2/6/2020

Use Cases for a VPN

Bypass Geoblocking

Watch anything online, without being watched back!

With a VPN, you can access TV and movies, sports and news, gaming sites, shopping sites and messaging services no matter what country they're from and what restrictions they enforce.

Imagine a massive movie theater complex or shopping mall with sections run by different countries, where you have to show your passport before watching any movie or walking into any store. Now remember how some countries won't let any foreigners in.

This is called geo-blocking, and it's used by companies like Hulu, Crackle and even YouTube in order to prevent people in foreign countries from accessing their native content. Maybe it's to prevent people from engaging with local users, or maybe it's just a way to squeeze extra dollars out of you by forcing you to pay for access from your own country.

Whatever the reason to keep people out, VPNhub has a global network of over 1000 servers to get you in. It's like we're giving you over 1000 passports to pick from. You will:

• Never miss a live sporting event

• Never get out of touch with foreign news sources

• Always get the best movie, TV and music streaming selections

• Get to shop for the best subscription prices

All this with the bleeding-edge data protection and no sacrifice to browsing speeds.

Get world class entertainment today!

Gain Professional Cybersecurity at Home

Your home should be your castle, not a glass house!

Logging on from home signals your exact location to every site you visit. This could lead to annoying geo-targeted ads, digital profiling, or much worse invasions of privacy along with data theft.

Remember Big Brother from George Orwell's novel 1984 or better yet, from the reality TV show that put cameras and microphones all around a house? That's sort of like using the internet from home without a VPN, except instead of just being spied on, you might be robbed. The contestants on that show agreed to their surveillance, but you certainly did not.

Even though you encrypt your Wi-Fi with a password, your ISP still knows everything about your online activity. Some ISPs might use that information to make money off your data, some try and control what you read, see and with whom you connect. What's worse, your ISP might just as easily be hacked themselves, compromising your privacy to boot.

A VPN masks your IP so that not even your ISP can follow your online tracks. It protects all your personal data like passwords, search history, and online communication. Finally, it wipes out all logs and records, cleans up any cookie crumbs, and exterminates any bugs or pixels that hopped on to your computer to follow you home.

Get a VPN, because home is where privacy protection begins!

Safely Use Your Workplace's Wi-Fi

It's not just your stapler that might get stolen!

Using a VPN at the office protects any proprietary information that might compromise your business secrets. It also lets you socialize with coworkers without nosey bosses butting in.

Chatting and sharing pics with your coworkers and buddies doesn't mean you're not doing a great job at the office, but bosses usually don't see it that way. Even the most diligent employees want to stay somewhat in touch with their social lives while stuck in their cubicles. VPNs give you the power to keep your online work activity and your online "break" activity totally walled apart.

What's more, all that hard work and intellectual property that gets shared through open office ISP networks might become worthless if scheming competitors hack your system or intercept your communications in order to steal your business secrets. Using a VPN is just good business sense to preserve your competitive edge.

Protect your privacy like a professional on the job and off!

Protect Your Privacy When Using Your School's Wi-Fi

Don't be an open book!

Campuses, dorms and seminar halls are a buzzing hive of personal data. This happens when so many bright young minds all share a communal internet connection.

If knowledge is power, then be weary of that dorm-room hacker amassing power by scooping up knowledge of your private online life. And since college is when so many of us are most curious about new things, our online searches can hand over a lot of power to anyone who accesses them.

There's worse than being hacked by a rogue computer-science major. Students and scholars might be judged by professors, admissions officers, financial aid administrators, or even college deans based on their personal beliefs, or even research that might appear scandalous without the right context. Even within institutions of higher learning can your online educational activity be held against you.

Getting a VPN is the educated move when connected to shared Wi-Fi networks in dorms and all over college campuses. Even if you need to agree to terms and conditions allowing the institutions to monitor your online activity, with a VPN they'll still see nothing but impossible-to-decrypt reams of code.

Close the book on unwanted school surveillance now!

Securely Connect to the Internet Using a Public Wi-Fi

Surf in public, not with the public!

Public Wi-Fis are a great convenience, but these open networks put you at risk from hackers, as well as with the Wi-Fi operator who might be planning to profit off your data.

You're in your favorite coffee shop going over photos for your Facebook or Instagram feed, but there's that one photo from your Thailand vacation nobody should ever see. Next thing you know, you get an anonymous email, and there you are, passed out on a Thai beach, with lewd drawings on your cheek, surrounded by scantily-clad natives laughing at you.

Or maybe you're killing time in an airport terminal and decide to check out that expensive luggage store with the rare lion-skin valise. Later, you're bombarded with ads for African safaris, as well as a barrage of hate mail for being a cruel animal killer. What's going on?

When you use a public Wi-Fi like in a coffee shop, gaming café, shopping mall or airport, you are basically handing over the keys to your privacy and your browsing history. To whom? It might be to the airport who will sell your data to advertisers. Or it might be a hacker sitting quietly in the corner of the café just waiting to get at your photos, emails and passwords.

Public Wi-Fi is not secure. With a VPN, however, you can take advantage of all the free public Wi-Fi, securing your own personal data, without ever worrying about trackers and hackers penetrating your personal privacy.

Make public Wi-Fi a safe surfing space!

Circumvent Censorship

Be beyond borders!

Some countries prevent their citizens from accessing web content outside their virtual borders. VPNs bring world media, news and communication channels to the most censored populations.

● Maybe you are in a country with strict morality laws that keep their citizens from watching some of the best TV shows just because they're a little violent or a tad sexy.

● Or there are laws against games of chance blocking gaming sites or shut you out of your fantasy football league right when you need to make that crucial trade.

● It could just be that national lobbyist greed keeps all of your online shopping within domestic sites even though they charge way more than they should.

There are lots of reasons the internet gets censored. Protectionist industries may want to enrich themselves. States may manipulate minds by controlling news narratives, or police morality by restricting entertainment and games. Or worse, by censoring the use of certain messaging apps and social media sites, governments can prevent their citizens from talking with their friends and families living in other countries.

Just like VPNs can get you access to media from other countries that keep outsiders out, VPNs can also bring you content that your own country won't allow in. This is

done by rerouting the location of your connection to other encrypted servers around the world.

Connect through over 60 locations to counter online censorship!