Private Network. It uses software to "tunnel" a connection from one computer to another, through an existing network. We won't go deeply into how that works. There are **good online tutorials which explain in detail**.



Without a VPN, when you access the Facebook web site, your message is passed from your computer to your ISP, through several routers at the ISP, then through one or more other networks until it reaches a Facebook server.

With a VPN, as shown in the diagram above, when you access Facebook, your message is encrypted and sent to your VPN provider first, where it is decrypted, and then forwarded on to Facebook.

The two important features of this kind of VPN connection are:

- It "cloaks" your IP address - When Facebook gets your message, they think it originated from an IP address at your VPN provider, not your home internet connection.
- It encrypts your data traffic - as the message leaves your computer, it is encrypted so your ISP (for example) can not look inside it.

Are either of these things important or useful? Let's look at the encryption feature first.

VPN Encryption

Encryption is the act of re-coding your data with a secret key so that if someone intercepts it, all they see is gibberish. Only someone with the right key can decode the data. In this case only you and your VPN service provider can decipher it.

If you live in a police state where your ISP is in fact spying on the citizenry, then this kind of protection could be essential. It diguises the content of your message, but also the recipient. Especially in a police state, if the authorities figure out who you are talking to, it can be almost as damning as knowing what you are talking about.

While not as scary as the secret police monitoring your political activity, **American ISPs have been found to be monitoring** and aggregating the activity of their customers to sell on to data brokers. That's not an existential threat, but it's creepy to think about them selling your location data or TV watching habits.

Another situation where you shouldn't trust your own internet connection is public WiFi. When you connect to the WiFi at a coffee shop, hotel, or airport, any number of people could be spying on you, for a variety of reasons. Criminals might be trying to siphon off valuable personal data, or rabid marketing companies might collect data about your browsing for resale.

Using a VPN service in these situations protects your network use from prying eyes, regardless of their motives.

Internet Wormholes

In a strange twist, something that is an incidental artifact of VPN technology has become a major selling point for VPN services. When you

access a service through a VPN connection, the servers see your connections as originating from the VPN service, not from your home internet connection. This has obvious benefits for dissidents trying to stay under the radar, or criminals trying to send a ransom demand without tipping off Interpol to their location. But a more prosaic use of this feature has become very popular.

International media rights for movies, TV, and music are a spider web of competing interests. The Internet has flattened the geography out of most things, except for media rights. One doesn't even consider "how far away" someone might be before calling them. It just doesn't matter anymore. But if you want to watch “Parks and Recreation” on Netflix, and you live in the US, you are out of luck. It used to be available, but got removed a few years ago and is now on a different streaming service.

However, it is available on Netflix in the UK. So if you could convince Netflix that you are in England, you could watch it without having to subscribe to a new service. If your VPN provider lets you "pick a country" for your apparent location, you can specify a UK address which may fool Netflix into letting you view that UK-only content.

Similarly, expats who are temporarily or permanently abroad can access the content of their home country, such as the local news from their home town.

This practice is legally and morally murky. In most cases it's illegal in the jurisdictions of the content providers (e.g. the UK or US), but the **VPN companies are often headquartered outside of those jurisdictions**, which makes enforcing such regulations difficult.

Morally, it would be hard to justify breaking the law to save a few bucks. On the other hand, simply allowing an expat to keep up with the local news of home seems justifiable. You'll have to consult your own inner compass to decide whether you want to use these wormholes.

Business VPN

The other common use of VPN technology is for businesses to allow their staff to access the corporate network from other locations. This was the original use case for VPNs 20 years ago and has become commonplace. The pandemic lockdowns radically increased this use. VPNs allowed office workers to connect to the company network from their home Internet connection and be just as productive as if they were in the office.

The technology for this type of VPN and "consumer" VPN services is identical. The main difference is whether there is a 3rd party VPN provider involved. For business use, the connection goes from your home computer directly to your company's VPN server on the company network.

Trust

When you use a VPN, the only people that can decode your data are you and your VPN service provider. You've successfully hidden your **activity from your ISP**, or lurkers on a public WiFi. But how much should you trust the VPN provider? That's a hard question to answer.

Perhaps the best approach is to check the online reputation of the different providers to see who is happy with them and who isn't. But there are still things it is all but impossible to know. For example, if they claim that they don't keep connection logs (so the authorities can't subpoena them for information later), how do you know they are really doing the job correctly? **VPN providers have been found to keep logs** in spite of claims to the contrary, and even leak them to others, through both malice and incompetence.

And remember that since most of these companies are purposely headquartered outside of your own jurisdiction, you're not likely to have much recourse if you decide they've mistreated you.

Don’t choose based solely on price. Remember that your VPN service is uniquely positioned to capture and analyse ALL of your network activity. If a company offers this service for an extremely low price, or even free, one should wonder where the money comes from to operate the service.

Perhaps the best you can do is try to pick a reputable option, keep your fingers crossed, and don't commit any crimes.

What About SSL?

You probably know that SSL lets your browser make secure connections to web sites. These days the browser “lock” icon is active for most sites, so most things you do are already encrypted. So why bother with a VPN?

The main issue is that the VPN can encrypt everything, including domain name lookup requests. With SSL, your computers still makes open requests for the addresses of the sites you visit. As we mentioned earlier, hiding who you talk to can be as important as hiding the conversation itself.

Southwest Cyberport - swcp.com
New Mexico’s Expert Internet Service Provider since 1994
505-232-7992* | *Support:* *help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110
Click on bold blue type in browser for links.