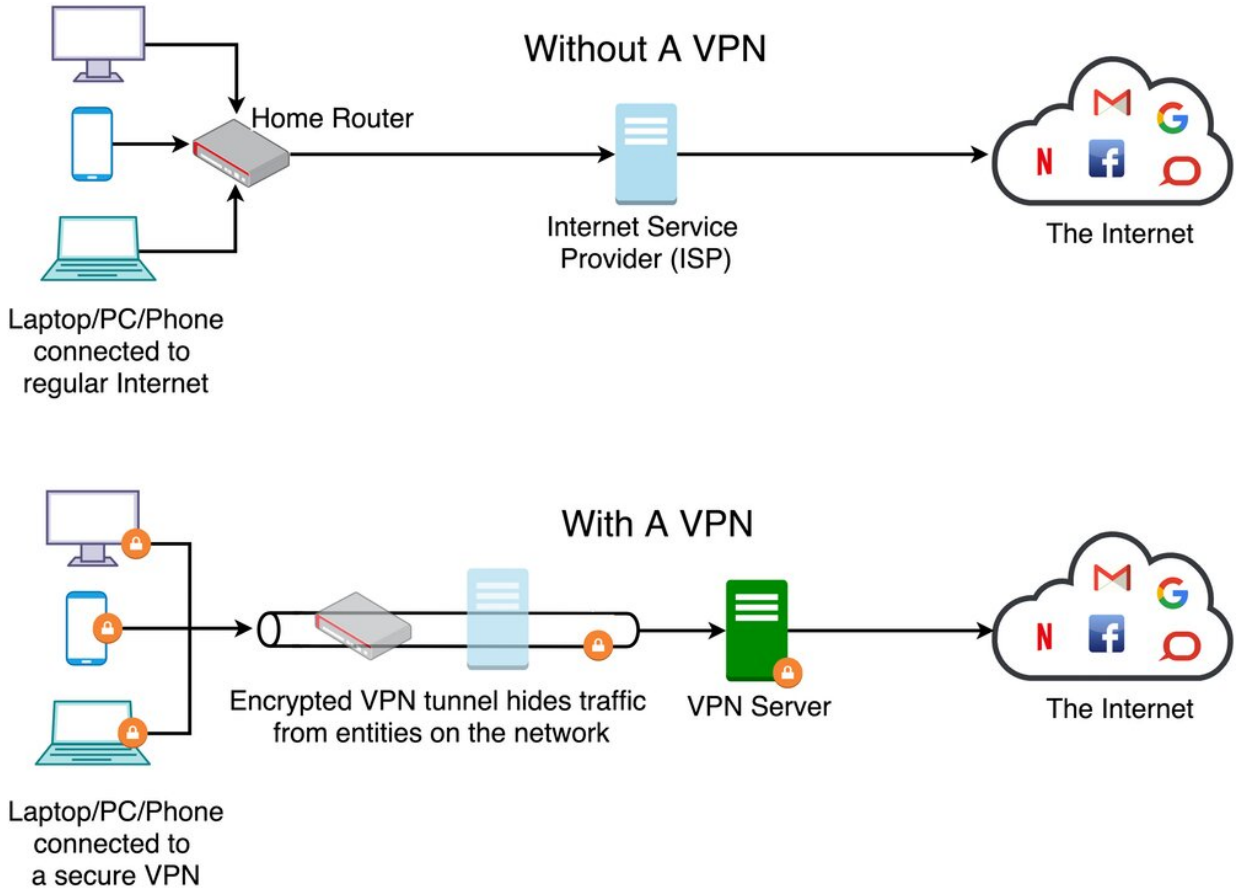
Is your VPN secure?

February 4 2019, by Mohammad Taha Khan And Narseo Vallina-Rodriguez



How a VPN secures internet activity. Credit: Mohammad Taha Khan, CC BY-ND

About a quarter of internet users use a virtual private network, a software setup that creates a secure, encrypted data connection between

their own computer and another one elsewhere on the internet. Many people use them to protect their privacy when using Wi-Fi hotspots, or to connect securely to workplace networks while traveling. Other users are concerned about surveillance from governments and internet providers.

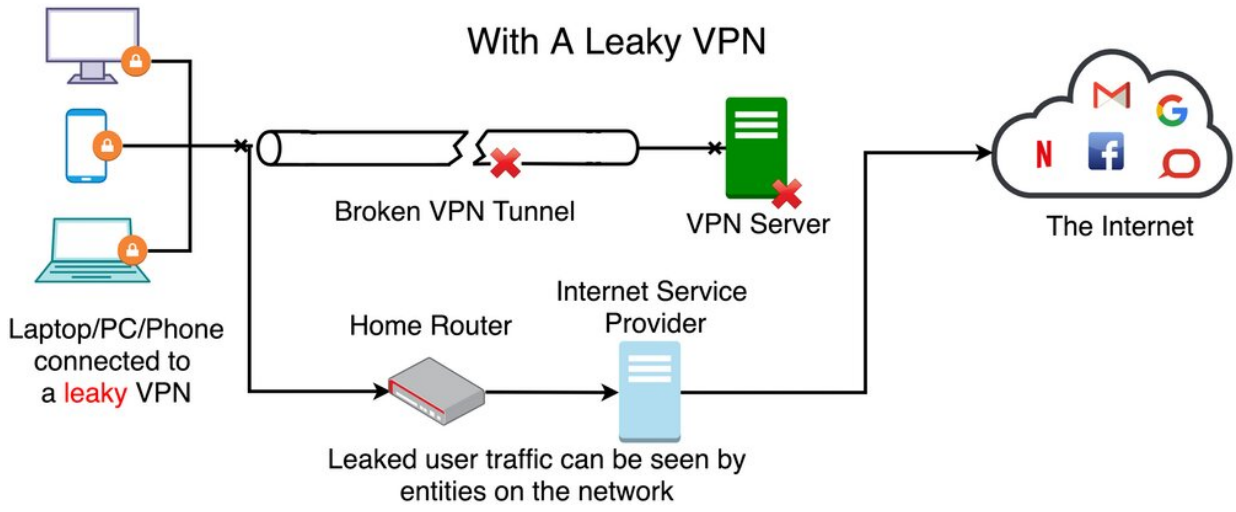
Many VPN companies promise to use strong encryption to secure data, and say they protect users' privacy by not storing records of where people access the service or what they do while connected. If everything worked the way it was supposed to, someone snooping on the person's computer would not see all their internet activity – just an unintelligible connection to that one computer. Any companies, governments or hackers spying on overall internet traffic could still spot a computer transmitting sensitive information or browsing Facebook at the office – but would think that activity was happening on a different computer than the one the person is really using.

However, most people – including VPN customers – don't have the skills to double-check that they're getting what they paid for. A group of researchers I was part of do have those skills, and our examination of the services provided by 200 VPN companies found that many of them mislead customers about key aspects of their user protections.

Consumers are in the dark

Our research found that it is very hard for VPN customers to get unbiased information. Many VPN providers pay third-party review sites and blogs to promote their services by writing positive reviews and ranking them highly in industry surveys. These amount to advertisements to people considering purchasing VPN services, rather than independent and unbiased reviews. We studied 26 review websites; 24 of them were getting some form of kickback payment for positive reviews.

A typical example was a site listing hundreds of VPN companies that rated more than 90 percent of them as 4 out of 5 or higher. This is not illegal, but it skews evaluations that could be independent. It also makes competition much more difficult for newer and smaller VPN providers that may have better service but lower budgets to pay for good publicity.



When VPNs don’t work right, users’ data leaks out. Credit: Mohammad Taha Khan, CC BY-ND

Vague on data privacy

We also learned that VPN companies don't always do much to protect users' data, despite advertising that they do. Of the 200 companies we looked at, 50 had no privacy policy posted online at all – despite laws requiring them to do so.

The companies that did post privacy policies varied widely in their descriptions of how they handle users' data. Some policies were as short

as 75 words, a far cry from the multi-page legal documents standard on banking and social media sites. Others did not formally confirm what their advertisements suggested, leaving room to spy on users even after promising not to.

Leaking or monitoring traffic

Much of the security of a VPN depends on ensuring that all the user's internet traffic goes through an encrypted connection between the user's computer and the VPN server. But the software is written by humans, and humans make mistakes. When we tested 61 VPN systems, we found programming and configuration errors in 13 of them that allowed internet traffic to travel outside the encrypted connection – defeating the purpose of using a VPN and leaving the user's online activity exposed to outside spies and observers.

Also, because VPN companies can, if they choose, monitor all online activity their users engage in, we checked to see if any were doing that. We found six of the 200 VPN services we studied actually did monitor users' traffic themselves. This is different from accidental leaking, because it involves actively looking at users' activity – and possibly retaining data about what users are doing.

Encouraged by ads that focus on privacy, users trust these companies not to do this, and not to share what they find with data brokers, advertising companies and police or other government agencies. Yet these six VPN companies don't legally commit to protecting users, regardless of their promises.

Credit: AI-generated image (disclaimer)

Lying about locations

A huge selling point for many VPNs is that they claim to allow customers to connect to the internet as if they were in countries other than where they really are. Some users do this to avoid copyright restrictions, either illegally or quasi-legally, like watching U.S. Netflix shows while on vacation in Europe. Others do this to avoid censorship or other national rules governing internet activities.

We found, though, that those claims of international presence aren't always true. Our suspicions were first raised when we saw VPNs claiming to let people use the internet as if they were in Iran, North Korea and smaller island territories like Barbados, Bermuda and Cape Verde – places where it's very difficult to get internet access, if not

impossible for foreign companies.

When we investigated, we found some VPNs that claim to have large numbers of diverse internet connections really only have a few servers clustered in a couple of countries. Our study found they manipulate internet routing records so they appear to provide service in other locations. We found at least six VPN services that claim to route their traffic through one country but really convey it through another. Depending on the user's activity and the country's laws, this could be illegal or even life-threatening – but at the very least it's misleading.

Guidelines for VPN users

Technically minded customers who are still interested in VPNs might consider setting up their own servers, either using cloud computing services or their home internet connection. People with a bit less technical comfort might consider using the Tor browser, a network of internet-connected computers that help guard its users' privacy.

Those methods are difficult and may be slow. When selecting a commercial VPN service, our best advice, informed by our research, is to read the site's privacy policy carefully, and buy short subscriptions, perhaps month-by-month, rather than longer ones, so it's easier to switch if you find something better.

Provided by The Conversation