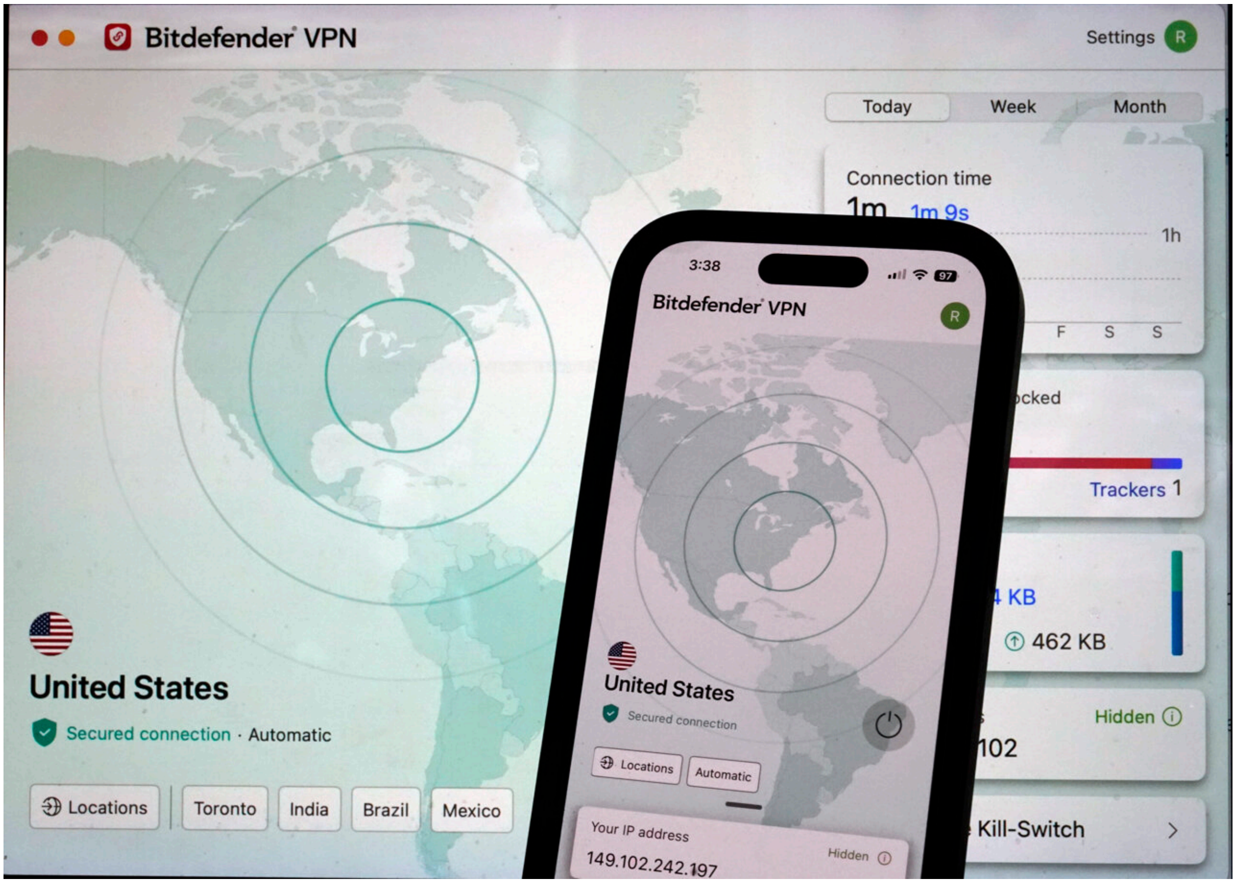
TechXplore

One Tech Tip: To hide your internet activity or your IP address, use a virtual private network

July 25 2024, by Kelvin Chan



Bitdefender's virtual private network connection page is shown on a computer screen and mobile phone screen, in New York, Monday, July 8, 2024. VPNs should be a part of most people's internet security toolbox, to be switched on in certain cases to hide your location or prevent prying electronic eyes from snooping on what you're doing online. Credit: AP Photo/Richard Drew

On the move and looking for an internet connection to check email or post a video to TikTok? It's tempting to jump onto the free Wi-Fi at the coffee shop or the shopping mall. But don't do it unless you've got protection.

Using unsecured internet access can be risky. Hackers can secretly put themselves between you and the internet and view everything you do online, slip malware onto your device or even set up a rogue hotspot that looks authentic. It's one of those times when it's best to use a virtual private network, or VPN.

VPNs should be a part of most people's internet security toolbox. For rookie users, they can initially seem technically bewildering.

What's a VPN?

A virtual private network is a service that hides your online activity from anyone else on the internet. A VPN encrypts your traffic data, which prevents anyone else from being able to read it, and routes it through private tunnels to secure servers around the world.

If normal internet use is like a passing city bus, then using a VPN is like riding in a limo with tinted windows. Anyone can see the bus's passengers and its destination sign. The limo, meanwhile, reveals little to people on the street about what it's carrying or where it's going.

Why do I need to use a VPN?

Privacy is one of the main reasons. If you connect to a free public Wi-Fi network, like at a hotel lobby or coffee shop, using a VPN will prevent anyone from electronically eavesdropping on you.

You can also use it at home if you don't want your internet service provider to know what you're doing. But if that's not a concern, then you probably don't need to as long as your network is password protected.

Another big reason for a VPN is to "spoof" your location, and make it appear like your phone or computer is elsewhere. Pick from a list of countries where your VPN provider has servers and presto, you've got a different IP address that makes a website think you're in, say, Singapore or Germany instead of at your desk in New York or on your phone in London. Now you can access localized versions of websites or stream video only available in a particular country.

VPNs also help people evade censorship in countries with tight internet controls.

Just remember a VPN won't hide everything. If you're logging into your Gmail account, for example, Google will still know who you're emailing.

Aren't VPNs illegal?

VPNs are perfectly legal in most countries. However, they are outlawed or restricted in places where the authorities control internet access or carry out online surveillance and censorship, such as North Korea and China.

How do I choose a VPN?

There are dozens if not hundreds of available VPN services, but not all are credible. Experts warn that some could be run by shady operators.

Start with tech review websites that have tested and analyzed their privacy policies, encryption practices, ease of use, speed, price and other categories. Some review sites rank VPNs according to specific uses like streaming.

Some better-known or established providers include NordVPN, Mullvad, Proton, Surfshark, ExpressVPN and Private Internet Access.

There are a few key features to look out for.

One is a "kill switch" that halts all internet traffic if the VPN's connection goes down, preventing stray bits of data from getting out.

"The kill switch is a pretty powerful security feature," because it will never leave you exposed, said Paul Bischoff, security and privacy advocate at consumer research group Comparitech. But he said some find it annoying because, for example, if your phone switches networks, your connection will go down briefly.

Experts also recommend VPNs with a "no-logging" guarantee. It's a promise that none of your online activity will be recorded. But it's not easy for an ordinary user to verify whether the VPN operator is fulfilling such promises, so look for audits by third-party inspectors.

Expect to pay a monthly fee to use the most reputable VPNs.

What about free VPNs?

Experts warn against using free VPNs because many offer sub-par security or could be harvesting your data.

Bischoff warned some free VPNs could be from rogue operators who disclose little information about who's behind them or the security they're using.

"Some of them are straight up malware," Bischoff said. They might inject ads into your browsing or not be able to unblock many streaming services. Free VPNs also tend to be slower because they "usually have too many users on too few servers," he said.

Some reputable VPNs provide a free version, but they typically come with restrictions such as limiting use to one device or a cap on data. They're a good option if you only need to occasionally browse privately.

Isn't it hard to install and set up a VPN?

You can install a VPN on your computer just like any other piece of software, or on your smartphone as an app. Or you can add it to your browser as a plugin.

Take note that a VPN plugin is mainly useful for quick browsing sessions and helps to block ads and trackers, while computer-based VPNs will cover all your online traffic, giving you more comprehensive protection.

Aren't there a lot of technical settings?

Most VPNs "usually come with pretty secure options straight out of the box," said Bischoff.

"Usually you can just open it and install it and then set it and forget it."

One important choice you'll need to pay attention to is the VPN protocol, which is the set of rules on how data is encrypted and sent over the network.

Most VPN services let you choose one of several protocols. Two of the most widely used are WireGuard, which has speedy connections that make it good for streaming, and OpenVPN, which supports strong encryption and is highly customizable. Both are considered safe and secure.

Are there any downsides?

VPNs tend to reduce your internet browsing speed slightly because all that data has to be encrypted when it goes out and then decrypted when it arrives, which takes a bit of extra time. Bischoff estimates a VPN slows your internet speed by about 5-10%.

You might also encounter more captchas—puzzles designed to weed out bots—or even be blocked by some websites. That's because cybercriminals often use VPNs to conduct their crimes, which leads to their IP addresses getting blacklisted, Bischoff said, adding that's more common with free VPNs.

Comparitech's research has found that some streaming sites are more aggressive at blocking VPN traffic, particularly sports site DAZN and the BBC's iPlayer service.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: One Tech Tip: To hide your internet activity or your IP address, use a virtual private network (2024, July 25) retrieved 26 July 2024 from https://techxplore.com/news/2024-07-tech-internet-ip-virtual-private.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.