# What is VPN? -IW9

# A virtual private network, or VPN, is a service that creates an encrypted tunnel to transmit data over the internet while ensuring the user’s online privacy and protecting sensitive data. Unlike [website security](https://www.wix.com/blog/2022/01/website-security/) tools used by site owners to protect visitors’ information on certain pages, VPNs keep users secure through their entire online journey *by hiding their* [*IP address*](https://www.wix.com/encyclopedia/definition/ip-internet-protocol-address) in order to make any action virtually untraceable.

A VPN works by creating a secure and private data tunnel between your computer and a server in another location, successfully masking your data and allowing you to browse the internet from a secondary location. In order to do so, the VPN first uses encryption to scramble all data sent over a Wi-Fi connection and make it unreadable. Then, it directs your traffic to a VPN server before forwarding to the rest of the web, thus concealing your IP address and showing only the VPN address to any websites and services you use.

As a result, anyone with the ability to see your online journey when navigating without a VPN - such as your internet provider, the government, other users on your shared network and even random strangers - will find it nearly impossible to view your identity, location or activities.

No one likes to feel like they’re being watched, even if they have nothing to hide. This is why as people become more conscious of their online privacy and the amount of data they’re sharing publicly, the use of VPNs is raising exponentially.

If you’re still wondering whether you need a VPN, here are some of the most important reasons why you should be using one:

Using public Wi-Fi

Connecting to public Wi-Fi, such as free internet hotspots offered in cafes, parks and airports, leaves your data at the mercy of hackers. These types of unprotected networks are usually a goldmine for hackers, but using a VPN to encrypt your data will protect you against their attacks.

Masking your location

For people living under authoritarian regimes, VPNs offer a secure way to create private networks that allow them to work and share sensitive messages without being limited by the country’s limited freedom of speech.

Accessing blocked content

In spite of the internet’s role in globalization, there’s still a lot of content restricted to certain geos. Whether you’re facing government censorship or simply copyright issues, changing your location using a VPN will allow you to bypass this blockage.

Streaming without restrictions

While streaming services like Netflix and HBO are available in hundreds of countries around the world, the extension and content of their media libraries depends on where you’re watching from. For example, while Netflix US library contains over 1,800 TV shows, only 17% of those are available in Netflix Italy. In order to gain access to the entire catalog regardless of your location, you can use a VPN to connect to the geographic area of your choice.

**Avoiding tracking and surveillance**

By using a VPN to encrypt your traffic and IP address, you’ll prevent government agencies from collecting your online activity, messages, social interactions and other private data.

**Playing online videogames**

The benefits of using a VPN for gaming are threefold. First, and most importantly, you’ll be protected from DDoS attacks and doxxing. Second, it will allow you to evade bandwidth throttling and reduce ping and lag. And lastly, you’ll be able to access maps, skins and add-ons restricted to certain geos.

**Encrypting your data**

Using a VPN to change your IP address will minimize your online footprint and protect your identity from websites and services that want to track you. Additionally, by encrypting your data you’ll hinder your internet service provider’s ability to sell your information to third parties.

**Getting better prices**

[Online stores](https://www.wix.com/blog/ecommerce/2020/01/how-to-set-up-and-manage-your-online-store-with-wix) and service providers generally show different prices depending on the site visitors’ geo. Changing your location using a VPN will allow you to find better deals and benefit from regional sales, all while avoiding commercial targeting. This is especially valuable in the travel industry, as airlines, hotels and rentals tend to show better deals for locals.

### What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

**Secure encryption:** To read the data, you need an encryption key . Without one, it would take millions of years for a computer to decipher the code in the event of a [brute force attack](https://www.kaspersky.com/resource-center/definitions/brute-force-attack) . With the help of a VPN, your online activities are hidden even on public networks.

**Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

**Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively “change” your location.

**Secure data transfer:** If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

### What should a good VPN do?

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

* **Encryption of your IP address:** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
* **Encryption of protocols:** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
* **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
* **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

What kind of VPNs are there?

There are many different types of VPNs, but you should definitely be familiar with the three main types:

### SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an **SSL-VPN** solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

### Site-to-site VPN

A **site-to-site VPN** is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

### Client-to-Server VPN

Connecting via a **VPN client** can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

This involves the user not being connected to the internet via his own ISP, but establishing a direct connection through his/her VPN provider. This essentially shortens the tunnel phase of the VPN journey. Instead of using the VPN to create an encryption tunnel to disguise the existing internet connection, the VPN can automatically encrypt the data before it is made available to the user.

This is an increasingly common form of VPN, which is particularly useful for providers of insecure public WLAN. It prevents third parties from accessing and compromising the network connection and encrypts data all the way to the provider. It also prevents ISPs from accessing data that, for whatever reason, remains unencrypted and bypasses any restrictions on the user's internet access (for instance, if the government of that country restricts internet access).

The advantage of this type of VPN access is greater efficiency and universal access to company resources. Provided an appropriate telephone system is available, the employee can, for example, connect to the system with a headset and act as if he/she were at their company workplace. For example, customers of the company cannot even tell whether the employee is at work in the company or in their home office.

References and much more:

<https://youtu.be/_wQTRMBAvzg>

<https://youtu.be/_-DekqEyAV0>

<https://www.wix.com/encyclopedia/definition/virtual-private-network>