Virtual Private Networks (VPNs)

A VPN creates a secure connection between you and the internet. When you connect to the internet via a VPN, all your data is sent through an encrypted “virtual tunnel”. This has three main advantages:

1) **Hide your identity and location.** You are anonymous on the internet. Your real IP address and location are hidden.

2) **Your data is secure.** You are safer on the internet - the encrypted tunnel keeps you safe from hackers and cybercriminals.

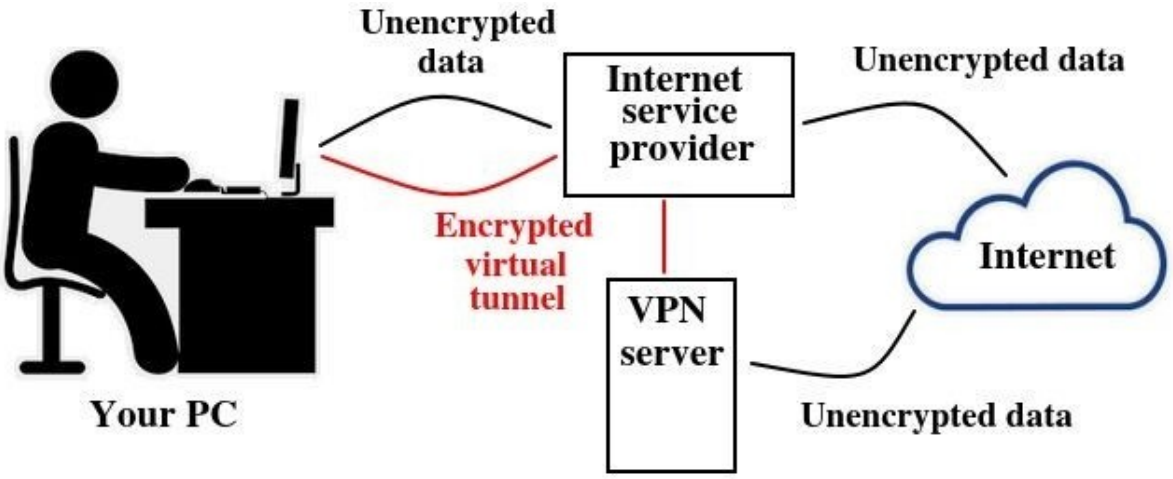
3) **Total access to the internet.** If you live in a country which restricts internet services, they are no longer restricted. You can access all websites and online services.

A VPN sends your data via an encrypted connection to a VPN server. From there, your data is sent to its final destination. Connecting to a VPN is very simple:

1) Firstly, you subscribe to a “VPN provider”. This usually has a small cost, but some are free.
2) Secondly, you download and install “VPN client software”.
3) Thirdly, you run the software and select a server that you want to connect to.
4) The VPN software will do the rest!

When a VPN connection is established, this is what happens to your data:

1) The VPN software encrypts your data and sends it to a VPN server through a secure connection. The data also goes through your Internet Service Provider, but they can’t “see” your data, because it is encrypted.
2) The encrypted data from your computer is decrypted by the VPN server.
3) The VPN server then sends anonymous data, together with its IP address, to a website. The website cannot “see” who you are nor your location. It knows, however, that a VPN is in use. Note that some websites deny communication with a VPN server.
4) The VPN server receives a reply from the website.
5) The data is encrypted again by the VPN server and then sends it back to your computer.
6) The VPN software on your computer decrypts the data so that you can understand and use it.



The VPN client software runs in the background of your computer, tablet, or smartphone. You can access the internet normally, and you don't notice anything different. Depending on your VPN provider, you may notice a small reduction in the speed of your internet traffic.

Exercise 1. Find out what your IP address is, for example using: https://ipleak.net/ Then connect to your VPN and check again. Your IP address will be different.

Exercise 2. Watch this short video (02:27) about VPNs:
https://www.youtube.com/watch?v=o6Fzq1PEQb4

Now let's look in more detail at the advantages of a VPN:

1. Anonymity
Without a VPN your location and your identity can be discovered very easily, thanks to your IP address. This IP address is unique to your internet connection. It is like an online postal code that tells people who you are and where you are. A VPN hides your IP address and location. When you use a VPN, your internet traffic is rerouted through a VPN server and your online activities can only be traced back to that server, but not your computer. By using a VPN, websites, marketeers, streaming services, commercial organizations, governments and cybercriminals can't identify you by your IP address, because they only see the IP address of the VPN server. Also, they can't see your real location, because it will seem that you are where the VPN server is. So, by using a VPN, your online activity is not linked to your real IP address. This way, you can browse the internet with complete anonymity. A VPN also makes sure that nobody knows what you are downloading or uploading.

2. Protection against hackers
A VPN encrypts your data through strong encryption protocols, which make intercepting and reading your data almost impossible. Why is this important? Well, these days, there are many companies, governments and cybercriminals that want to see what you are doing online. The security that a VPN offers makes it almost impossible for them to look at your data. This increases your online safety. However, a VPN isn't the ultimate solution to all cybercrimes. We recommend combining a VPN with a good antivirus package, to keep you completely safe.

3. Secure browsing
Using a public Wi-Fi network can be very risky. Other users on the same network (for example hackers) can easily tap into your data and personal information. Since you don't want others to have access to, for example, your logins, images, documents or credit card information, it is always wise to use a VPN connection.

4. Fight online censorship
In a lot of countries (like China, Turkey, Russia and Iran) governments heavily censor the internet. These countries block access to certain internet services and websites. Examples of apps and websites that are often blocked are WhatsApp, Google, Instagram, YouTube, Skype, Spotify and Facebook. Also, news websites and journalist platforms are often blocked because they are seen as a threat to the nation's government. In these countries, this censorship prevents the freedom of speech of their citizens. In some western countries there are also some online restrictions. For example, many countries block the Pirate Bay website because they do not want their citizens to download illegal materials. A VPN can help you bypass censorship and restrictions by allowing you to connect to a server in a different country. By doing this you can go online as if you were in that other country. This way you can gain access to websites and services that are not available in your own country.

5. Bypass geographical restrictions

It's not just countries that impose restrictions on the internet. Some online services also restrict access to their content in certain regions. This happens with streaming services that only have broadcasting rights in certain countries and not in others. If you are on holiday, or if you move to a different country, you might be unable to view your usual streaming services. A VPN will enable you to connect to the internet via servers in your home country, so that you can watch your favorite shows. It also works the other way around - if you want to gain access to streaming services from a different country (for example to watch a different version of Netflix), you can do so with a VPN.

6. Avoid Big Brother

Advertising networks such as Facebook, Google, and Twitter are constantly collecting information about you through your online traffic. With this information, they can show you tailored ads but more importantly, they are free to sell this information to a third party. By encrypting your data using a VPN, these networks will have a harder time collecting information about you. They will also have less influence on what you see online.

7. Working from home

More and more companies are giving people the possibility to work from home or abroad. Some people connect to the internet via a VPN to access the company network at home. This enables people to work from home safely and efficiently.

What Limitations do VPNs Have?

1) Cookies

A VPN connection does not control cookies on your computer. It's recommended that you regularly clear your cookies.

2) Logged in

Let's suppose that you're logged in to your Google account. You can be connected to a VPN on the other side of the world, but Google can still maintain a profile of you as an internet user. The same is true for services like Facebook.

3) GPS

When using Google Maps, you're often required to turn on your GPS. This means that Google can see exactly where you are.

4) Browser fingerprinting

There are some advanced methods to identify internet users, such as "browser fingerprinting". This method uses your browser's and device's settings to distinguish you from other internet users.

5) Speed

A VPN can slow down your internet connection.

6) VPNs not welcome

VPNs are banned in some countries. There are also some websites, apps and services that will deny you access if you use a VPN.

Is a VPN Safe?

You may wonder how safe you are with a VPN provider. Your internet traffic is redirected through the servers of the VPN provider. The provider can see everything you do if it wants to. Therefore, it's important that you have confidence in your VPN service. Most VPN services do not log what you do and don't store your data.

However, there are some VPN providers that abuse the data that travels through their servers and sell your data to advertisers. This happens more frequently with free VPNs. These are not safe. Before using a VPN, it is therefore important that you do research in advance.

Is Using a VPN Legal?

Some people wonder whether it's legal to use a VPN. After all, the service enables you to become anonymous online, which is very useful for hackers and online criminals. If those people can't be traced online, it's much harder to punish them for their crimes. Even so, this doesn't mean that using a VPN is illegal. On the contrary - many companies and businesses work with VPNs and recommend their use. The European Union, too, supports internet freedom, which a VPN can give you.

Many countries consider the use of a VPN completely legal. Conducting illegal activities while using a VPN, however, remains illegal. Therefore, using a VPN for legal activities, such as browsing, gaming, Netflix, and YouTube, isn't a problem at all. If you use a VPN to download illegal files, such as unofficial copies of movies and music, then you're breaking the law in your country. While the VPN gives you anonymity online and makes it harder for officials to trace you, such downloading is still illegal.

There are some countries that consider the use of a VPN illegal, such as China, Russia and Iran. These countries have dictatorial regimes or authoritarian leaders.

Source: https://vpnoverview.com/vpn-information/what-is-a-vpn/