CYBER WORKS

Virtual Private Networks

What are they?
How do they work?

Audience: General

Reading Time: 10 Mins

Virtual Private Networks (VPNs) are increasingly being used to work from home and have many uses, from being able to access the office IT network, or critical business systems; to being able to watch TV normally available in your own country.

Key Points

- By default the Internet does not have security protections built into it for communications, hence the need for additional protection like VPNs.
- VPNs use technology to make protected tunnels through the Internet for two or more people to communicate securely.
- VPNs can prevent the prying eyes of criminals and other malicious actors from seeing what you do online.
- Not only does a VPN protect communications, but can also make your device appear to be connected to a different part of the Internet than it is.
- They enable us to work from home, or in public locations, securely to access office IT services remotely.
- VPNs increase our privacy online by hiding what we do, but someone will always be able to see what we do.
- VPNs are often provided by companies for workers to connect, but individuals can buy VPN services for their own private use.

Virtual Private Networks

We are constantly bombarded by adverts for Virtual Private Networks (VPNs) through TV and online advertising. They make claims offering a range of security benefits to allow you to "stay safe online". Yet, it is not always fully explained what VPNs are? How do they work, and are they really the all-in-one solution of computer security?

How does the Internet work?

To understand how a VPN works, we first need to understand how the Internet works. When you connect to the Internet at home, you normally do so through an **Internet Service Provider (ISP)** such as BT, Sky or Virgin Media etc. if you are in the UK. Similarly a business would also connect to the Internet through the services of an ISP. Your ISP gives you an **IP Address** that is used to identify you as their customer and identifies you uniquely on the Internet – you can check out your ISP and IP address on https://bgp.he.net/

Comparing the Internet to the Postal Service, the ISP is the courier that delivers the mail and accessing a website is the same as sending someone a letter. A postal address has multiple parts: Postcode, Town, Building Number and Street Name. Similarly, an IP address has two parts: the network and the host. Just as the street name identifies a community of people, the network part of the IP address identifies which ISP you, and their other customers, belong to. The host part identifies the particular device in that community, in the same way a house number identifies a particular building.

Imagine that your return address is placed on every single letter you send, and thus any letter that you send can be traced back to you - this is the same with your IP address and your ISP. Websites you visit can see your IP address and might be able to determine where in the world you live; they can work out which ISP owns that IP address and see where they operate. Now consider that because all of your letters go through your ISP they can see who you are sending letters to and what these contain. This can be prevented by encrypting the contents of the letters that you send; so that only you and the person you are sending the letter to (the website) can read it. This is comparable to writing a letter to the website, but instead you place the letter in a box and then lock the box with a padlock that only you and the website have keys to. The ISP can still

Definitions

IP Address - An IP address uniquely identifies you on the internet, much like your home address uniquely identifies where you live. IP addresses come in two formats that are easily recognisable: 4 numbers separated by dots (such as 216.58.211.174) or a longer series of both letters and numbers separated by colons, such as 2a00:1450:4009:81c::200e.

Internet Service Provider (ISP) - The organisation that provides you access to the internet.

VPN Provider - The organisation that manages and hosts the VPN, this may be your employer, but there are plenty of commercial offerings available.

HTTP - A mechanism used to access websites on the internet, it does not encrypt any data and anyone can see what you do on websites when using HTTP.

HTTPS - A mechanism used to access websites securely by preventing anyone but you and the website from seeing what you do on a website.

Geographic-based content restrictions - Restrictions put in place by a website to restrict access to certain content based upon a geographic location, such as a country or region.

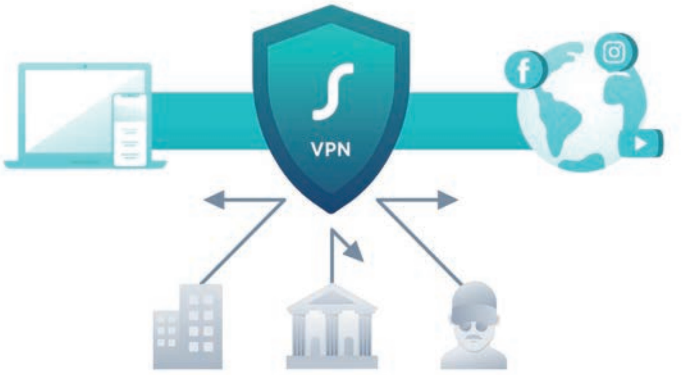
see who you are communicating with because they can read the address on the box, but they cannot unlock the padlock and read the letter because they do not have the key. This mechanism is called **HTTPS** on the internet, it prevents anyone but you and the website from reading the data you exchange. A website is using HTTPS if the website address starts with https:// - this is shown in some web browsers as a padlock in the address bar. Pay attention to the 's' - or lack of it! If HTTPS is not used, then a mechanism called **HTTP** is used instead, which is not encrypted and just like sending a letter in an envelope that anyone can open.

What is important to note is that by default the Internet does not have security protections built into it. Additional protections, as described previously with HTTPS, are layered on top to provide more protection. Adding additional security, like a VPN, to your Internet communications is like buying a vintage car and fitting an aftermarket alarm system.

So, what happens when I am using a VPN?

When you use a VPN, instead of sending the letter (HTTP or HTTPS) to the website directly, you instead send it to your VPN provider placed inside a special padlocked box - let us call it the "VPN box". This is locked with a key that only you and the VPN provider have, and so only you and your VPN provider can read the contents.

You put your IP address as the return address of this "VPN box" and send it to your VPN provider. The VPN provider unlocks the "VPN box", takes out the letter addressed to the website, replaces your IP Address with the VPN's IP address before they forward on the contents of the letter they unlocked to the website. When the letter is received, the website reads the return address to determine who sent it, but when a VPN is used this return address belongs to your VPN provider – not you! This means that the website thinks that your IP address is the one belonging to your VPN provider. When the website sends its response back, it sends it to your VPN provider, who then place it in a locked box and send it back to you. You then unlock this box and can then read the response from the website inside.



This advantage of sending the data to the VPN provider first, instead of directly to the website, inside of a locked box is twofold, it ensures that only the VPN provider can see which websites you are viewing and what data you send.

There are a few key points about this:

- In spite of the encryptions, your ISP will know you are using a VPN as this traffic passes through the ISP, so they can see your traffic is addressed to the VPN provider. However, as they cannot see the contents the ISP does not know which websites you are visiting.
- The websites you visit will not know your real IP address, where you are or who you are (unless you sign and give them your information). The website will know you are using a VPN as they are sent boxes with the VPN provider as the return address.
- The VPN knows which websites you are using as all your traffic is sent through them and they unlock the box which contains the package to forward to the

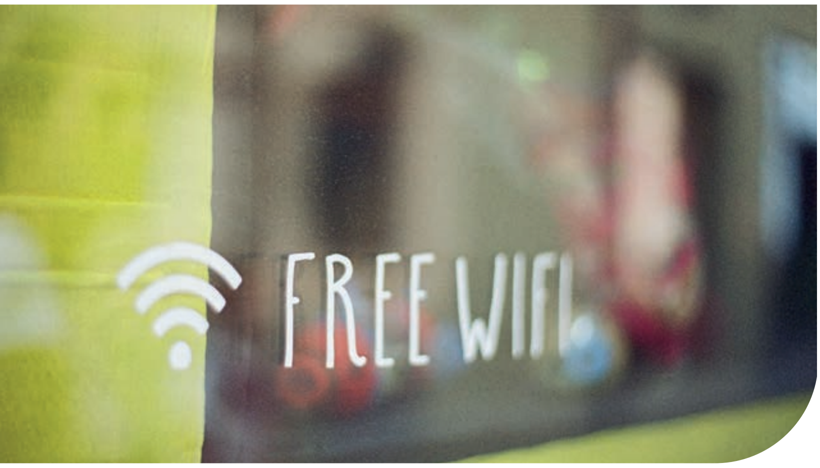
website. If the website is using HTTPS, then the VPN provider will not know the content of the messages sent between you and the website, but they will if you are using HTTP.

A VPN simply shifts which party can see who you are communicating with from your ISP to your VPN provider.

So why use a VPN?

VPNs can be used for many reasons, both by businesses and by individuals. A VPN can be used by employees of a business to work from home, but still use the company's IT network as if they were physically in the office. This can give access to certain resources, such as a company intranet that would otherwise not be available. As working from home has become increasingly more common, this enables the transition to be just as seamless as working from the office in many respects.

An additional benefit is that all data between you and your VPN provider, in this case your employer, is encrypted. You can be sure that working from home is equally as secure as working in the office.



Individuals can also use VPNs, but an individual's main motivation for using a VPN would be to mask their real location and IP address. This is usually for one of two reasons: privacy; or bypassing **geographic-based content restrictions.**

A VPN can improve privacy by preventing as many parties as possible from seeing which websites you visit. This can protect your data from prying eyes from both your ISP and people using the same Wi-Fi network. The classic example being freely available Wi-Fi such as that available in cafés, restaurants and other public spaces, which often lack any kind of security mechanisms. Potentially, anyone on the same Wi-Fi network as you can see which websites you visit and what data you submit to these websites when not using HTTPS, such as your passwords and card details. However, when you use a VPN nobody using the same Wi-Fi network can see which websites you use, or what you do on these websites – even if you are not using HTTPS.

Many VPN providers appeal to those concerned with their privacy and offer a "no logs" policy. Despite them being able to see which websites you visit they often claim not to store or do anything with this information, but this is not always the case.

On the other hand, as the website knows neither your real IP address nor location, only that of your VPN provider; geographic content restrictions can be bypassed, such as those used by streaming services. VPN providers often have servers in multiple different countries, allowing you to use their IP address in country of your choice. For some services, this allows the films and TV shows available to you to be reflected in the country of your VPN provider. Many VPN providers specifically sell to this market – offering many countries to choose where you will appear to be, for example giving you the choice of which version of Netflix you see!

What about The Onion Router (Tor)?

Tor is an anonymity network which provides privacy to its users. It is a web browser based off the popular Firefox browser by Mozilla. It was originally developed by the US Naval Research Laboratory with the aim of protecting US government communications

– it still receives funding from the US federal government.

Using a technique called "Onion Routing" it aims to give users anonymous access to the internet by bouncing traffic through many thousands of volunteer global computers acting as network nodes before reaching its destination. It has historically been the target of multiple successful attacks over the years aiming to de-anonymise its users.

It is Tor's strong anonymity features which draws people to it. Although it is used for legitimate and ethical reasons, the privacy and anonymity it can potentially provide may also attract less ethical and illegitimate activity. Political activists, whistle-blowers, those in oppressive regimes or in countries with strong censorship all make use of Tor to bypass restrictions placed on them in their countries. However, it also draws the attention of malicious actors and other people committing crimes attempting to evade identification from law enforcement agencies. Using the Tor network is not illegal in the UK, and is actually the only way to access certain website which use an .onion address, otherwise known as Tor's hidden network.

Onion routing works by the Tor browser first randomly selecting three special computers called "Tor relays" from a list provided to it – these chained together form a "circuit". The browser gets the message you wish to send to the website – which may be using HTTP or HTTPS – and placing it in a box that is locked with a padlock that only the first Tor relay and you have keys for. This box is then placed inside another box and is locked with a padlock only you and the second Tor relay have access to. This is then locked again in a box with a padlock that only you and the third Tor relay have. By this time, you end up with the original message locked in three additional boxes – just like Russian nesting dolls!

The next process is where Onion Routing gets its name, like peeling the layers of an onion. To peel off the padlocks, we send it first to the third relay as its padlock is locking the outer box. This removes its padlock and sends it to the relay whose padlock locks the new outer box – the second relay. This also removes its padlock and sends it to the first relay which removes its padlock. We are now back to the original message.

The relay sends the package inside the box to the website. Just like a VPN, the last relay can see which website you are using, if HTTPS is not used the last relay will be able to read the data you send. Although this process may seem redundant, it ensures that no relay knows both the person sending the message, and where it is going, which is what gives Tor users their anonymity.

When the website sends its response, the process now works in reverse. This relay places the message in a box and adds its padlock to the message and forwards this to the second relay, and so on and so forth. It then sends this back to you and you receive this message-in-a-box-in-a-box-in-a-box. You take each padlock off and remove it from the box in turn and can read the message sent to you from the website.

This multi-layered mechanism ensures that no relay, knows both the sender and receiver of the message.

The first relay knows that someone is accessing a website through Tor but does not know the website they are visiting. The second relay knows neither the user nor the website, meanwhile the third relay knows only the website that someone is visiting – but does not know who is.

In summary, VPNs can offer security to otherwise unsecured networks such as those found in cafes, restaurants and public spaces and prevent prying eyes from being able to see what we are doing online. VPNs are being increasingly used to enable working from home to give access to the office IT network. They can also be used to provide a degree of privacy to users and to mask their real geographical location. However, they do not make you truly anonymous, they only shift who is able to see your online activity to a different 3rd party, whom you still have to decide if you trust or not.

At minimum, you should use a VPN when working on an unsecured network (i.e. public Wi-Fi) to protect your data.

READ MORE

1. VPNMentor. 2020. Report: No-Log VPNs Exposed Users' Logs and Personal Details for All to See [ONLINE] at https://www.vpnmentor.com/blog/report-free-vpns-leak/ [Accessed 3rd September 2020].
2. Electronic Frontier Foundation. HTTPS Everywhere [ONLINE] at https://www.eff.org/https-everywhere [Accessed 3rd September 2020]
3. NCSC. Virtual Private Networks (VPNs) [ONLINE] at https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks [Accessed 3rd September 2020]
4. ZDNet. 2020. A mysterious group has hijacked Tor exit nodes to perform SSL stripping attacks [ONLINE] at https://www.zdnet.com/article/a-mysterious-group-has-hijacked-tor-exit-nodes-to-perform-ssl-stripping-attacks/ [Accessed 3rd September 2020]
5. Privacy.net [2018] Everything you wanted to know about Tor but were afraid to ask [ONLINE] at https://privacy.net/what-is-tor/ [Accessed 3rd September 2020]
6. The Tor Project https://www.torproject.org/

About the Author

Henry Clarke is currently studying at Lancaster University. Henry has completed his BSc in Computer Science at Lancaster and is now studying his MSc in Cyber Security. Henry is part of Lancaster's Cyber Security society **LUHack**, his interests are cyber security and programming.