

Why you need a VPN: here's what a VPN can do for your online security

Be safe and secure on the internet with a VPN and unlock blocked sites and services

By Roland Waddilove | PC Advisor | *18 September 13*

A VPN is useful facility and is essential if you travel with a laptop computer, tablet or smartphone. It can be used by both private users and businesses, but in different ways. There are free and paid versions, and each has pros and cons, so let's take a look at what one is and what it does.

A Virtual Private Network (VPN) connects two computers securely and privately over the internet, even though that is a public network. A VPN client on one computer connects to a VPN server on another computer and by using encryption and other security measures, no-one can see what information is being exchanged.

One use of this technology is to extend a private network across the internet to another location. For example, a business can enable workers with laptops on the road or at home to connect to the company network as if they were sat at a desk in the office. The network traffic is routed across the internet from the user to the company, but it is encrypted and therefore secure from eavesdropping and interception. A company that has offices in two locations can connect them using a VPN across the internet so there appears to be one network.

VPNs aren't just for businesses and because the connection is private and secure, another use is to access the internet anonymously. Anyone that wants to protect their privacy and security online should use a VPN. Everywhere online someone is tracking your activities. ISPs monitor internet usage and may restrict the bandwidth if they detect certain activities. P2P file sharing and BitTorrent traffic is speed-limited for instance. Websites you visit get your IP address, location, browser and operating system, screen resolution, ISP and more. To see what information you reveal, go to stayinvisible.com. A VPN stops websites spying on you by hiding data that could identify you.

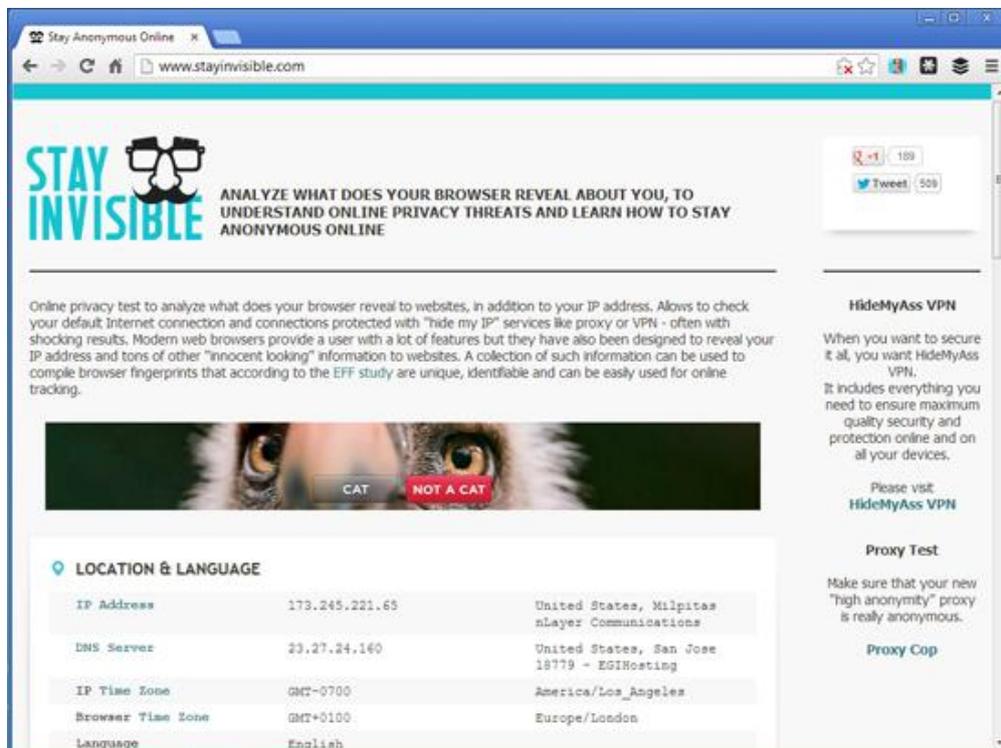
If you use a laptop, tablet or smartphone at a public Wi-Fi hotspot like a cafe, hotel, train station and so on, your activities could be monitored and private information collected. Online shopping and banking may not be safe because of the open nature of the network, and among the people around you could be a hacker. It's unlikely, but you never know. A VPN boosts security because eavesdroppers cannot make sense of your encrypted communications.

If you travel abroad and have tried to watch live TV or catchup TV such as BBC iPlayer you will have discovered that they don't work. That's because they check your location to make sure you're in the UK. So even though you are a BBC license payer and a UK resident, you can't watch BBC when you are away on holiday or business abroad. A VPN can make it seem

like you are in another country, so you can unlock services and websites that are normally blocked.



Try to use iPlayer when you are abroad and it won't let you watch TV.



A VPN substitutes your IP address and location with an alternative one.

How do VPNs work?

VPNs make use of a client and a server. A client program is run on your own computer, tablet or smartphone and it connects to a server to establish a secure and private link. When you run a web browser and enter a website URL the request is sent to the VPN server. The server requests the web page from the site and sends it back to you.

If the website tries to work out who you are and where you live, it queries the computer that requested the web page, but that was the VPN server, not you. If the server is located in the US and has a US IP address for example, the website sees the request coming from a US resident. Similarly, if you are in the US on holiday or a business trip and connect to a UK VPN server then websites you access think you are located in the UK. Your location appears to be the country where the VPN server is running.

Communications between the server and your computer are encrypted, so someone spying on you wouldn't know which websites you access and can't see private information like passwords, usernames, bank or shopping details and so on. A VPN can be turned on and off as and when you need it.

Free vs paid VPNs

There are many VPN servers on the internet and some are free, but the best ones require a monthly subscription. By all means try a free server, but there are disadvantages. For example, they attract lots of users, which means they may be slow. Some are ad-supported and place adverts on web pages you access. Others limit the speed, your time online or data transferred.

When choosing a paid VPN service, check which countries it operates servers in. If you want to appear to be Australian for example, you need a VPN that has servers in Australia. Are there bandwidth limits? Frequently this is linked to price and paying more provides greater bandwidth and speedier internet access. Does the company keep logs of what you access? To really be anonymous you want a VPN that doesn't store logs. Some provide virus and spyware protection, which increases your safety. Are apps for Android and iOS phones and tablets available? Don't forget that they are vulnerable too. Finally, check what protocols are allowed. Do you need VoIP support or BitTorrent?



Your VPN might log your activity, so don't access content you shouldn't.

Popular VPNs

VPN service	Price	Website
JustFreeVPN	Free	justfreevpn.com
Hotspot Shield	Free	hotspotshield.com
VPNBook	Free	vpnbook.com
Free VPN Access	Free	freevpnaccess.com
Private Internet Access	£26 a year	privateinternetaccess.com
Pure VPN	£32 a year	purevpn.com
Strong VPN	£35 a year	strongvpn.com
Boxpn	£45 a year	boxpn.com
Internet Anom VPN	£79 a year	steganos.com/UK

Source: [Why you need a VPN: here's what a VPN can do for your online security - PC Advisor](#) Accessed 12/4/2015