

What is VPN? How It Works, Types of VPN

VPN stands for "**Virtual Private Network**" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

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](#) . 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.


Browse like nobody's watching

Hide your online actions with VPN, included in our premium product.



Kaspersky
Total Security

Explore Now



Why should you use a VPN connection?

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

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.

The history of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defense already got involved in projects working on the encryption of internet communication data back in the 1960s.

The predecessors of the VPN

Their efforts led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).

The **TCP/IP** had four levels: **Link, internet, transport and application**. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as swlPe: Software IP encryption protocol.

In the following year, Wei Xu developed the IPSec network, an internet security protocol that authenticates and encrypts information packets shared online. In 1996, a Microsoft employee named Gurdeep Singh-Pall created a Peer-to-Peer Tunneling Protocol (PPTP).

Early VPNs

Contiguous to Singh-Pall developing PPTP, the internet was growing in popularity and the need for consumer-ready, sophisticated security systems emerged. At that time, anti-virus programs were already effective in preventing malware and spyware from infecting a computer system. However, people and companies also started demanding encryption software that could hide their browsing history on the internet.

The first VPNs therefore started in the early 2000s, but were almost exclusively used by companies. However, after a flood of security breaches, especially in the early 2010s, the consumer market for VPNs started to pick up.

VPNs and their current use

According to the ***GlobalWebIndex***, the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, **one in fiveinternet users** uses a VPN. In the USA, Great Britain and Germany, the proportion of VPN users is **lowerat around 5%**, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions. For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries. With contemporary VPNs, you can encrypt your IP address so that you appear to be surfing from another country, enabling you to access this content from anywhere.

Here’s how to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

1. Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
2. Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
3. You can now surf the internet at will, as the VPN protects all your personal data.

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.

How do I install a VPN on my computer?

Before installing a VPN, it is important to be familiar with the different implementation methods:

VPN client

Software must be installed for standalone VPN clients. This software is configured to meet the requirements of the endpoint. When setting up the VPN, the endpoint executes the VPN link and connects to the other endpoint, creating the encryption tunnel. In companies, this step usually requires the entry of a password issued by the company or the installation of an appropriate certificate. By using a password or certificate, the firewall can recognize that this is an authorized connection. The employee then identifies him/herself by means of credentials known to him/her.

Browser extensions

VPN extensions can be added to most web browsers such as Google Chrome and Firefox. Some browsers, including Opera, even have their own integrated VPN extensions. Extensions make it easier for users to quickly switch and configure their VPN while surfing the internet. However, the VPN connection is only valid for information that is shared in this browser. Using other browsers and other internet uses outside the browser (e.g. online games) cannot be encrypted by the VPN.

While browser extensions are not quite as comprehensive as VPN clients, they may be an appropriate option for occasional internet users who want an extra layer of internet security. However, they have proven to be more susceptible to breaches. Users are also advised to choose a reputable extension, as ***data harvesters*** may attempt to use fake VPN extensions. Data harvesting is the collection of personal data, such as what marketing strategists do to create a personal profile of you. Advertising content is then personally tailored to you.

Router VPN

If multiple devices are connected to the same internet connection, it may be easier to implement the VPN directly on the router than to install a separate VPN on each device. A router VPN is especially useful if you want to protect devices with an internet connection that are not easy to configure, such as smart TVs. They can even help you access geographically restricted content through your home entertainment systems.

A router VPN is easy to install, always provides security and privacy, and prevents your network from being compromised when insecure devices log on. However, it may be more difficult to manage if your router does not have its own user interface. This can lead to incoming connections being blocked.

Company VPN

A company VPN is a custom solution that requires personalized setup and technical support. The VPN is usually created for you by the company's IT team. As a user, you have no administrative influence from the VPN itself and your activities and data transfers are logged by your company. This allows the company to minimize the potential risk of data leakage. The main advantage of a corporate VPN is a fully secure connection to the company's intranet and server, even for employees who work outside the company using their own internet connection.

Can I also use a VPN on my smartphone or other devices?

Yes, there are a number of VPN options for smartphones and other internet-connected devices. A VPN can be essential for your mobile device if you use it to store payment information or other personal data or even just to surf the internet. Many VPN providers also offer mobile solutions - many of which can be downloaded directly from Google Play or the Apple App Store, such as [Kaspersky VPN Secure Connection](#).

Is a VPN really so secure?

It is important to note that VPNs do not function like comprehensive anti-virus software. While they protect your IP and encrypt your internet history, a VPN connection does not protect your computer from outside intrusion. To do this, you should definitely use anti-virus software such as [Kaspersky Internet Security](#) . Because using a VPN on its own does not protect you from Trojans, viruses, bots or other malware.

Once the malware has found its way onto your device, it can steal or damage your data, whether you are running a VPN or not. It is therefore important that you use a VPN together with a comprehensive anti-virus program to ensure maximum security.

Selecting a secure VPN provider

It is also important that you choose a VPN provider that you can trust. While your ISP cannot see your internet traffic, your VPN provider can. If your VPN provider is compromised, so are you. For this reason, it is crucial that you choose a trusted VPN provider to ensure both the concealment of your internet activities and ensure the highest level of security.

How to install a VPN connection on your smartphone

As already mentioned, there are also VPN connections for Android smartphones and iPhones. Fortunately, smartphone VPN services are easy to use and generally include the following:

- The installation process usually only downloads one app from the iOS App Store or Google Play Store. Although free VPN providers exist, it's wise to choose a professional provider when it comes to security.
- The setup is extremely user-friendly, as the default settings are already mostly designed for the average smartphone user. Simply log in with your account. Most apps will then guide you through the key functions of the VPN services.
- Switching on the VPN literally works like a light switch for many VPN apps. You will probably find the option directly on the home screen.
- Server switching is usually done manually if you want to fake your location. Simply select the desired country from the offer.
- Advanced setup is available for users requiring a higher degree of data protection. Depending on your VPN, you can also select other protocols for your encryption method. Diagnostics and other functions may also be available in your app. Before you subscribe, learn about these features to find the right VPN for your needs.
- In order to surf the internet safely from now on, all you have to do is first activate the VPN connection through the app.

But keep the following in mind: A VPN is only as secure as the data usage and storage policies of its provider. Remember that the VPN service transfers your data to their servers and these servers connect over the internet on your behalf. If they store data logs, make sure that it is clear for what purpose these logs are stored. Serious VPN providers usually put your privacy first and foremost. You should therefore choose a trusted provider such as [Kaspersky Secure Connection](#) .

Remember that only internet data is encrypted. Anything that does not use a cellular or Wi-Fi connection will not be transmitted over the internet. As a result, your VPN will not encrypt your standard voice calls or texts.

Conclusion

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks. That's because only you can access the data in the encrypted tunnel – and nobody else can because they don't have the key. A VPN allows you to access regionally restricted content from anywhere in the world. Many streaming platforms are not available in every country. You can still access them using the VPN. VPN solutions from Kaspersky are available for both [Windows PCs](#) and [Apple Macs](#).

There are now also many providers of VPN connections for smartphones which keep mobile data traffic anonymous. You can find certified providers in the [Google Play Store](#) or the [iOS App Store](#). However, remember that only your data traffic on the internet is anonymized and protected by using a VPN. The VPN connection does not protect you from hacker attacks, Trojans, viruses or other malware. You should therefore rely on an additional trusted [anti-virus software](#).

What security solutions include VPN protection?

[Kaspersky VPN Secure Connection](#)

[Kaspersky Anti-Virus](#)

[Kaspersky Internet Security](#)

[Kaspersky Total Security](#)

[Kaspersky Security Cloud](#)

More articles about VPN (Virtual Private Network)

[Work securely online in your home office](#)

[Security of public WiFi networks](#)

[Defence against a man-in-the-middle attack](#)