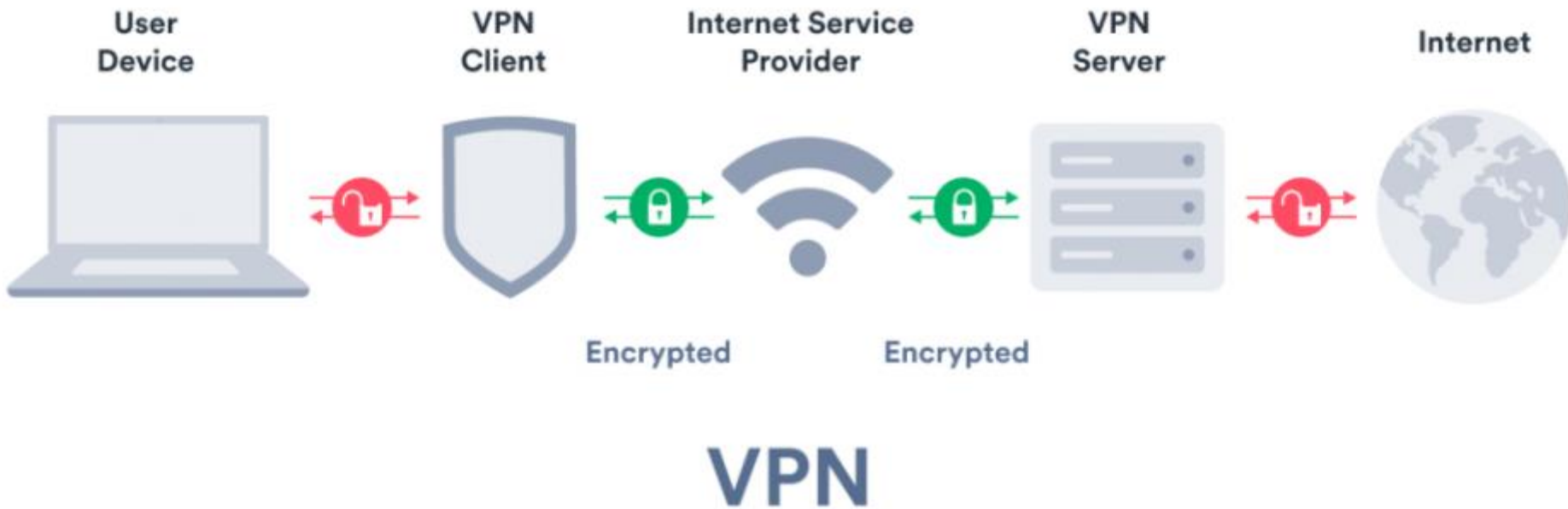
What Is a Virtual Private Network (VPN)?

When you switch on a VPN, it sends your web traffic through an encrypted tunnel to a server controlled by the VPN company. From there, it exits onto the web as normal. If you make sure to only connect to websites secured with HTTPS, your data will continue to be encrypted even after it leaves the VPN.

Think of it like this: If your car pulls out of your driveway, someone can follow you and see where you are going, how long you are at your destination, and when you are coming back. They might even be able to peek inside your car and learn more about you. With a VPN, it's as if you drive from your house into an underground tunnel, into a closed parking garage, switch to a different car, and drive out. No one who was originally following you knows where you went.


User Device
VPN Client
Internet Service Provider
VPN Server
Internet
Encrypted
Encrypted
VPN

Why use a VPN?

A VPN:

- Helps you to stay secure when using **public Wi-Fi hotspots.**
- **Hides your IP** (Internet Protocol) address.
- Encrypts your internet traffic, making your **browsing more secure and private**.
- Ensures that your internet traffic isn’t tracked and recorded, later to be sold by your internet service provider (ISP), ad brokers, or snoops.

What Are the Limitations of a VPN?

VPN services, while tremendously helpful, don't protect against every threat. Using a VPN can't help if you unwisely download ransomware or if you are tricked into giving up your data to a phishing attack.

There's some debate among security experts about the value of VPNs. Since most sites now support secure HTTPS connections, much of your online experience is already encrypted.

Some feel VPNs are overkill. Still, a VPN covers the information not already protected by HTTPS, places an important buffer between you and the people controlling internet infrastructure, and makes online tracking more difficult.

How to Choose a VPN Service

The VPN market has exploded in the past few years, growing from a niche industry to an all-out melee. Many providers are capitalizing on the general population's growing concerns about surveillance and cybercrime, which means it's getting hard to tell when a company is actually providing a useful service and when it's selling snake oil. In fact, there have even been fake VPNs popping up, so be careful.

When looking for a VPN, don't just focus on speed, since that's the factor you and the VPN company have the least control over. Since nearly all VPN companies offer some mixture of the same technologies, consider value instead.

How can you get the most for the least? Look for extra features like split tunneling, multi-hop connections, and so on. You may not need these all the time but they're useful when you do.

You can see PC Magazine’s recommendations of the best VPN services, but if you're in a hurry, here are three to investigate:

- NordVPN
- Surfshark
- VyprVPN

Further Information

The information presented today came from three sources:

1. techadvisor.com

This site has a detailed approach for setting up your VPN
https://www.techadvisor.com/how-to/internet/how-use-vpn-3466190/

2. Pcmag.com

This site recommends VPNs as well as describing what they are:
https://www.pcmag.com/picks/the-best-vpn-services?utm_source=email&utm_campaign=whatsnewnow&utm_medium=title.

3. Surfshark (VPN provider) website:
https://surfshark.com/learn/what-is-vpn