How to recognize a bad VPN

To really understand if VPN is right for you, there is no other way than to try it. Install some clients, connect to the best servers, check your favorite websites and see how they work.

To really understand if VPN is right for you, there is no other way than to try it. Install some clients, connect to the best servers, check your favorite websites and see how they work.

But that takes time, effort and money. Or, at the very least, users should expect that a refund guarantee like the VPN provider has declared will be unconditional.

But there is a simpler way. Empirically, users can identify part of the VPN quality by simply visiting the website and reviewing in detail how the unit provides presentations about themselves and their products.

This approach cannot tell users whether VPNs are good, whether clients are easy to use, whether the server is fast or if the provider has blocked the sites and services you need.

But what it does is help users determine if it's a bad VPN before wasting time and money to use. That's a great starting point, isn't it? The following are signs to identify a bad VPN.

How to distinguish a VPN is good or bad?

1. 1. Ambiguous feature details
2. 2. Unrealistic requirements
3. 3. Dead website
4. 4. Difficult to identify
5. 5. Poor website support

1. Ambiguous feature details

Access to most VPN provider websites and major advantages will immediately hit you. Take the time to read each part and see all the details that the company provides to users.

A good provider understands the main details that users are looking for and makes them clear. Locations, supported platforms, technical features, prices and any refund commitments - all of these elements will be displayed on the front page or just a click away.

Bad vendors will focus almost entirely on the benefits of using VPN in general, such as encrypting connections or helping users access blocked websites. Important points like the number of countries included or the applications provided may not even be mentioned. Details of switch kills (the ability to cut off all network

connections when a VPN connection is dropped), supported protocols or anything related to the technology are very fuzzy.

The reason for this is very simple: That VPN provider has nothing to be proud of. Whatever the cause, it is a reason to be skeptical and you should switch to a service with a clearer feature list.

2. Unrealistic requirements

When browsing the VPN provider website, do not go through the requirements section. Take the time to read any description of the requirements, and think about how realistic they are.

A good VPN will provide users with more details about common service benefits and talk about special features. Sometimes, the provider may say a bit too much. For example, some VPNs advertise themselves as the fastest in the world. But statements like this can at least make sense. Perhaps they are really the fastest VPN in some areas.

A bad VPN often overstates everything to make them misleading. For example, make sure to unblock all websites in the world or use the Netflix logo to imply that the VPN provider will unblock the site but not actively say it.

Some other vendors have gone too far on security. A good VPN will indicate that it protects users on public WiFi networks and may include a feature to block malicious websites. A bad VPN will make it seem to provide complete protection against all types of malware, hacks and trackers. A VPN that the article previously reviewed claims that "detects and protects you from all forms of online threats."

Or a VPN that no longer exists claims that it will make the user's Internet connection 4 times faster.

There are a few situations in which VPN can improve speed, for example if traffic is being adjusted, but they are exceptions, not fixed rules. Most people will see reduced performance when using VPN and users should be wary of any provider saying the opposite, if not explain why.

3. Dead website

When browsing the website about a VPN provider, look for signs that this is an active company and always do something to improve the service.

A good VPN will not only have a news site, a blog and possibly social networking sites, but also regularly updates them with really interesting and worthwhile content.

A bad VPN will not care much about that. If there is a social network, users can see that it has not been updated for months or only automatically revolves old posts.

Please check the rest of the service too. Go to any of the frequently asked questions **(FAQs)** or support pages and find a date indicating when the document was created or updated. If the service has an iOS or Android client, visit their app store page and find the last release date.

This is just a general indicator and regular updates do not guarantee that it will be a good VPN. But an almost dead site is a strong sign that this may be a bad VPN and users should not waste their time or money there.

4. Difficult to identify

The VPN may be responsible for securing some very important and confidential information, so it is important for users to know if their provider is trusted. Start by trying to identify the company, find out who or what organization is behind the service and where the person or unit is located.

The best VPNs will have a general introduction **(About Us)** or similar page that can provide users with a company name, location, history, some general information about the service. Not just a generic line, like 'we are a group of security experts who together create the best VPN ever', which must be something with realistic details.

Other providers will at least let users know a bit about themselves. And they will provide users with an email address, live chat feature or some other system to ask questions.

A bad VPN will actively hide the basic details. The VPN application may not have a website, the company name does not exist anywhere else on the Internet and the general email address **'greatvpnsupport@gmail.com'** does not have a clear connection to the service.

If you just want to use that type of VPN to unblock YouTube, users may not be interested. But think carefully before trusting such a secret service.

5. Poor website support

All VPNs are problematic and sometimes even the most knowledgeable experts in the field need help. Taking the time to check out the vendor's support pages will help confirm that the company is aware of what they are doing and let users know how much time and effort they have spent helping customers. my goods.

ExpressVPN is a great example of a good support site. There are many detailed setup guidelines for many applications and on many different platforms, including 8 applications for Windows alone. Frequently asked questions about troubleshooting help users solve problems and feature live chat, as well as email addresses if need help from experts.

A bad VPN will look very different. If there is any web-based support, it will also include only a few questions. Most of those things will not relate to the information you really need (setting up, problem solving, major account issues). Themes seem incomplete or outdated, such as having a way to set up VPN on Windows 7, but there is no information about Windows 10 at all. And if browsing a few articles, users may find them short, poor quality and do not provide the necessary information.

In fact, an experienced VPN provider will be able to create a simple minimal support website within a week, so if a company has not completed that job in a year or more, that's a sign. The signal shows that something is wrong. Unless there are some other compelling reasons to believe, look for another provider.