VPN – Virtual Private Network

The Internet takes away more and more of our privacy. Data disclosed by our browsing behaviour, e. g. our search requests, are used by both organisations and crooks for their own ends, such as market analyses or criminal machinations. Such data can be protected by a VPN.

Tips on using a VPN

- Only use a renowned and trustworthy VPN provider, for instance ProtonVPN (https://protonvpn.com/) , NordVPN (https://nordvpn.com/) or ExpressVPN (https://www.expressvpn.com/) .
- Please remember though that even a VPN provider cannot guarantee 100% security.
- Take into account that only the connection up to your VPN provider (VPN server) is protected.

VPN: A secure "tunnel" through the Internet

Usually, your browser will directly contact the required web server when you visit a website or online shop. This will result in data, for instance your location, being transmitted directly. If you access a website via a VPN provider, it will be interposed in all communications. Your browser therefore first connects to your VPN provider via an encrypted connection, which will then contact the website requested. Please note however that a connection between your VPN provider and a website might still remain unprotected under certain circumstances.

A VPN should not be mistaken for an "https" connection. Unlike a VPN, "https" will only ensure that the communication between your browser and the website you visit is encrypted. A VPN however encrypts all communications between your device and your VPN server, for instance your e-mail communications as well.

A VPN can be integrated into the settings of each relevant device.

Windows

In Windows 11, you can either directly integrate a VPN connection into your network settings ("VPN settings") or use the software offered by your VPN provider for this purpose. In any case, you will need a VPN provider, e. g.

- ProtonVPN (also have a free version) (https://protonvpn.com/)
- NordVPN (https://nordvpn.com/)
- ExpressVPN (https://www.expressvpn.com/)

macOS

In macOS, a VPN connection is integrated directly into your network settings once you have downloaded and installed the app. You can also use your VPN via software offered by providers. You will always need a VPN provider, e.g.:

- ProtonVPN (also have a free version) (https://protonvpn.com/)
- NordVPN (https://nordvpn.com/)
- ExpressVPN (https://www.expressvpn.com/)

📱 Smartphone and tablet

On a smartphone or tablet, you will need to install and use the app offered by the provider, e.g.

- ProtonVPN (also have a free version) (https://protonvpn.com/)
- NordVPN (https://nordvpn.com/)
- ExpressVPN (https://www.expressvpn.com/)

A VPN can make sense in a variety of situations:

- **Working from home or remotely:** If you work from home or any other place outside an office, a VPN ensures secure access to your organisation’s network.
- P**rivacy protection:** VPN are also useful if you would like to protect your online activities from prying eyes. This way, you can stop criminals or organisations aiming to send you targeted adverts gaining access to your data to analyse your user behaviour.
- **Browsing on public Wi-Fi connections:** Public Wi-Fi networks are frequently not sufficiently secure. If you use a VPN, your data will be protected better on such networks, too.
- **Abroad:** If you use a VPN abroad, you will benefit from increased anonymity. Despite your change in location, this will for instance enable you to watch TV programs back home without any limitations. In countries implementing severe Internet restrictions, a VPN will enable you to access Internet pages which would otherwise not be available. When planning any long-distance journeys you should note that VPNs are prohibited in some countries and that you could end up getting into trouble with their laws by unthinkingly using them. It is in countries censoring the Internet in particular that VPNs are prohibited.
- **Online shopping:** If you would like to save money online shopping, a VPN could also come in useful. Due to your apparently different location, you will be able to access lower-priced offers in other countries.

Please note that no VPN can offer 100% protection. It simply moves the target: Instead of data being read during transmission between your device and a website, they might now be read between a VPN server and a website. VPN providers themselves could theoretically also access your data.

How to find the right VPN provider?

The number of VPN providers is steadily increasing. Due to VPNs becoming ever more popular, new providers keep appearing on the market, so that it can be quite a challenge finding the right one for you. Amongst other things, a renowned and trustworthy VPN provider offers strong encryption, does not keep any logs of your actions on the VPN and does not pass on any data.

You should therefore check the following when choosing a VPN provider:

- **Provider location:** Consider where the provider has its registered office. Some countries have more stringent data protection laws than others. In countries such as Switzerland or Germany, your data are generally better protected.
- **Reputation:** Look for online reviews and consider both positive and negative ratings.
- **Encryption and security protocols:** Make sure your VPN provider uses strong encryption (e. g. AES-256, currently considered secure) and employs strong security protocols such as OpenVPN or IKEv2.
- **No logs (No-log policy):** Select a provider with a strict no-log policy. This means a provider does not store any data in connection with your Internet activities.

A Virtual Private Network (VPN) is an encrypted "tunnel" between your device and the VPN provider via the Internet.

VPNs are generally used to connect a device via an existing (unsecured) network, e.g. the Internet, with another (secured) network, e.g. your company network, in a secure manner. In the process, content is protected by way of encryption (end to end encryption) during transmission.