Beginner’s Guide to Virtual Private Networks (VPN’s)

A good VPN is a must-have if you:

- Use public Wi-Fi regularly
- Shop and bank online
- Want to stay safe while streaming

Security

A VPN redirects your connection to the internet through a remote server run by a VPN provider. Once connected to the server, users experience safe and secure internet browsing.

Personal vs. Corporate VPN

At Volta, our VPN services are designed for personal use. However, corporate solutions are also included in the VPN definition. Business VPNs allow employees to access their company’s network outside of the office.

What does a VPN do?

When accessing a website on the internet, you connect to your internet service provider (ISP). They then redirect you to any website (or other online resources) that you want to visit. Everything you do on the internet passes through your ISP’s servers, meaning they can see and log and see everything. Your internet activity, like your browsing history or timestamps from certain websites you visited, can easily be handed over by your ISP to advertisers, government agencies and other third parties who are looking to use this information for their own benefit.

This is why many users online opt to use a VPN. VPNs redirect your internet traffic through a carefully constructed remote server. This way, your IP address remains hidden and all the data you send or receive is encrypted. The encrypted data is impossible to read by anyone who crosses it’s path, meaning it will remain secure.

Secure internet connection

When you’re in a public place, like a crowded airport or a small coffee shop, you don’t think twice about connecting to the available Wi-Fi network. But do you know who is on

the other side of that network, monitoring the internet traffic of every user who is connected? Who even knows if the Wi-Fi you connected to is legitimate. That network could've been set up by a stranger, waiting to prey on every user who connected to the Wi-Fi. Your passwords, banking details, credit card numbers, and every other bit of your personal data could easily be hijacked without you even knowing.

With a VPN, every bit of data you send and receive travels through an encrypted tunnel so that your personal information is only accessible by you. Even if a shady third party managed to intercept your data, it would be indecipherable to them.

Complete online privacy

Without a VPN, your connection is exposed. Random devices, like the Wi-Fi router in the coffee shop, can look at and log your data with the ill intent to use it in other ways that are beyond your control. Sometimes, the people looking at your data aren't so random, like your ISP or your employer. Based on your IP address, which depends on your location, sites and services may charge differently or show invasive ads specifically targeted to you.

Government agencies can track your online activity and share the metadata they find with each other. They also share intelligence across country borders through alliances such as "14 Eyes."

When connected to a VPN, you can have peace of mind knowing your IP address is hidden and your personal data is encrypted. The websites you visit are no longer common knowledge to your ISP because all your online activity takes place on the VPN server. They can't collect your metadata nor log your browsing history, and since they can't collect it, they can't share it with anyone else.

Safe content access

Several countries around the world restrict certain types of online content. This includes social networks, games, chat apps and even Google. Many workplaces and academic institutions also use firewalls to limit access to websites for a range of reasons, from increasing productivity to restricting inappropriate content.

Websites and services are blocked by denying access based on your IP address. When you connect to the internet, your IP shows the country you're currently in, so country-specific restrictions apply to you.

A VPN allows you to connect to servers in different countries by making your IP address look like you are somewhere else. This helps you access restricted websites while keeping your personal information safe.

Why do I need a VPN?

Feeling spied on has become the norm. VPN services offer extra safety and security online, and internet users choose to use them because of this.

Your communications on the internet are 100% encrypted using a VPN. This way, your ISP, government agencies and cybercriminals can't see which websites you frequent and can't interfere with your online activities.

Another great feature about VPNs is that you can access the global internet from any location. A VPN allows you to connect to hundreds of remote servers virtually anywhere, this way bypassing censorship.

Here are a few most common cases when you should strongly consider using a VPN:

You use public Wi-Fi regularly

When you're using a public Wi-Fi network – even one that's password protected – a VPN is a must-have. Public hotpots are not guaranteed to be safe. Hackers have countless methods to hijack your internet traffic and steal your passwords, files and photos.

On the bright side, VPNs ease your anxiety about possible data loss or identity theft. With a VPN, you can securely check your email and social networks, make banking transactions and shop online. Even on free Wi-Fi.

You travel a lot

Planning a trip abroad? A PVN can help you access services that may not be available in that country. Even if you just cross the border to a neighboring country, you most likely will not have access to all the sites you normally use.

Not being able to stream content you paid for is irritating. That's where a VPN can step in. It changes your IP address, making it look as though you're browsing from a completely different location. If you connect to a VPN server in your home country, you will be able to access all your favorite shows and movies securely.

You want to shield your browsing from third parties

Even when browsing the web at home, it's still a good idea to use a VPN. For example, you may want to buy your sibling a wacky Christmas gift without being followed by gag gift ads on every website you visit. Or you may want to research health clinics in the area without attracting the suspicion of your employer. If you live outside the U.S., you may want to know your ISP isn't selling your online activity to strangers.

A PVN encrypts your internet traffic and changes your IP address, making it almost impossible to link it to you. It keeps you from leaving a digital footprint of your online whereabouts for your ISP and other third parties to track.