The worst privacy protection VPNs users should avoid

The growing popularity of VPN technology has led to a series of scams in a variety of ways, different ways and levels of daring.

The growing popularity of VPN technology has led to a series of scams in a variety of ways, different ways and levels of daring.

Experienced VPN users and those who value privacy should know a little about how to choose a reputable VPN provider. However, if you're just starting your search, prepare yourself for basic understanding. The VPN market is a mess of dangerous things of fake reviews, tricking into strange links, circumventing law and illegal surveillance. At the same time, virtual private network - VPN - is a mandatory tool for online privacy and security protection.

Of the hundreds of VPNs, how do you choose the best one? Reading reviews is essential, but still need to check some selected VPNs to make sure at least one of them meets your requirements. And even if the specification looks good and the performance is good, VPN can still leak IP addresses, record logs of all online activities or infect malware to your device. users, sell user data to advertising companies, NSA or some malicious entities on black websites.

Stay away from bad VPNs to protect privacy?

1. What makes a bad VPN?
    1. A bad VPN will keep a log of the user's online activities
    2. Bad VPN reveals user data
    3. Bad VPN infects malware to users' devices
    4. VPN does not work well
    5. A bad VPN does not respect the refund policy
2. The bad VPN users should avoid
    1. 1. ExpatSurfer
    2. 2. Earth VPN
    3. 3. Betternet VPN
    4. 4. Onavo Protect
    5. 5. Cryptostorm VPN
    6. 6. Faceless.me
    7. 7. Liberty VPN
    8. Some other VPNs are blacklisted

What makes a bad VPN?

The biggest strength of VPNs is the ability to protect privacy, security, online streaming services are not blocked and the ability to 'bypass' the firewall.

But up to 99.9% of VPNs are now committed to these features. To choose reliable suppliers from scammers, find out carefully before signing up. Here are some signs to help users identify a bad VPN provider.

A bad VPN will keep a log of the user's online activities

While a thorough examination of a Netflix VPN can be quite simple, vendors' privacy and security commitments are difficult to verify. Users need to carefully review the service provision and security policy of the provider, paying special attention to policies that record user activity logs.

This does not mean that only bad guys need a logbook provider. Keep in mind the rule of thumb: Choose a provider that does not keep user activity logs. If a VPN company promises to protect privacy and security, but still violates its commitment and logs connection data and works or filters user content, appeal them to agencies. competent authority.

Bad VPN reveals user data

This comes directly from the VPN logging policies. Vendors record user activities very likely to cooperate with bad organizations. If the VPN service provider is based in countries within the Five Eyes or Fourteen Eyes group, the company must comply with data storage laws. That's why VPNs located in the United States and the United Kingdom are often not recommended by privacy organizations and security experts.

Reliable VPNs follow the direction of transparent information and do not record any data that can identify your customers. Reliable VPNs delete connection logs every few hours or just log details that are not personally identifiable (ie, cannot rely on this information to retrieve a specific user).

Similarly, to protect users' personally identifiable information, trusted VPNs accept many anonymous or semi-anonymous payment options, including cash, gift cards and Bitcoin.

Bad VPN infects malware to users' devices

Some providers offer free VPN services to benefit from displaying ads. The benefits for these vendors come from the applications and ads they display, with a full range of tracking capabilities that allow logging of user browsing activity logs.

Some providers even take a step further to infect malware, sending important information about users' devices, identities and web usage habits to their servers. .

Most free VPNs are thriving by selling user data to data brokers, advertising agencies, NSA, etc. If using VPN infected with malware, traffic will be recorded, filtered, censored and reported. The content of the link is displayed instead of the content that the user really needs. Finally, the devices will be more easily targeted and hacked by hackers.

VPN does not work well

The scam from VPN is very diverse. Occupying a website of a service that is no longer provided and collecting registration information from new users, then ignoring the refund request is one of them.

To avoid this type of phishing VPN, you need to research your provider's social network account and contact customer service before making a payment.

A bad VPN does not respect the refund policy

Some vendors impersonate registration layers to create short-term packages at high prices, making long-term packages look like a bargain. They guarantee a refund, but when a refund request is made, they will constantly make requests with stupid questions and eventually declare the refund period has ended.

The bad VPN users should avoid

The authors on BestVPN tested countless VPNs and compiled a list of VPN service providers that users should avoid.

1. ExpatSurfer

ExpatSurfer.co.uk is a good example of a phishing VPN. ExpatSurfer takes users' money and then forgets all about them. It does not provide the server address that users need to set up PPTP connections and of course, does not bother answering customer emails.

With a price of $ 10.26 / month (238,000 VND) for a single PPTP connection that doesn't work, this VPN deserves to be blacklisted.

2. Earth VPN

EarthVPN.com is a supplier based in Cyprus and used to be very popular. Earth VPN advertises all the things users need when using VPN - OpenVPN, P2P, unlimited data, affordable packages but in fact it doesn't work.

This service has been canceled, but strangely, users can still register. Although when I tested, the author did not continue to pay, but six months later still received notice of Earth VPN's unpaid bills. But email questions about this issue are not responded by Earth VPN.

If you don't want to keep receiving spam for months from EarthVPN's automated system, stay away from this ghost company and let it sink into oblivion.

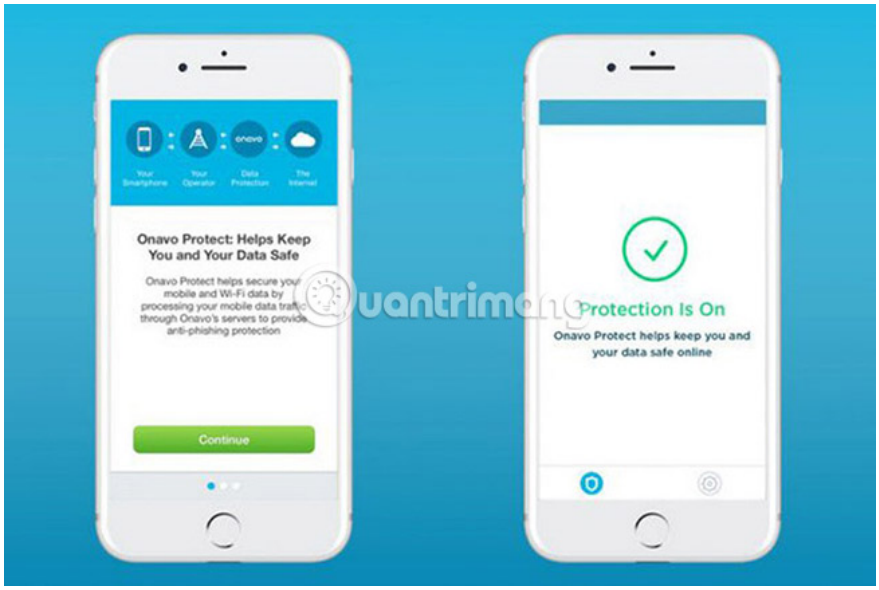
3. Betternet VPN

Betternet VPN is a classic VPN scam. It spreads malware under the guise of providing free VPN services. With millions of downloads, it means that a lot of people provide their browsing activities to shady data brokers.

RevoUninstaller found a large number of files left behind by Betternet's Windows application, while Total AV Virus ranked Betternet VPN in the 13th position (1st place is completely virus-free). The specifications of this VPN are extremely shady. Although the statement does not keep the logs active, in fact, this VPN still stores user connection logs.

Many third parties have access to user data and Betternet will not protect its customers if law enforcement agencies 'visit'.

4. Onavo Protect



Onavo Protect (onavo.com), also known as Protect Free VPN + Data Manager, is a free Facebook VPN itself. It is a mobile application available for iOS and Android, requires a lot of permissions to run. Instead of acting as a regular VPN, Onavo Protect accesses and logs the user's application activity. This is absolutely true. Facebook wants to know which applications you use, with how often, then route them across UK servers.

It runs in the background, screening all user traffic. If you're using Facebook's VPN, it's a shame to say that your privacy has been seriously compromised.

5. Cryptostorm VPN

Cryptostorm.is actually has some pretty powerful features, such as anonymizing the purchase process with a token, the user does not need email or a username to access its VPN. It has a good network, top security specifications, flexible pricing structure, good performance and usability.

But Douglas Spink, owner of Cryptostorm, who was accused of smuggling cocaine worth $ 34 million, was released after three years of sentence (while the verdict was 17 years) that led the security community to believe he had Disclosure of user information from Cryptostorm VPN servers.

Meanwhile, Cryptostorm declined to comment on how the company complied with data storage regulations in Canada. Honestly, a decentralized company under the control of mysterious characters may not sound safe.

6. Faceless.me

Faceless.me has existed for more than 5 years, has a stable download on Google Play, making it look like it still works normally. In fact, Faceless.me is no longer active, without support. Social networking sites of this VPN have not been updated for many years.

For some reason, Google does not remove apps that have many poor reviews from the app store. Therefore, protect yourself by staying away from this VPN.

7. Liberty VPN

LibertyVPN.net can look pretty good thanks to its ability to unblock streaming services, but the shady source and ridiculous service terms make many people wonder how long this VPN can last so long. . The return policy is very unreasonable because users cannot use more than 50MB while the VPN packages are at an average of $ 15 (348,000VND / month) or $ 108 (2,500,000VND) / year.

This VPN is very complicated and difficult to use, the location of servers is also very limited. No P2P, do not bypass firewalls, do not use Skype from Cuba, do not connect simultaneously, not Bitcoin. Moreover, if violating ToS (terms of service), the company will charge a fee of $ 250 / hour (VND 5,800,000) to delete the account.

Some other VPNs are blacklisted

Unfortunately, the list of bad VPNs is still very long:

1. **VPNReactor.com** is an established US provider, recording user online activities and the usage fee is $ 77.88 / year (VND 1,800,000).
2. **ZPN.im** is still another VPN on the mobile platform, claiming to be the best free VPN, but in fact, its functions are disruptive, seem to be shady and even inactive. It is unclear who or the organization is behind and its ToS indicates that they can activate activity monitoring if forced. Do not choose this VPN, even if it allows you to register for a free, best account.
3. **Hotspot Shield** is another VPN that makes money thanks to customer data. It logs user activities, tracks the device library and adds JavaScript ads to web pages. It shares user data with third parties, sells it to data brokers and complies with US data storage laws.
4. **Rocket VPN** is a free VPN on mobile platform provided by HotSpot Shield above. It's no wonder that Rocket VPN comes with shady logging, adware and ToS policies.
5. **UnoTelly** is Canada's ridiculous expensive DNS and VPN service with poor performance, only 5 VPN server locations, no P2P and weak encryption. It logs connection logs and user usage data. As a supplier in Canada, it complies with the laws of every country where the server is located. Even if it is not deceptive, it is very bad for the role of a VPN.
6. **DefenseVPN.com** is a new provider in Canada. The name subsided in 2017 and by 2018, it reappeared for a short time, claiming that everything was back to normal. Many people wonder what is 'normal' in terms, when users pay for a package and do not receive login information. Support has refunded instead of providing login details to customers. That's weird!
7. **Dot VPN** is based in Hong Kong and provides 4096-bit encryption, but poor performance, originating in Germany, watchdog Five Eyes, records user log and user logs. The fact that the company keeps those logs

for two years makes it possible for users to believe that it is better to ignore it.

8. **HideMyAss** from AVG is a UK-based provider, logging user connection metadata and giving it to Scotland Yard immediately.
9. **SuperVPN** for iOS and Android is a free mobile VPN and has quite a lot of functions, except it has all the signs of an MI5 honeypot. In addition to having deep access to users' sensitive information, it stores browsing sessions in the UK and the United States, and will disclose them to law enforcement agencies if required.
10. **Proxy Server Pro** has all honeypot signs. Located in the US, it logs user data, user names and addresses and shares it with third parties.
11. **BTGuard.com** logs personal information and connected metadata, has vague security policies and primarily serves torrents.
12. **OneVPN.com** does not respect the commitment to guarantee refunds but ignores this request from users. In the meantime, it makes a bold statement that is the fastest VPN, not the best logbook and privacy protection. In fact, they keep users' connection logs but hide this information.
13. Cargo VPN is a 'conceited' VPN, giving many false statements. The free trial is not available while support is as bad as KeepSolid, another VPN provider. It also has Mac and iOS exclusive, too expensive and ineffective.

This list is still incomplete. New VPNs appear almost every day, while older VPNs have been removed or stopped, and scammers take advantage of the opportunity to hijack the site. Some popular VPNs have a fairly high ranking, whether giving out incorrect features or not appreciating their customers.

You can rest assured if your VPN is not found in this list. But also not subjective. Study it thoroughly. Contact supplier support, consult with technology communities or leave a comment in the comment section below if you suspect you may be a victim of a phishing VPN. Finally, remember not to rely too much on VPN.

Take the time to find a reliable supplier. Suppliers like ProtonVPN, Mullvad or NordVPN accept Bitcoin and even pay cash, which means you can protect your identity when you register and these companies don't keep any logs. User's.

Stay away from shady companies and always check VPN services before registering anything for longer than a month.

Wish you find a suitable VPN provider!

See more:

1. Why should I stop using VPN for free immediately?
2. 5 Security application you should consider removing and replacing
3. How to use VPN Gate fake IP to stabilize the Internet

You finished reading the article "**The worst privacy protection VPNs users should avoid**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
