A Virtual Private Network or a VPN is a useful tool in the online world. Its basic application is security and anonymity on the internet by encrypting your data. Recently, VPN usage has gained more popularity due to its purpose of providing online security. Furthermore, internet users have found its applications beyond security and also use it for streaming, shopping, and travelling.

In this article, we will list down 10 uses of VPN that you may not be aware of. Let’s have a look at each of them.

1. **Shopping online from a different location**

Suppose that you are currently out of country, but you want to buy something and want it to be delivered to you by the time you reach back home. If you go to the website, you will land on the country-specific page according to your current location. Using a VPN server of your home country will help you access your website just like as if you are present there. You can use your [local credit card](http://www.cardzgroup.com/PvcCard.html) or bank account to purchase and ship the item to your home address.

1. **Avoiding being tracked by Internet Service Providers**

ISPs nowadays track their subscribers, mainly for the purpose of targeted advertising. Too much of targeted advertisements can sometimes interfere in your routine browsing, and many users prefer to seek anonymity. Not only this, but ISPs have recently found to be selling their user’s data, including browsing history, app usage, and location data to third parties.

1. **Accessing your home network**

You may have a home desktop with a large collection of important files that you would want to access from a remote location one day. The best and most secure way to do that is by using a VPN.

1. **Using public Wi-Fi Safely**

Many public places have free Wi-Fi access for facilitating users. These include hotels, schools, restaurants, airports, and libraries. However, public Wi-Fis are not secure and hackers can easily get your sensitive information such as passwords or payment card details.

If you have no other option but to use a public Wi-Fi, it is best to use a VPN so that your traffic is encrypted. This means that your data is scrambled even if someone tries to intercept it.

1. **Preventing websites from gathering your information**

Just like ISPs, websites also gather user information such as the pages they clicked, the time they spent on a particular page, or the products they bought. This information is then sold to third parties who target users by advertising them to buy same products or services.

If this kind of unnecessary targeted advertising concerns you, using a VPN is a good way to hide your real IP and sidestep unnecessary ads.

1. **Streaming Geo-Restricted Content**

Geo-blocking means that a particular content is blocked in some parts of the world. For instance, accessing iPlayer is blocked for users outside the UK. You must have to respect and adhere to a website that does not allow content to be displayed in your country. However, sometimes if you are travelling outside of your country and need to watch the next episode of your favorite series on the website that is blocked in the country you are visiting, using a VPN is your best bet.

1. **Connecting to on-campus resources**

Your campus can be a college or a workplace. Universities have information and computer resources that can benefit their students, but the same information cannot be accessed outside the campus due to security concerns. If you wish to access your campus resources remotely, a VPN can admirably perform this task for you.

1. **Avoiding Hackers**

You may have known that firewalls keep hackers and malicious users away from your home network. These cybercriminals use your IP address to find your network. With a VPN, you are connected to a server that is offsite, and thus you get a different IP address. If any attack takes place, it is actually directed against the VPN server. Thus, a VPN gives additional security and keeps you away from cybercriminals.

1. **Using VoIP**

In many countries, voice calling apps like WhatsApp and Skype are banned, mostly to promote local voice calling apps. If you are living in such a country and you really need to make and receive calls through these apps, you can do so by using VPN.

1. **Escaping Data Throttling**

Data throttling happens when you use a certain amount of data, and afterwards, the ISP slows down the service for you. By using a VPN, you can not only keep prying eyes of ISPs away from your activity, but also stop it from putting a data cap on you.

**Choosing a VPN**

When choosing a VPN, go for the one that is affordable and also fulfils your purpose. A free VPN service may not provide all the features you are looking for. Also, if a VPN service is not charging fees to its users, it may pay for the costs incurred by collecting and selling your data to a third party, or through advertising. If you truly value your privacy online, choosing a paid service is a desirable option. A VPN should offer secure private network that helps keep personal information safe from hackers and cyber criminals.