Published in Us News 360 report in June 2020.

What Is a VPN Connection?

A VPN, or virtual private network, tunnels your information from point A (you) to point B in secrecy. “Surfing the web or transacting on an unsecured Wi-Fi network means you could be exposing your private information and browsing habits,” according to Norton, a company that produces antivirus and security software. It calls VPNs “a must for anyone concerned about their online security and privacy.”

Your IP address is your “name” or ID that transmits who and where you are – your digital coordinates, if you will. A VPN encrypts, or converts into code, your IP address, and any data you send, and then decrypts it on the receiving end. It can make it look like your connection is coming from another country, which can unblock some geo-restricted websites.

“Think about all the times you’ve been on the go, reading emails while in line at the coffee shop, or checking your bank account while waiting at the doctor’s office,” Norton explains. “Unless you were logged into a private Wi-Fi network that requires a password, any data transmitted during your online session could be vulnerable to eavesdropping by strangers using the same network.

“The encryption and anonymity that a VPN provides helps protect your online activities: sending emails, shopping online, or paying bills. VPNs also help keep your web browsing anonymous.”

A good VPN also blocks most advertising trackers that bombard you with targeted ads and messaging you want to avoid.

It’s the virtual version of the tubes that pull a capsule containing your checks, debit card, and ID to the teller at your local bank. At your end, you’re securing your personal data in the cylinder and sending it through the pneumatic tube (encryption). The bank teller receives the capsule and opens it securely, revealing the data you sent through (decryption). In between, your information is protected during the journey in a layer of plastic (tunnelling).

Do I Need a VPN?

Pros:

- Keeps your passwords secure from prying eyes.
- Protects all of your transmissions from hackers when you’re on public Wi-Fi networks.
- Removes geo-restrictions, allowing you to access your local streaming services when you travel to other countries.

- Allows you to browse anonymously.
- Safely connects to sites in regions that restrict social media and censor content.

Cons:

- Cost, which varies from VPN provider to VPN provider.
- Choosing a VPN without full security when your internet connection drops puts your data at risk.
- Doesn’t protect you from viruses or block all malicious websites.

Your passwords, medical history, private conversations, financial information, and more are nobody’s business but yours. Using a VPN when conducting any type of personal business protects your information from hackers while you’re connected to a public network.

VPNs are also helpful for business reasons. For example, if you have your own business, you’ll want to secure all of your proprietary information, and a VPN is a great way to do that. It’s also a smart idea if you’re a freelancer or remote employee working from a coffee shop or library with public Wi-Fi. A reputable VPN backs up your business with a comprehensive privacy policy and doesn’t store or record your activity online.

A VPN isn’t all-knowing and all-seeing, so also employing a malware blocker and antivirus software is a smart practice. This suite of security software works together like elbow pads and a helmet when you’re riding a skateboard, protecting all your vulnerable areas.

On the negative side, a VPN may slow down your connection if you’re on VPN servers that are maxed out. “Using a VPN means redirecting most or all of your network communications through the VPN provider, which is adding another hop to whatever path your communications would normally take. This extra hop will increase latency and may eat up some of your bandwidth if the VPN provider's servers are overloaded,” says SitePen Senior Software Engineer Jason Cheatham. “Encryption and decryption require some computing power. On a phone, this can lead to decreased battery life. On both desktops and phones, it can consume some bandwidth.”

Most VPN connections with top-rated companies are reasonably fast, though overall speeds can vary from one to the next. If you’ve never used a VPN before, read over the money-back guarantees for the VPN you choose (if applicable) if the service is downgrading your online experience overall. Changing a few settings can also help improve your speeds. For example, using a server close to your location can help mitigate the latency issue.