VPN Research

Liam Hughes

What is a VPN

A Virtual Private Network (VPN) is an encrypted connection, also known as a tunnel between your device and the server operating the device. It can be turned on or off when needed. For commercial and business use, VPNs can be used to go through the remote server hosting the VPN to reach the Internet as regular without a VPN.The same goes for data coming from the Internet to your device, it travels the same path.

A VPN can mask your IP Address so you can create a private network connection on a public network. A VPN hides a decent amount of information from bad actors. Bad actors are hackers, malicious people, anyone wishing to steal your information. Some content a VPN hides is browsing history, your location, your IP Address, etc. VPNs usually protect you from bad actors on many public Wi-Fi networks. An important thing to remember instead of paying for a VPN is that you can just choose not to connect to any private information such as banking information and such.

As for the question of whether VPNs allow a person to become anonymous or not, the answer is simply no. Although it does provide you with increased privacy on networks you use it on. Such examples of not having privacy include your Internet Service Provider (ISP). Even if you have a VPN connection your ISP has figured out ways to see your data going through and out the VPN. Another group that can see information are site advertisers. They cannot see your data straight away but over time they will be able to build up unique characteristics about your device by using trackers and cookies. Once they build up enough unique characteristics, they can eventually get a unique signature identifying the device you are working with.

So, are VPNs worth purchasing? Find this out in the Why you should use a VPN?

[What is a VPN? How does a Virtual Private Network Work? | Fortinet]

[Why You Need a VPN, and How to Choose the Right One | PCMag]

History of VPNs

VPNs were first created and used in government projects and corporations. They were originally used to offer government and corporate employees a way to access their work devices from elsewhere. The first set of Virtual Private Network (VPN) protocols were created in the year 1995. This is the history of VPNs:

1995: PPTP and IPSec

Point-to-Point Tunneling Protocol (PPTP): The main purpose of this protocol was to create a secure connection to work and home computers when needed. Used by Microsoft and other companies such as that.

Internet Protocol Security (IPSec): This protocol started off as a DARPA (Government Protection) project in the 1970's and was then backed by NSA in 1986. NSA creates security protocols for the Internet.

1998: IKE

Internet Key Exchange (IKE): Used in IPSec to set up an encryption exchange between the two devices that will form a secure VPN connection. Although due to flaws it has been upgraded to IKEv2. IKE is not as secure as its predecessor and the 2nd version is much more secure.

2000: L2TP

Layer 2 Tunneling Protocol (L2TP): This protocol helped ISPs deliver their services and supported VPN connections. One major flaw of this protocol is that it did not have any encryption. This protocol always was paired with IPSec and will continue to be so that there is encryption. The L2TP/IPSec protocol allows for double encapsulation.

2001: OpenVPN

OpenVPN: This protocol was developed by James Yonan. OpenVPN was the first open-source VPN. This marked the first changing point in VPN history. OpenVPN made it possible for devices using VPNs to authenticate each other using pre-shared keys, usernames and passwords, and digital certificates. This protocol is still in use to this day.

2005: IKEv2

Internet Key Exchange version 2 (IKEv2): Fixed IKEv1's security vulnerabilities and added more functionality. One of these is MOBIKE which helped resist network changes in a VPN.

2008: SSTP

Secure Socket Tunneling Protocol (SSTP): This protocol still used PPTP to encrypt packets but added an extra SSTP header to add an extra layer of SSL encryption. This protocol is a closed source VPN protocol and used by Microsoft.

2014 & 2019: Soft Ether, Chameleon, and Wireguard

Soft Ether: A more recent protocol made in 2014 that was open source, offered high-end security, and provided better speeds compared to OpenVPN and PPTP.

Chameleon: The only VPN protocol created by a VPN provider in 2014. Although this marks this protocol as closed source. This protocol allows you to hide both your VPN and regular traffic. This is to prevent the ISP and government from seeing that you are using a VPN.

Wireguard: The latest form of a VPN protocol made in 2019. This protocol looks to pass OpenVPN and IPSec. It uses many new forms of encryption and other security measures. Although Wireguard is a work in progress.

VPN History - From 1995 to The Present | TechNadu

Where are VPNs Used

The original intended use for VPNs was to access work devices from the safety of your home. Nowadays we have a few more uses for it. Some of these uses include being able to view movies or other content on the internet only available in other countries and banned in your own. Although VPNs are secure, the term only belongs to the encrypted connection from the device you are using to the VPN server. Any data past the server and on the Internet is not protected and can still be stolen. Go to Why should you use a VPN for more on that topic.

What are the Types of VPNs?

Remote-access VPNs: Allows users to connect to a remote network in a secure way. Used in businesses to connect to your work devices on the company's network.

Site-to-site VPNs: Used by bigger organizations to connect multiple company networks using a VPN. These kinds of VPNs are also known as intranets and are used still to this day from companies with multiple locations.

Personal VPNs: designed for individual people, allowing access to VPN servers and the blocked country restricted content. Examples of some include NordVPN, Surfshark, Norton, etc.

What Is a VPN? How Does It Work & Why Should You Use It? (techrepublic.com)

Why should you use a VPN?

Personal VPNs, despite what many believe, can be considered useless due to the many companies that do this for profit. Many things have changed about VPNs to where they are no longer as valuable as they once were. ISPs as previously stated, have basically caught on to VPN tunneling making it more and more useless which means they could turn off the connection or adjust it so that it does not work as well. Hackers are also starting to target VPNs more and more due to the belief that they are safe. A lot of the known ones are getting less and less secure over time.

Unless you are using a VPN to connect to your workplace, they are not as viable as much anymore. That does not mean you still can't get to other countries. Its just getting a little harder to do so.

What are the Pros and Cons of VPNs?

Pros:

- Secures data and internet traffic from the connection going from the device to the VPN server or device.
- Prevents tracking up to a certain extent.
- Allows for access to country restricted items.
- Allows you to access work-related items from anywhere.

Cons:

- Slower internet speeds
- Payments for fully functional VPNs

- VPNs are not always being secured.
- Not any protection past the VPN server.
- Not always reliable.
- Some VPNs not actually doing anything other than taking your money
- Some free VPNs can sniff the data you send out.

What Is a VPN? How Does It Work & Why Should You Use It? (techrepublic.com)

Bing Videos

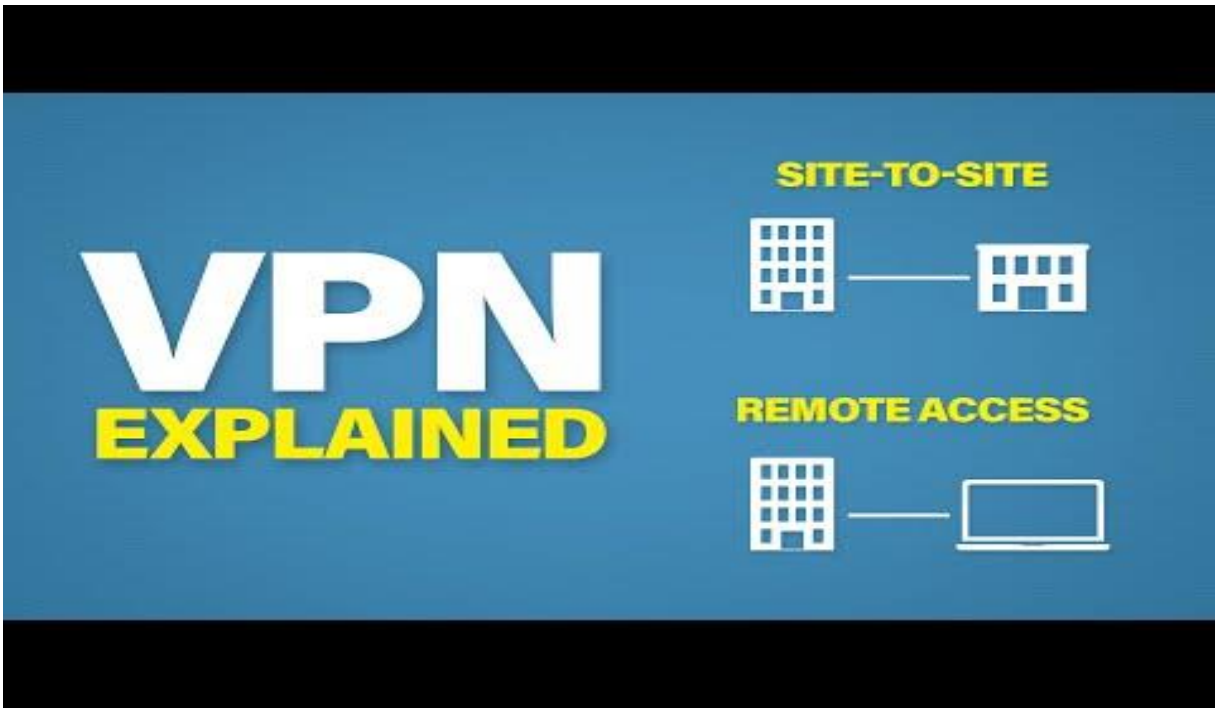
If you want to look at more:

What is VPN? How It Works, Types of VPN (kaspersky.com)

Why VPNs are a WASTE of Your Money (usually...) (youtube.com)

Don't Use a VPN...it's not the ultimate security fix you've been told (youtube.com)

VPNs Explained | Site-to-Site + Remote Access - YouTube



5 Pros and Cons of Using a VPN (youtube.com)


5
PROS & CONS
OF USING
A VPN