Can free VPNs be trusted?

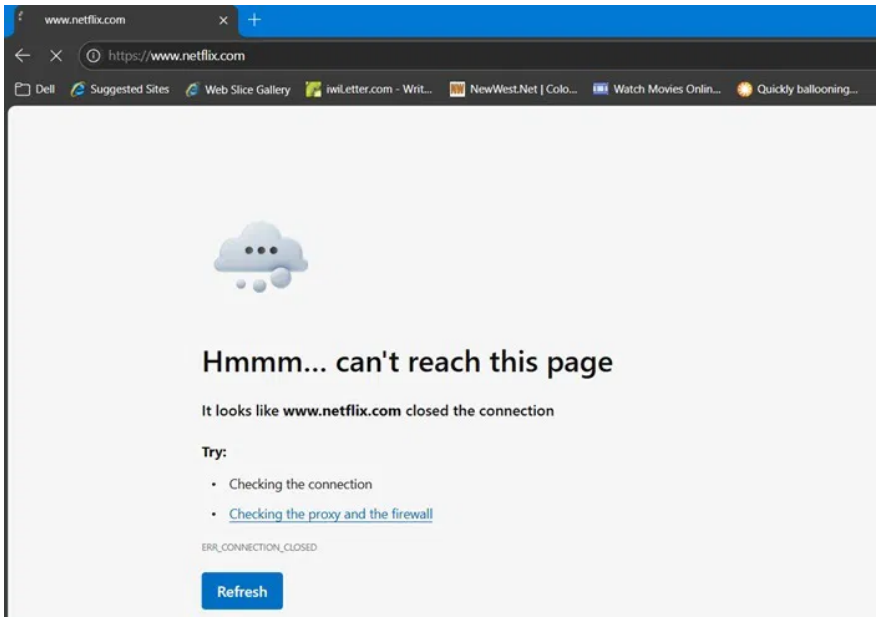
With so many free VPNs available, why would you consider paying for one? The simple answer is that free VPNs are pretty ineffective at unblocking the websites you need.

With so many free VPNs available, why would you consider paying for one? The simple answer is that free VPNs are pretty ineffective at unblocking the websites you need. Plus, they can leak data or steal user information, posing a significant privacy and security risk. Let's explore all the key reasons why you can't trust a free VPN!

1. They can't unblock important websites

With free VPNs, you may enjoy good performance at first, but eventually you will notice that they cannot unblock websites. This can become increasingly frustrating over time, leading you to give up altogether.

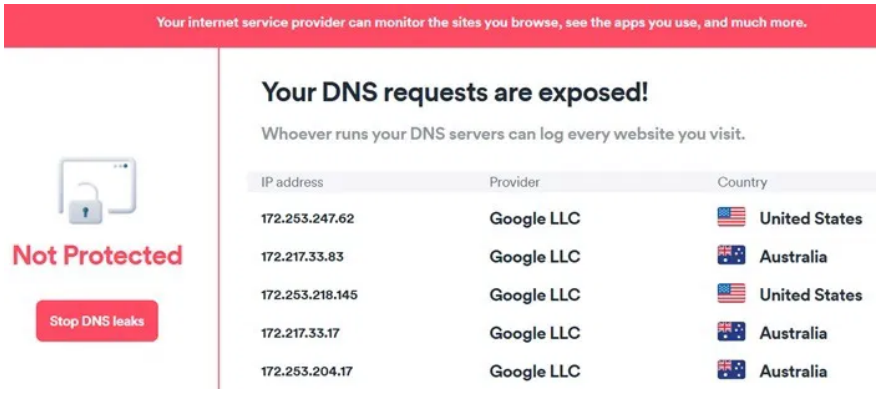
Streaming sites like Netflix have their own methods of detecting VPN usage, often causing websites to crash.



The streaming site issue also shows up on gaming platforms, Zoom calls, and some social media sites. Most modern websites are easy to spot if a free VPN provider is involved. But that's not the case with top-rated VPNs like ExpressVPN, Surfshark, or NordVPN.

2. They reveal your real DNS and IP address

Every time you visit a website, your device sends a DNS request through your ISP or router to resolve the domain name into an IP address. In return, the website receives your real IP address. Websites can use cookies and referrers to access your browsing history and online activity.

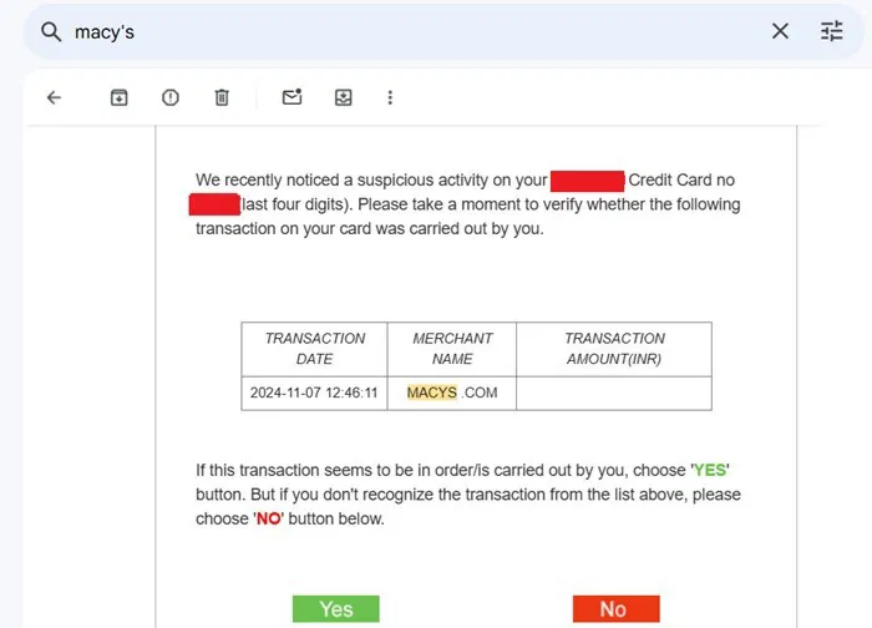


The main purpose of using a virtual private network (VPN) is to prevent your IP address from being exposed. However, if your DNS information keeps leaking to random websites, you can't trust your free VPN. It's only a matter of time before your real IP address is exposed.

3. Free VPNs are a gold mine for data collectors

The adage 'if you don't pay, you become the product' couldn't be more true when it comes to free VPNs and proxies. While you can access region-restricted videos through a free VPN, data collectors benefit even more. They gain extensive insights into your interests and browsing habits.

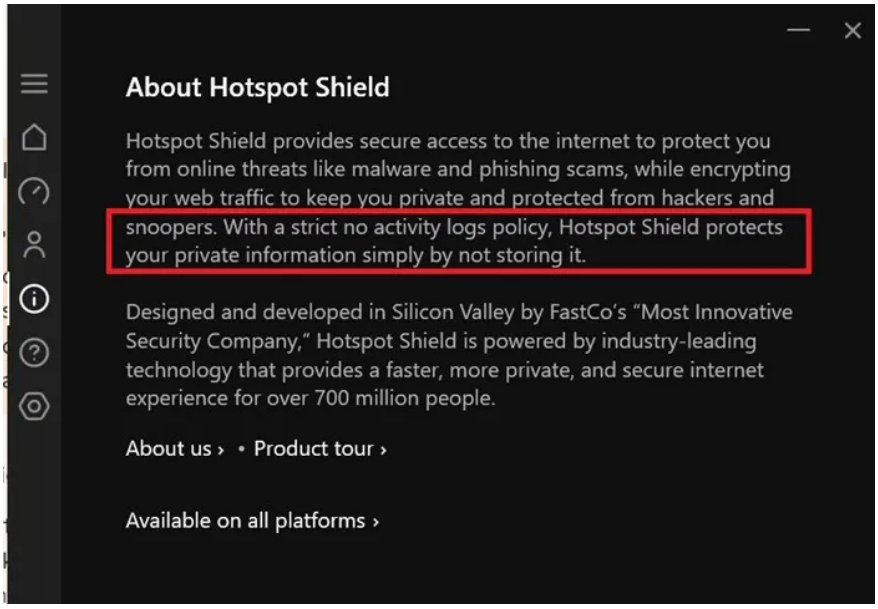
Since free VPNs need to be funded, they often sell user data to third parties. While these brokers are just selling you targeted ads, the biggest threat comes from cybercriminals on the dark web.



4. Lack of no-logs policy

The main difference between reputable commercial VPN providers and regular free VPNs is their adherence to a no-logs policy. It's worth noting that there have been significant advances in this area in recent years. For example, both ExpressVPN and NordVPN have switched to RAM-only servers, ensuring that all user data is wiped clean after every reboot.

Since these VPN providers are based in the British Virgin Islands and Panama, which are outside the jurisdiction of the Fourteen Eyes, users can rest assured. Even if a VPN provider is based in the United States, such as Hotspot Shield, they still have a clear no-logs policy in place.



5. They can track you

Even if you're indifferent about your data being sold to third parties, you can't ignore the issue of cyber surveillance. You may not think you're important enough to be a target for spying, but many ISPs monitor your online activities. Government agencies, not necessarily from your country, can monitor your internet traffic to gather intelligence, even if you're not a high-profile individual.

6. Slow Speeds – Stolen Bandwidth

Everyone loves free stuff. And when everyone is connected to the same free VPN service, it's inevitable that speeds will suffer. Most free VPN services don't have a lot of resources allocated to them, and when there are too many users, you'll start to experience throttling or even disconnections.

Since free VPNs need to get their money from somewhere, it's not uncommon for them to sell your bandwidth to third parties. There's no way to know if the person using your bandwidth knows they're using stolen bandwidth. Plus, if the person using it does something illegal (since it's your bandwidth), you'll be the one in trouble with the authorities.