The Complete Guide to VPN

Table of Contents

The internet wasn’t built with your privacy in mind

The internet excels at many things. It enables global communication at the speed of light, the ability to browse without borders, and provides a window into new concepts and ideas that seem to be multiplying by the day. What it’s really, really bad at is protecting our personal privacy.

The fact is, the creators of the internet weren’t concerned about privacy. They were more concerned about getting packets of data from point A to point B. Protocols were built around data failure, not ensuring privacy. While some standards are in use today, there’s no guarantee that the websites you visit or apps you use are protecting your identity at all.

That’s why VPN security is a must-have in today’s world.

A VPN allows you to connect to the internet anonymously. Various protocols create a private network that hides your internet traffic over public Wi-Fi, preventing spying and hacking. In a world where “online privacy” is becoming the biggest oxymoron of our time, think of a VPN as an invisible cloak on the web when you need it.

A closer look at VPNs and how they protect you

VPN is an acronym that stands for “virtual private network.” Just like a firewall keeps your computer’s data safe from outsiders, a VPN keeps your data and identity safe on the web. With a VPN, what you search, the websites you visit, and your sensitive information can’t be read or snooped on.

VPNs protect your privacy and identity in three important ways:

1. By disguising your IP address and geographic location

A VPN can be used to disguise your IP address and location. It does this by creating a data tunnel from your local ISP and placing you onto the web from a completely different gateway city or country. Even if your VPN provider is based in the United States, you can appear to be in places like Canada, Australia, Germany, Turkey, or even the Bahamas. As far as the internet is concerned, you're an online phantom.

2. By encapsulating your internet traffic inside a hidden tunnel

All internet traffic moves across networks in data packets. These packets contain a wealth of information about you, including your IP address, the recipient's IP address, Telnet, BitTorrent, and more. A VPN protects your online traffic by encapsulating any data packets you send inside a secondary, encrypted packet. This process, known as encapsulation, creates an extra layer of security for your data as it travels through the hidden VPN tunnel.

3. By encrypting your data and keeping it private

As your data travels through a private VPN tunnel, it's scrambled via encryption. This scrambling makes your VPN connection virtually impossible to hack. It's like having your own private network inside the public internet that can't be seen or penetrated by outside forces. Some of the most popular types of VPN encryption in use today include OpenVPN, L2TP/IPSec (Layer 2 Tunneling Protocol) and IKEv2/IPSec (Internet Key Exchange version 2).

The fact is, we no longer live in a world where privacy can be taken for granted. This is especially true as we move through the world, using different Wi-Fi connections. While convenient, public Wi-Fi is a hacker's dream, transmitting your data in clear text which can be easily viewed and stolen. Without VPN-level security, it's like stealing candy from a baby.

When you should use VPN-level security

VPNs are convenient and work independently of specific Wi-Fi networks.

The technology is fully portable and can be used over any connection. This means you can use a VPN while traveling, at a library or cafe, or even at home.

You should consider using a VPN when you want to:

Connect to unsecured network. Free Wi-Fi hotspots found at airports, hotels, and cafes are not secure, even with a password. With the right tools and a little know-how, hackers can easily snoop around free Wi-Fi connections. They can read your emails, eavesdrop on your conversations, and steal your logins and passwords. With a VPN, you don't need to worry about this. Your data is always private thanks to tunneling protocols and encryption.

Hide your IP address and geographic location. Your IP address gives your geographic location away. This identifying information can be used to find where you are and where you're browsing. With a VPN, your IP address, identity, and location remain a secret. Anything you do online will appear to be originating from a completely different IP address — the IP address assigned by the VPN.

Prevent spying by websites and advertisers. Companies and websites don't value your privacy. Using your IP address, advertisers and companies can create a profile of your activities. They may not know you by name, but they can track your location, online behaviors, and personal preferences. Instead of leaving a trail of breadcrumbs for every website and marketer to follow — a VPN hides your identity and covers your tracks online.

You should consider using a VPN when you want to:

Help avoid a permanent digital footprint. It's no secret that search engines and popular social networking sites like Facebook are storing lots and lots of personal information about their users. In many cases, this data has a permanent lifespan and can't be easily erased. With a VPN, you can minimize these invasions of your personal privacy.

Bypass content filters and blocked websites. We all want to live in a free world. Yet today, governments actively block websites from other countries. Meanwhile, some companies prevent you from viewing content on their sites if you're not local. They can do this based on your IP address. With a VPN, you can get around censorship and content bans by browsing with an IP address from another country than the one you're actually in.

Circumvent deep packet inspection by ISPs: Deep packet inspection is the process of analyzing data as it passes over a network. Many ISPs perform deep packet inspections of their customers' data for marketing and troubleshooting purposes. A VPN helps thwart these activities.

Are there any risks to using a VPN?

The main job of a VPN is to protect your identity and data. So, it may be surprising to learn that there are shady VPN services that may compromise, rather than protect, your privacy.

These most often come in the form of “free” VPN services which are plagued with security issues, unwanted advertising, and other negatives.

Always be wary of free VPN services that are too good to be true.

Some free VPNs may actually be honeypot services under the hood. A honeypot is a decoy system used by cybercriminals (or government agencies) to lure users and gain unauthorized access to their personal information. If a VPN offers super-fast speeds and multiple locations for free, be suspicious. You should wonder how a company can offer such great service when charging nothing.

Additionally, a lot of free VPN apps for mobile devices may be clickbait VPN companies. These free apps are designed to collect and sell your personal data to third parties or direct you to partner websites. Instead of protecting data, these free services make a profit off of unsuspecting users.

Taking back privacy is your choice

Whether at home or on the road, you shouldn't have to sacrifice online privacy for mobility or convenience. You should have the freedom to use the internet while protecting your private information no matter where you are. FigLeaf wants to restore your autonomy by giving you the tools to control your privacy, any time, anywhere.


figleaf