



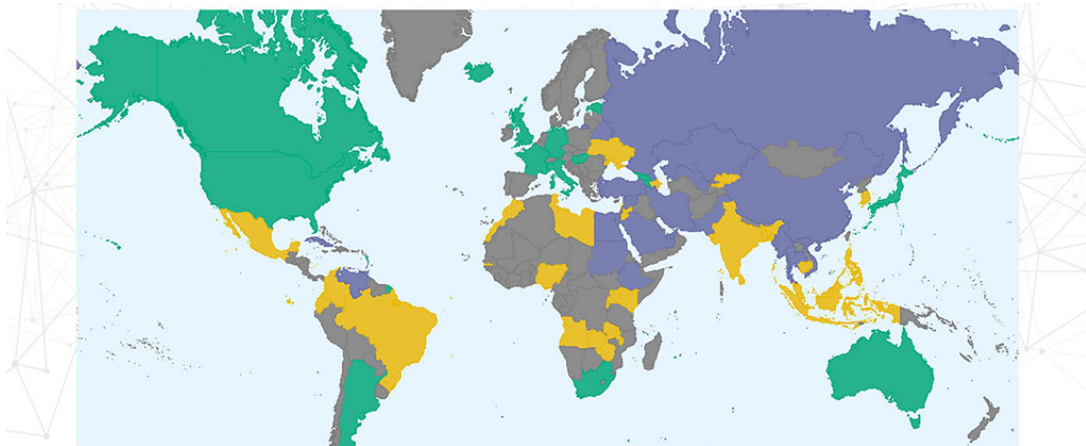
Why Do I Need A VPN?

- 2021-03-23 - Frequently Asked Questions

Although the answer to this question can be extremely complicated, the most notable reason someone would need a VPN is for security and privacy. Below we have put together some of the most common reasons why any person should be using a VPN:

1. You Want Extra Digital Security

From personal photos and social media to health Records or finances: most of our lives are online nowadays. Using a VPN provides extra encryption and security when you are transferring your data. It can also shield your browser activity from prying eyes on public WiFi to your ISP monitoring your home network and so much more.



Looking at the map above, you can see that various Governments around the world either censor the Internet or demonstrate intrusive surveillance. This map shows that out of 65 countries assessed by [Freedom House](#) that 26 countries are experiencing a deterioration in internet freedom. This is why using a VPN is one tool that will allow you more freedom that would allow you a feeling of security and privacy knowing that your Government cannot see what you are doing or where you are located.

For more information on Government censorship please review this article from [Who is Hosting This?](#) as they go in-depth about countries and their internet censorship today. Any country with an icon actively monitors its citizens and people visiting the country.

2. You Log Onto Public Wi-Fi

Public WiFi networks like those found at most cafes, airports, and popular public areas are notorious hangouts for hackers. That's because these hotspots are generally very weak with their security to the public and hackers can gain access to these hotspots with little to no

effort.



Using a VPN will add the security that you need to access these hotspots by encrypting your connection traffic, making it appear as you are coming from somewhere else helping to protect your physical safety just as much as your virtual safety.

3. You Use Online Cloud Storage

Online storage solutions like Dropbox, Box, and OneDrive do a decent amount of work securing your files on their servers. However, when the data is in transit, that's another issue altogether.

Using a VPN can add the extra encryption to your cloud storage uploads and downloads so that your data is protected while it is being transmitted to and from your Cloud storage.

4. Downloading Torrents

There are as many legitimate, legal reasons for downloading torrents as there are torrent users who download pirated movies. The problem is ISPs have a very hard time distinguishing between the two. That means they sometimes block or traffic shape users who are using torrents for legitimate reasons (for example game updates and Linux ISOs).

5. You Are A Researcher or Journalist

For many, most email service providers provide sufficient privacy when transmitting emails. But journalists and researchers send messages containing data that some people, more often than not, might want to try to intercept.



Using a VPN will provide that extra encryption for your messages and even make you look like you are sending or receiving them from a location you are not in; helping to protect your physical safety if you are researching or reporting on a story someone doesn't want to get out. Additionally, we recommend that researchers and journalists read our [Best Security Practices](#) guide for more tips and tricks on keeping their information and identities safe.

6. Communicating via VOIP services

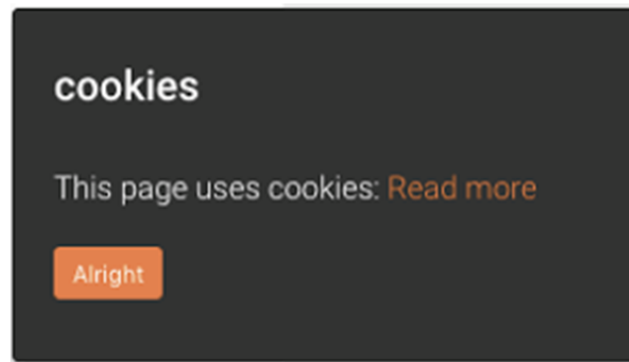
While companies have stepped up their game encrypting texts and emails, they still lag behind on VOIP security. That is calls and video chats made over Skype, FaceTime, and similar services.



Using a VPN can add extra security and encryption to your video chats, making them harder to be intercepted. However, we can not guarantee that the IP address that your VOIP systems are connecting over will be the one that was whitelisted on our network. Connecting with a VPN and your VOIP system can result in an unstable connection.

7. You Don't Like Companies Keeping Tabs On You

Most companies store cookies on your computer or they track your IP (or both) to see what you do online and what you click on. They then use this information to show you ads. Amazon is notorious for doing this.



You can stop Amazon, Google, and other similar sites from building up an anonymous database of your clicks by using a VPN each time you surf the web. It will then look like it's a different computer because your IP will change each time.

Tags
Need
VPN
Why