Best free VPNs: 5 reasons why they don't exist

You need to take your privacy and security seriously enough to avoid the malware, ad tracking and slow connections that free VPNs involve.

When it comes to free VPNs, there's always a price to pay.
Getty

Think of a good virtual private network like a bodyguard for your bank account. When you go for a stroll through the bustling lanes of public Wi-Fi, your VPN shields you from password pickpockets and keeps you out of unsafe areas. You trust your VPN -- a set of technologies that link computers together, then encrypt your data as you browse online -- with your most precious information. Maybe even your family's too. So when a

VPN provider offers to guard your digital life for free, the first question you should ask yourself is: What's in it for them?

With password-stealing malware on the rise, it's no surprise that the VPN market is booming, as consumers seek to protect their online information. The Global Web Index reports that 25% of internet users accessed a VPN within the past month, while VPN apps account for hundreds of millions of installs across mobile operating systems. Meanwhile, the VPN global market value's growth is projected to hit $35 billion in revenues by 2022.

Read: Best mobile VPNs: Android and iPhone VPNs compared

Finding a VPN you can trust isn't easy in this market. But there are some VPNs you should never, ever choose: The free ones. Here's why.

1. Free VPNs simply aren't as safe

As our sister site Download.com previously reported, free VPNs can be very dangerous. Why? Because to maintain the hardware and expertise needed for large networks and secure users, VPN services have expensive bills to pay. As a VPN customer, you either pay for a premium service with your dollars or you pay for free services with your data. If you aren't ordering at the table, you're on the menu.

Some 86% of free VPN apps on both Android and iOS -- accounting for millions of installs -- have unacceptable privacy policies, ranging from a simple lack of transparency to explicitly sharing user data with Chinese authorities, according to two independent 2018 investigations into free VPN apps from Top10VPN. Another 64% of the apps had no web presence outside of their app store pages, and only 17% responded to customer support emails.

As of June 2019, Apple reportedly brought down the hammer on apps that share user data with third parties. But 80% of the top 20 free VPN apps in Apple's App Store appear to be breaking those rules, according to a July 2019 update on the Top10VPN investigation.

As of August 2019, 77% of apps are flagged as potentially unsafe in the Top10VPN VPN Ownership Investigation -- and 90% of those flagged as potentially unsafe in the Free VPN Risk Index -- still pose a risk.

"Google Play downloads of apps we flagged as potentially unsafe have soared to 214 million in total, rocketing by 85% in six months," the report reads. "Monthly installs from the App Store held steady at around 3.8 million, which represents a relative increase as this total was generated by 20% fewer apps than at the start of the year as a number of apps are no longer available."

On Android, 214 million downloads represent a lot of user login data, culled from unwitting volunteers. And what's one of the most profitable things one can do with large swaths of user login data?

Read more: All the VPN terms you need to know

2. You can catch malware

Let's get this out of the way right now: 38% of free Android VPNs contain malware, a CSIRO study found. And yes, many of those free VPNs were highly-rated apps with millions of downloads. Your odds of catching a nasty bug are greater than one-in-three.

So ask yourself which costs less: A quality VPN service for about a hundred bucks a year, or hiring an identity theft recovery firm after some chump steals your bank account login and social security number?

But it couldn't happen to you, right? Wrong. Mobile ransomware attacks are skyrocketing. Symantec detected more than 18 million mobile malware instances in 2018 alone, constituting a 54% year-over-year increase in variants. And last year, Kaspersky noted a 60% spike in password-stealing trojans.

But malware isn't the only way to make money if you're running a free VPN service. There's an even easier way.

Read more: Red flags to watch out for when choosing a VPN

3. The ad-valanche

Aggressive advertising practices from free VPNs can go beyond getting hit with a few annoying pop-ups and quickly veer into dangerous territory. Some VPNs sneak ad-serving trackers through the loopholes in your browser's media-reading features, which

then stay on your digital trail like a prison warden in a B-grade remake of Escape from Alcatraz.

HotSpot Shield VPN earned some painful notoriety for such allegations in 2017, when it was hit with an FTC complaint for over-the-top privacy violations in serving ads. Carnegie Mellon University researchers found the company not only had a baked-in backdoor used to secretly sell data to third-party advertising networks, but it also employed five different tracking libraries and actually redirected user traffic to secret servers.

When the story broke, HotSpot parent company AnchorFree denied the researchers' findings in an email to Ars Technica: "We never redirect our users' traffic to any third-party resources instead of the websites they intended to visit. The free version of our Hotspot Shield solution openly and clearly states that it is funded by ads, however, we intercept no traffic with neither the free nor the premium version of our solutions."

AnchorFree has since offered annual transparency reports, although their value is still up to the reader.

Even if possible credit card fraud isn't a concern, you don't need pop-ups and ad-lag weighing you down when you've already got to deal with another major problem with free VPNs.

Read more: How to identify a good VPN: 3 features to look out for

4. Buffering... buffering... buffering

One of the top reasons people get a VPN is to access their favorite subscription services -- Hulu, HBO, Netflix -- when they travel to countries where those companies block access based on your location. But what's the point in accessing the geo-blocked

video content you've paid for if the free VPN service you're using is so slow you can't watch it?

Some free VPNs have been known to sell your bandwidth, potentially putting you on the legal hook for whatever they do with it. The most famous case of this was Hola, which was caught in 2015 quietly stealing their users' bandwidth and selling it, mercenary-style, to whatever group wanted to deploy their userbase as a botnet.

Back then, Hola CEO Ofer Vilenski admitted they'd been had by a "spammer," but contended in a lengthy defense that this harvesting of bandwidth was typical for this type of technology.

"We assumed that by stating that Hola is a [peer-to-peer] network, it was clear that people were sharing their bandwidth with the community network in return for their free service," he wrote.

If being pressed into service as part of a botnet isn't enough to slow you down, free VPN services also usually pay for fewer servers. That means your traffic is generally bouncing around longer between distant, over-crowded servers, or even waiting behind the traffic of paid users.

To top it off, subscription streaming sites are savvy to those who try to sneak into their video services for free. These services routinely block large numbers of IP addresses which they've identified as belonging to turnstile-jumping freeloaders. Free VPNs can't afford to invest in a long list of fresh IP addresses for their users the way a paid VPN service can.

That means you may not even be able to log into a subscription media service you've paid for if your free VPN is using a stale batch of IPs. Good luck getting HBO to load over that connection.

Read more: Avoid these 7 Android VPN apps because of their privacy sins

5. Paid options get better all the time

The good news is that there are a lot of solid VPNs on the market that offer a range of features, depending on your needs and budget. You can browse our ratings and reviews to find the right VPN service for you. If you're looking for something mobile-specific, we've rounded up our favorites for 2020.

If you'd like a primer before deciding which service to drop the cash on, we have a VPN buyer's guide to help you get a handle on the basics of VPNs and what to look for when choosing a VPN service.

Read more: The best VPN services for 2020