What is a VPN? Is it something I need?

VPN stands for “virtual private network” – a service that protects your internet connection and privacy online. It creates an encrypted tunnel for your data, protects your online identity by hiding your IP address, and allows you to use public Wi-Fi hotspots safely.

A VPN is a group of computers that are set up as a network on the internet and which you can access from your personal computer in order to protect yourself from eavesdropping. A VPN takes your private network and extends it across a public network, so that your IP address and data are encrypted and hidden.

Many people use VPNs today not only for security, but also in order to change the location of their computer so that they can watch their favorite TV shows from a foreign country or stay connected to a work network even when outside of the office. In addition, in countries where there is rigid state control of the internet, a VPN can help you sidestep the authorities and access banned websites, while also covering your virtual tracks.

How to use a VPN

VPNs can be connected via a free app provided through your home router. Connecting through an app is more common since it connects to your phone, laptop, and other mobile devices and is therefore available wherever you go.

Most providers will offer tutorials on their website. There you should find installation videos for Windows, Mac, Linus, Android, and iOS. The process is similar to what you’re used to, and regardless of whether you’re on a phone, computer, or tablet, the process will revolve around a few familiar steps: download, install, and sign in. From there, you’ll connect to a server location. Typically, an automatic connect feature will choose a recommended server location for you, though users who wish to can navigate server locations and choose their own. Once connected, you’re good to go. An icon should appear which you can click on to manage and customize your VPN settings, though no further actions are needed to surf the web freely and securely.

How to Choose a VPN

What should you look for when buying a VPN? There are 3 main factors to consider: logging, security protocols, and servers.

Logging

There are 2 types of logs—connection logs and usage logs. Connection logs are a basic record of your connection to the VPN server, including your IP, how long you were online and how much data was transferred. These logs are kept by the VPN to deal with technical issues. Usage logs on the other hand show which websites you’ve visited, the files you’ve downloaded and which files you've used. You want to look for a VPN provider that has a strict no usage log policy. Some companies have been known to make money by selling the data from customers’ usage logs, which can include sensitive information that you don't want getting out there.

Security protocol

A VPN uses a security protocol to encrypt your information and keep it out of the hands of third parties. That said, some protocols are stronger than others, and some, like PPTP (point to point tunneling protocol) are known to have security flaws. OpenVPN is seen as the best in the industry, but many providers allow for multiple security protocols and you want to make sure that yours uses one that is known for airtight security.

Another handy and common security feature is an automatic kill switch, which will automatically take you offline if the VPN for some reason stops working.

Subscriptions to VPN’s seem to average between thirty dollars and one-hundred dollars per year.

Top 5 VPN Providers

1. ExpressVPN
2. NordVPN
3. CyberGhost
4. Hotspot Shield
5. PureVPN