Do VPN providers keep track of your browsing data?

We use VPNs to protect our privacy in the internet world, avoiding the eyes of hackers, network service providers and data thieves. However, have you ever wondered if it is the companies that provide VPNs that collect your browsing data?

We often put a lot of faith in the VPN provider we use. But be careful!

VPN providers can follow you completely

With that said, the main purpose that makes us use a VPN Virtual Private Network is to protect our privacy. A VPN helps prevent malicious attacks from hackers, blocks your internet service provider (ISP) from accessing traffic, and also conceals your private information from malicious websites. micro collection of personal data. Overall, these 'claims' aren't false, but there's one big issue that you should still be cautious of: the companies that provide VPN services themselves.

Before we dive into how VPN providers can track your browsing data, it's important to have a grasp of how a VPN works. Basically, a VPN is responsible for routing the internet connection, which is provided by your ISP, through an encrypted, more secure network provided by a third party. This will change the IP address that websites can see, while also eliminating your ISP's ability to access your traffic. These encrypted networks can simulate many different IP addresses and locations. This is essentially the same way you can fool a streaming service like Netflix into thinking you're in another country.

During this process, your traffic goes to a third party, and is managed by the server of the VPN provider you are using. This VPN company can theoretically record all the traffic going through their system, thereby getting a full picture of a particular user's online browsing behavior and habits. While most reputable VPN providers claim not to track users and have no incentive to do so, this risk is in fact quite possible and well documented. In reality.

VPN spy issues

The most famous issue about a VPN provider compromising customer data came to light in 2018. It was accompanied by a huge controversy regarding the Onavo Protect platform owned by Facebook. Accordingly, Facebook has released a VPN with a claim to protect and encrypt users' traffic. However, in reality, it is this company that collects sensitive information from users, such as visited websites or applications that users have opened on their devices. Although Facebook has revealed that the application will forward information to Facebook servers, this is generally still something that makes many people difficult to accept.

The data is then used for a program called Facebook Research - which supports business development initiatives and sells ads on Facebook's social network. In addition, it will also give Facebook more insight into how users use rival platforms, such as Snapchat.

Besides the Facebook incident, there are dozens of other free VPN providers that have been accused of spying on users. A report from Buzzfeed News shows that Sensor Analytics, an analytics platform used by many investors and developers, owns many free VPN apps that collect user information without their knowledge. These apps have millions of downloads and it's unclear who they belong to. The company will then migrate the collected user data onto its own analytics platform.

Overall, you should be especially wary of free VPNs, and there doesn't seem to be a paid version or a clear business model. It's very likely that these apps are making a profit by collecting user data and selling them to third parties.

Should I continue to use a VPN?

Given the above problem, the question arises should we also continue to use VPN? The answer is yes, but in a more conservative and selective way.

The best way to avoid problems like this is to look for VPNs with a zero logging policy. This is what ensures that these companies will not log user traffic. Many of the top paid VPNs, such as NordVPN, ExpressVPN, and Mozilla VPN, have a no-logging policy clearly outlined on the website and within the app. This also means that they will be held responsible if they violate the policies that they have put in place.

Before signing up for a VPN, make sure you do a thorough test of its website and go through reliable reviews first. Here are some questions you should get answers to before signing up for the free VPN trial: