The New York Times https://www.nytimes.com/2021/10/06/technology/personaltech/are-vpns-worth-it.html

TECH FIX

It’s Time to Stop Paying for a VPN

Many virtual private network services that were meant to protect your web browsing can no longer be trusted. Here are other ways.

By Brian X. Chen

Oct. 6, 2021

I’m done with paying for a virtual private network, a service that claims to protect your privacy when you’re connected to a public Wi-Fi network at the local coffee shop, the airport or a hotel.

For more than a decade, security experts have recommended using a VPN to shield your internet traffic from bad actors who are trying to snoop on you. But just as tech gadgets become outdated over time, so does some tech advice.

The reality is that web security has improved so much in the last few years that VPN services, which charge monthly subscription fees that cost as much as Netflix, offer superfluous protection for most people concerned about privacy, some security researchers said.

Many of the most popular VPN services are now also less trustworthy than in the past because they have been bought by larger companies with shady track records. That’s a deal-breaker when it comes to using a VPN service, which intercepts our internet traffic. If you can’t trust a product that claims to protect your privacy, what good is it?

“Trusting these people is really critical,” Matthew Green, a computer scientist who studies encryption, said about VPN providers. “There’s no good way to know what they’re doing with your data, which they have huge amounts of control over.”

I learned this the hard way. For several years, I subscribed to a popular VPN service called Private Internet Access. In 2019, I saw the news that the service had been acquired by Kape Technologies, a security firm in London. Kape was previously named Crossrider, a company that had been called out by researchers at Google and the University of California for developing malware. I immediately canceled my subscription.

In the last five years, Kape has also bought several other popular VPN services, including CyberGhost VPN, Zenmate and, just last month, ExpressVPN in a $936 million deal. This year, Kape additionally bought a group of VPN review sites that give top ratings to the VPN services it owns.

A Kape spokeswoman said that Crossrider, which has long been shut down, was a development platform that was misused by those who distributed malware. She said Kape’s VPN review sites maintained their independent editorial standards.

“It kind of sets a concerning precedent from the consumer standpoint,” said Sven Taylor, the founder of the tech blog Restore Privacy. “As the average user goes online to look for information about the product, do they know that what they’re reading might have been written by the company that owns the end product?”

A caveat: VPNs are still great for some applications, such as in authoritarian countries where citizens use the technology to make it look as if they are using the internet in other locations. That helps give them access to web content they cannot normally see. But as a mainstream privacy tool, it’s no longer an ideal solution.

This sent me down a rabbit hole of seeking alternatives to paying for a VPN. I ended up using some web tools to create my own private network for free, which wasn’t easy. But I also learned that many casual users may not even need a VPN anymore.

Let Us Help You Protect Your Digital Life

- With Apple’s latest mobile software update, we can decide whether apps monitor and share our activities with others. Here’s what to know.
- A little maintenance on your devices and accounts can go a long way in maintaining your security against outside parties’ unwanted attempts to access your data. Here’s a guide to the few simple changes you can make to protect yourself and your information online.
- Ever considered a password manager? You should.
- There are also many ways to brush away the tracks you leave on the internet.

Here's what you need to know.

What Has Changed About VPNs

Not long ago, many websites lacked security mechanisms to prevent bad actors from eavesdropping on what people were doing when browsing their sites, which opened doors to their data being hijacked. This helped VPN services become a must-have security product. VPN providers offered to help cloak people's browsing information by creating an encrypted tunnel on their servers, through which all your web traffic passes.

But in the last five years, the internet has undergone immense change. Many privacy advocates and tech companies pushed for website creators to rewrite their sites to support HTTPS, a security protocol that encrypts traffic and solves most of the aforementioned problems.

You've probably noticed the padlock symbol on your web browser. A locked padlock indicates a site is using HTTPS; an unlocked one means it's not and is therefore more susceptible to attack. These days, it's rare to stumble upon a site with an unlocked padlock — 95 percent of the top 1,000 websites are now encrypted with HTTPS, according to W3Techs, a site that compiles data on web technologies.

This means that VPNs are no longer an essential tool when most people browse the web on a public Wi-Fi network, said Dan Guido, the chief executive of Trail of Bits, a cybersecurity firm.

"It's very difficult to find cases where people were harmed by signing on to the airport, coffee shop or hotel Wi-Fi," he said. These days, he added, the people who benefit from a VPN are those working in high-risk fields and who might be targets, like journalists who correspond with sensitive sources and business executives carrying trade secrets while traveling abroad.

Simple Alternatives

So what to do? Fortunately, most of us can secure ourselves online with basic protections that, unlike VPN services, are free, Mr. Guido said.

Importantly, people should keep the software on their devices and web browsers up to date because new software updates include security protections against the latest vulnerabilities, he said.

Another crucial step is setting up online accounts with two-step verification, which requires two forms of verification of your identity before letting you log in. That safeguard can help prevent attackers from gaining access to your data if they obtain your passwords.

For those who would still prefer not to browse the web on a public Wi-Fi network, there's an easy solution included on most smartphones. The personal hot spot, a feature for wirelessly sharing a smartphone's cellular data connection with other devices, like your computer, can be activated in the phone's settings. Many phone plans don't charge extra to use this feature, though hotspotting does count against the monthly data allotment in your cellular plan.

How to Create Your Own VPN

Some people (including myself) still benefit from using a VPN, and not all providers are bad.

Wirecutter, a New York Times publication that tests products, recommends a few that are still trustworthy. But if your next VPN gets bought by a larger company, you may have to vet its trustworthiness all over again. I'm tired of the whiplash, so I created my own private network service.

I turned to Algo VPN, a free tool developed by Mr. Guido that automatically builds a VPN service in the cloud, which shields my browsing activity by allowing me to create a virtual tunnel on an outside server for my internet traffic to pass through.

Following the instructions listed on the Algo VPN project website, I set up a cloud service where my VPN service would be located on Amazon's web services, a reputable and widely trusted cloud provider. The rest of the steps involved installing some scripts on my computer and typing in commands to generate my VPN.

After about an hour, I set up a VPN that worked flawlessly. The best part? Not only is it free to use, but I no longer have to worry about trust, because the operator of the technology is me.

Brian X. Chen is the lead consumer technology writer. He reviews products and writes Tech Fix, a column about solving tech-related problems. Before joining The Times in 2011, he reported on Apple and the wireless industry for Wired. @bxchen

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: Once Sound Data Security, VPNs Develop Trust Issues