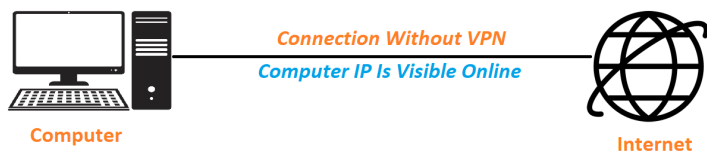


Virtual Private Network



Overview

Virtual Private Network (VPN) basically means that you're routing all of your internet traffic through a remote server before sending it out to the internet. This is a useful service because it adds an extra layer of protection while online. However, before we dive deeper into how a VPN helps protect you. We first need to have a general understanding of encryption and IP addresses.

Every device that connects to the internet is assigned an IP address. This is a string of numbers that identifies your device and allows other devices to communicate with it. This string of numbers can be viewed almost like a street address. For example, let's say you want to try a new restaurant in town but you don't know how to get there. By typing the address into a GPS it will show you the fastest route to reach your destination. An IP address fundamentally works the same way. Now that we know what an IP address is, let's move on to encryption.

Encryption is a way to jumble data into a seemingly useless string of numbers, letters & punctuation that have no meaning. The only way to turn this useless string into something that is readable and makes sense is to have the passkey and algorithm originally used to encrypt it. Below is an example of what encrypted text looks like before and after. Now that we've covered the basic concept of IP's and encryption, let's take a look at how a VPN plays into all this.

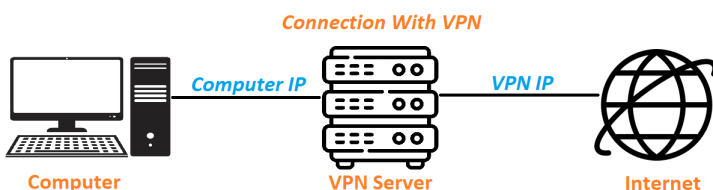
Plain Text

Example of encryption

Encrypted Text

6LQBcKhw04tBUa8/qHQ2s+B88yST2tXn+jT1t75qoU=

VPNs act as a buffer between your device and the rest of the internet by keeping your identity, location and data secure. It does this by creating an encrypted link between your device and the VPN server. This prevents other people from being able to understand your data if they try to intercept it. Once your device hits the VPN server it's assigned a new IP address before being forwarded to whatever website you're trying to access. This is how your identity and location is kept private and secure. On one side of the connection (between your device and the VPN server) anyone trying to view your traffic will only see you connecting to the VPN's IP. On the other side of the connection (between the VPN server and the website) anyone viewing the traffic will only see your VPN's IP and not your personal IP.



In summary, it's easy to see how adding this security feature can affect your connection speed. By adding extra security steps to your internet connection you essentially trade a small amount of your speed for better privacy and protection. Which means you may notice more latency and lag while connected.

Note: Using a VPN won't make your connection 100% safe and secure, nothing will ever be able to do that. However, it does help quite a bit with keeping your data, identity and location safe.