

Virtual Private Network (VPN)

Current Internet Connection:

→ ISP: Internet Service Provider can see which website you are accessing

→ HTTPS: Secures most website connections (internet traffic is being encrypted)

→ Your online activity is always being tracked by more companies you might realize (using tools like cookies)

→ IP: Internet Protocol addresses get assigned to every device → provides Information about your geographic location

→ Security & privacy is a product of TRUST → We can encrypt our data and transit! How about your log in data/information or credit card information? You have to trust the ISP, owner of Wi-Fi and **VPN companies** (It is impossible to be 100% private)

VPN: It is a good tool for location spoofing, and it allows to hide your location and make the internet think you are located somewhere else. The most common use is streaming blackout content from major networks or geographic restricted content on platforms like Netflix and Disney+

Example: Thailand hasn't got Disney+, however by connecting to a VPN server in the US and paying for my Disney+ subscription fee I can → access this geo restricted content as if I were in the US

Ironically, the last legitimate reason to use a VPN is that it was initially developed for encrypted data. VPN doesn't make that connection stronger; it just acts as a safety network. However, VPN does encrypt your Domain Name System (DNS) request. Web browser → Internet → DNS Server. VPN will hide the information, for example, the ISP and the connection with your university (university doesn't know anything about your connection).

VPN does not do:

1. ...isn't an internet connection
2. ...isn't a cloak of invisibility (first connection with internet and then with VPN). VPN company have access about your activity (Illegal things). China regulates the access of his population on the internet with VPN.
3. Doesn't protect you from viruses. The VPN can encrypt any kind of data including viruses and malware being delivered on your devices

Be secure of the threat of the internet: Protect yourself

01: Better password, 02: Using 2FA, 03: Monitor Identify, 04: Be skeptical