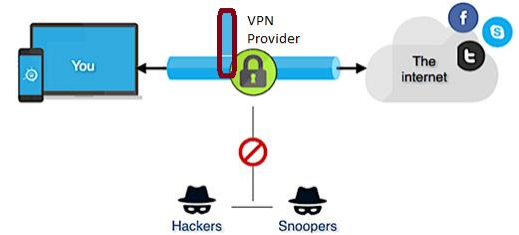


## Use of commercial VPN to protect to your online privacy

A virtual private network or VPN is a type of electronic communication to secure connections between two points. VPN is usually used by organisations to allow users to communicate over wider networks in a private way to protect the data being exchanged.

The focus of this article is on commercially available VPNs that allow users to communicate securely to various sites over the Internet. This article does not address the use of specific VPN to access internal corporate resources (e.g. clinic/hospital systems, shared files, etc.) Please contact your IT for instructions related to your organization.



A commercial VPN creates a secure, encrypted connection - which can be thought of as a tunnel - between your device and a server operated by the VPN service. While connected, all network traffic passes through this protected tunnel, and data sent and received is encoded.

### When to use a VPN

- Anytime you need to access or share critical information over a Wi-Fi or networks with unknown security levels – e.g. when travelling and access Wi-Fi at hotels, airports, and coffee shops.
- To bypass geo-block or restricted content and resources based on location or IP (Internet Protocol) addresses.
- To reduce sites tracking that collects information about your clicks, interests, and behaviour for later use in advertising.
- When shopping online, some sites (e.g. book flights) tend to change prices depending on your location.



Note: Using a VPN cannot help if you unwisely download ransomware or malware from a site, or if you are tricked into giving up your data through a phishing attack. Even though using a VPN increases your overall online privacy with traffic encryption, the site you visit can still see what you do on their site.

### Situations when you should not use VPN

- In countries where regulations do not allow it. Check the local laws in advance of such use.
- When restrictions are imposed on specific range of IP addresses or country boundary. For instance, some organizations restrict access to their services from specific geographical boundaries.
- If you are experiencing speed issues, it is possible that connecting to a VPN will slow you down even more.
- If you transfer money (e.g. using PayPal or online banking) and your VPN IP address indicates a different country, there is a possibility that the provider locks your account to prevent it from being hacked by cybercriminals.

Note: Some services have built in protections against possible hacker activities. If they notice your access from multiple countries or IP addresses within a short time, access may get denied or account locked.

### General recommendations

- Obtain VPN from a well-reputed provider who has been in business for a long time.
- Before subscribing, carefully read the end user agreement and fine print to understand their privacy policy.
- Avoid free VPNs since they have limitations (encryption, speed, etc.) which reduce the expected benefits.
- Look for VPN that provides you with various features including encryption strength (AES-256, or better), unlimited data usage, various server locations, higher compatibility, speed, non-logging policy, Ad tracker blocking, and extended support.

For more content

- [Best VPNs for Canada in 2019](#)

- [How to choose the VPN that is right for you](#)