Finally…. VPNs: What they are used for and how do they work?

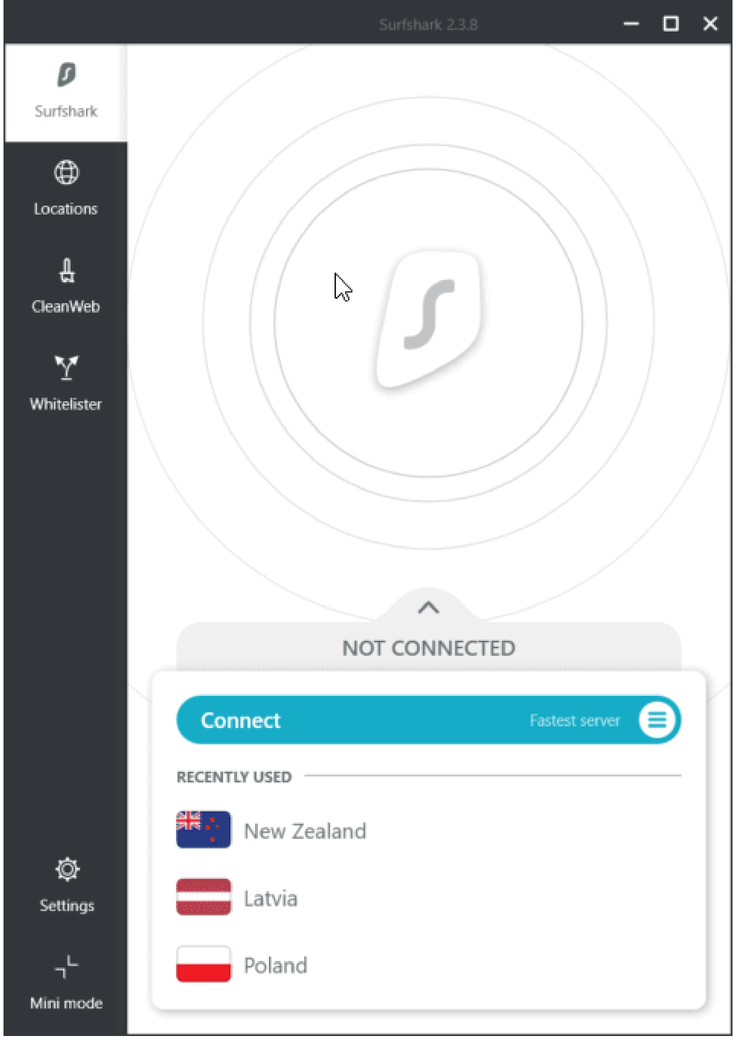
Finally we've come to the discussion topic that we've been waiting for: **VPNs. A Virtual Private Network.** According to Cisco, a VPN is defined as "an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely." The key word here in the definition is encryption which we briefly mentioned in part two but will discuss later in this article. But for now, after hearing that definition, I'm sure you're wondering what this exactly means and how it works. We will first give you a very broad overview as to how a VPN works in this section and then afterwards, we will get into the more detailed explanations of how A VPN operates.

Now you may have heard about VPNs one way or another in these past couple years either pre or post pandemic. Whether it was advertised to you in an ad on a website or on TV, or most likely talked about by a Youtuber you watched before. The big takeaway from this is that more people either have already heard about VPNs or may already be using one either for commercial use or for a job. It's important to note the differences between commercial VPNs and enterprise/corporate VPNs.

Commercial VPNs are ones that are sold to users as a pay-to-use monthly service and these users primarily utilize these VPNs in their leisure time day in and day out. One of the most popular reasons that users may begin paying for access to a commercial VPN is their ability to bypass geographically restricted content online. This is online content that is inaccessible if the location you are using the internet from does not match the location that the content is being hosted for. A common example of this is a handful of Netflix's shows and movies being accessible only to one of their many service locations worldwide. For example, Netflix UK has access to watch the movie "The Wolf of Wall Street" for all Netflix subscribers that live in the UK. But the movie is not accessible in Netflix's US locations or any other Netflix users outside the UK. That's where commercial VPNs come in handy.

Image Source: https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access

Lets use Surfshark VPN as an example of this. If you want to watch Wolf of Wall Street on Netflix and you are located in the US, but its only available for viewing on Netflix in the UK, you can use Surfshark VPN's location changing feature where it takes your signal and makes the request to view Wolf of Wall Street from one of Surfshark's UK server. Making it seem like to Netflix UK that you are accessing the site to view from the UK, when technically you aren't.



This whole process of a user connecting to Surfshark VPN, changing locations and accessing geo-restricted content using Surfshark's server's to use it is essentially you **virtually** accessing Surfshark's **network** of computers that is **privately** accessible to only you and other Surfshark users paying for their service.

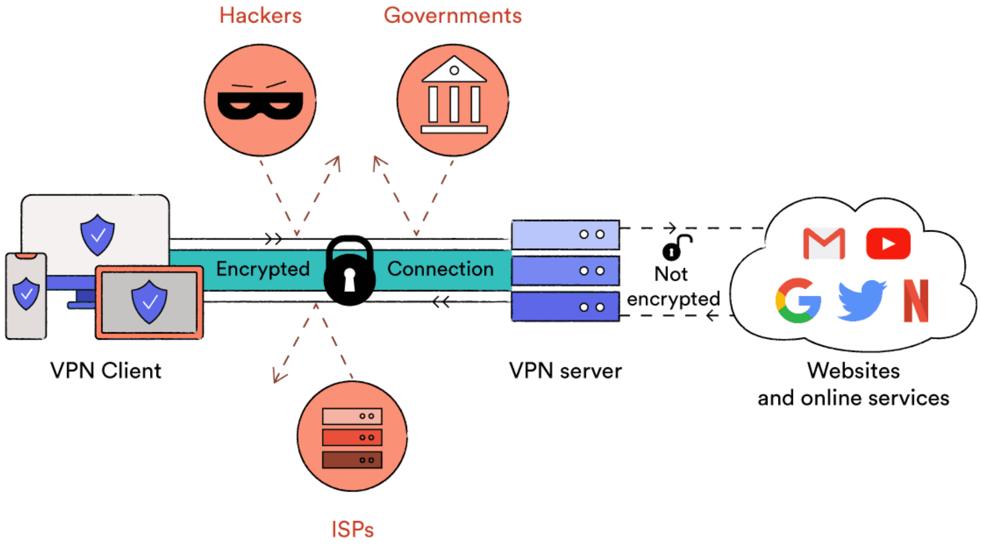


Image Source: https://www.top10vpn.com/what-is-a-vpn/how-does-a-vpn-work/

Enterprise/Corporate VPNs operate very much in the same way. The only difference is they are used by employees on company-distributed devices to access resources exclusively to the business or company they work under. These work resources are restricted or near unreachable to anyone else outside of the organization and that's why employers usually require the use of an enterprise VPN for their employees to access them.

Encryption is a word you will want to hold onto as it is very important to the world of IT, tech and internet Security in general. Encryption is defined as a method of securing data by encoding the data mathematically as it traverses the internet and it can only be decrypted and read by those with the correct key or cipher. In other words, it's a way of taking the data that you send out from your computer or device, taking that data, blending it up in a way to where it's no longer legible when traveling the internet and reaching its destination so that hackers can't intercept and see what you are searching for or looking at in your data.

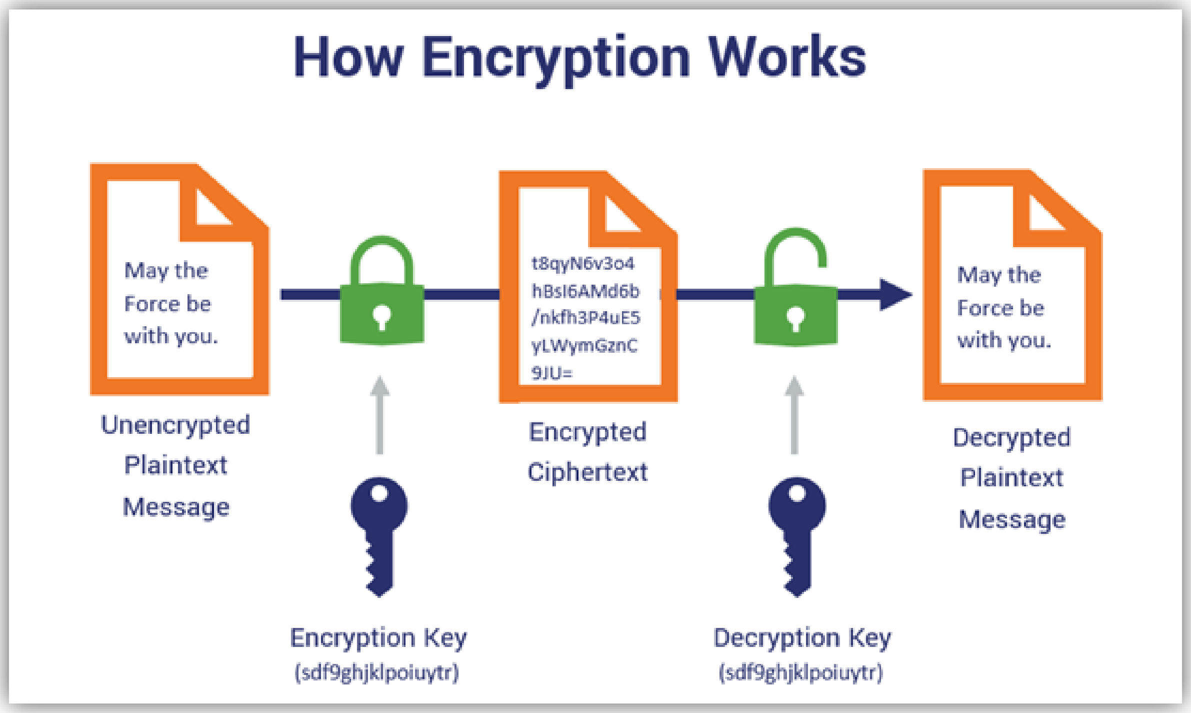

How Encryption Works
May the Force be with you.
Unencrypted Plaintext Message
t8qyN6v3o4 hBsI6AMd6b /nkfh3P4uE5 yLWymGznC 9JU=
Encrypted Ciphertext
May the Force be with you.
Decrypted Plaintext Message
Encryption Key (sdf9ghjklpoiuytr)
Decryption Key (sdf9ghjklpoiuytr)

Image source: https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/

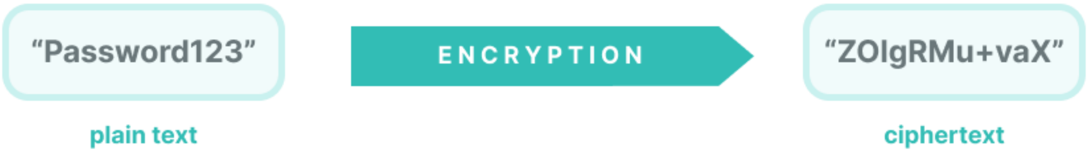


Image source: https://www.egnyte.com/guides/governance/data-encryption

The practice of encrypting data takes many shapes and forms in the Internet and IT world but it especially takes its own when applied to a VPN. All VPN Services that you see advertised have their own particular methods and ways of creating a protective "tunnel" (aka an encryption tunnel) that makes the data you send out illegible to snoopers, potential hackers and even your ISPs. There is a fantastic article that dives into detail about the various types of VPN encryptions and I will link this article here.

OpenVPN is an example of a type of encryption that is used on the app you are reading off of right now! Yes, OpenVPN is an open source VPN technology that uses parts of OpenSSL to create a reliable and efficient VPN service that securely encrypts a user's data and makes it

easy to adjust and add on more features if needed to the service. We will not be revealing all of the tricks under magician's hat as to how our app exactly operates, but we will give you a bare bones example of how the OpenVPN encryption works.
Getting an OpenVPN-based VPN service to begin is like with any other service hosted online; it begins with a **server**. Now a **server is the home and host for all websites, services, systems, controllers, applications** etc. hosted on the internet, internally within a company or anywhere else in the world that you cannot reach locally on your own home network by yourself. Now a computer is just a computer if it's not hosting a service or website to be used by others. Once it's hosting a service or website or something else to be used by you and others either in your home or work or outside, then it's a Server. And a server can be a regular computer with hardwares and wires, or it can be a server you can create in a cloud. Either way, An OpenVPN server is created once the OpenVPN service is added to a computer to host it. This can be done in several ways, but the easiest way is to download a version of the OpenVPN service either on Github or on their official website that is fit for your computer's operating system.

Next after installing, you configure the baseline settings of the server such as which port the service will be hosted on the server, and what protocol it will use to receive and transfer data from people using the OpenVPN service. Next is the step of creating client profiles. These profiles can range anywhere from being accounts objects that can be created in a few clicks of the mouse to .ovpn files that are created for users to be used in a broader sense. These profiles and .ovpn files are very important as they contain "certificates" that are one of a kind for the user and the user will need to have when trying to connect to the VPN to verify themselves to be able to use the VPN service. Once you have the client profile or client ovpn file created, you then need to give the users that will use the OpenVPN service the client profile/file information.

This can vary in form depending on how they connect to the server. You can download the OpenVPN client application to use on Windows, Mac, Linux or mobile to use. Once the client profile/file has been provided to the user by entering the information into the client application, they should be able to click the connect button on their devices, the certificate contained within their client profile/file will be sent to the server, the server will check to see if the certificate matches what they have on file, and the server will send back confirmation that they are now connected to the OpenVPN service.

Vulnerabilities, Threats and Attacks

Now with all this talk about VPNs, Firewalls, and Encryption that have to do with protecting your data, your traffic, your packets, etc. it's time we talk about the scary stuff. The stuff that IT guys and tech industries look out for and take all these measures to prevent from happening. And that is Vulnerabilities, Threats and Risks as they relate to the computing and IT world.

Now what exactly are the definitions and meaning behind these words. Sure they sound intimidating, but what about them makes them so terrifying? The best place to start would be their definitions.

Vulnerability: Any weakness that could be triggered accidentally or exploited intentionally to cause a security breach (Example: Exposed ports, flimsy security in a building)

Threat: Any potential violation of security policies or procedures (Example: someone use the wrong account, someone gives themselves more access and privileges)

Threat agent: A person or event that triggers a vulnerability accidentally or exploits it intentionally

Risk: The likelihood/chance and impact (or consequence) of a threat actor exercising a vulnerability.

All dangerous or mal-intentioned activities out online can fall into any of these categories. Now it's also very important to keep in mind that while these are all quite concerning to say the least, these are not always done with bad intentions behind them or may have been committed by accident in some cases. This is what is known as an Unintentional threat or vulnerability.

Unintentional threats are considered to be human error, environmental hazards, and computer failures. Most people don't purposely cause harm.

If you ever wonder why someone in IT might get snippy with an employee who has passwords for their corporate accounts all written down on a sticky note, that employee obviously does not mean to cause harm by doing that. They are just trying to remember their passwords after all in the case that they forget to login. But it is a very serious ***risk or threat*** to be leaving written passwords lying around anywhere near your desk area or even anywhere around an office space. This is because while you may have no bad intentions behind jotting down your password on a piece of paper to save for later, someone else at your company may have other ideas. Perhaps they got demoted or were recently written up.

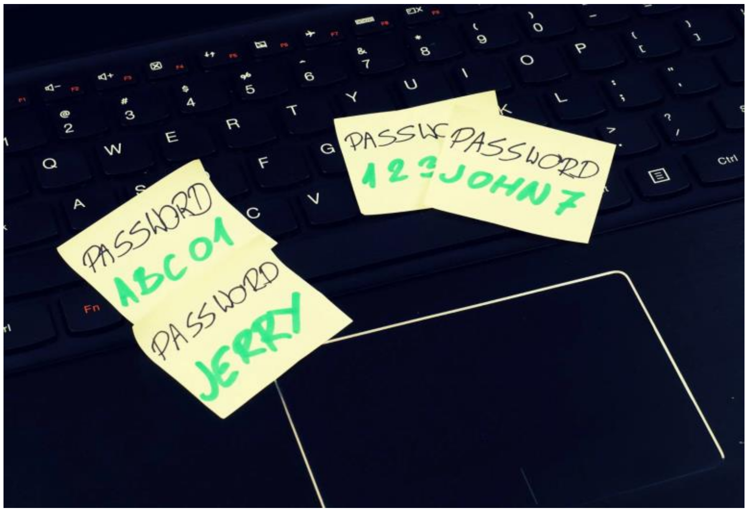


Image source: https://calls2tech.com/are-you-using-the-same-password/

They may be pretty bitter and if they feel like getting back at the company and see your password, they may use it for their benefit to mess or screw over the company and then quit shortly afterwards. Just as the idea has been mentioned that the internet and the world of technology can be an unpredictable and scary place, the sad reality is that it's not the technology that’s scary, it's the people behind these attacks that make the internet scary and unpredictable. The AI, bots, scams and attacks that are deployed would only be a bundle of ones and zeros if a person didn’t make them. This leads us into our next discussion being **Intentional threats.**

Intentional threats refer to purposeful actions resulting in the theft or damage of computer resources, equipment, and data.

Going back to our employee with the password written down on a sticky note, whether it was done with malice or not, to the IT guy, either way doesn't matter to him; the common factor that lies behind both ways of creating a threat or risk is **negligence**.

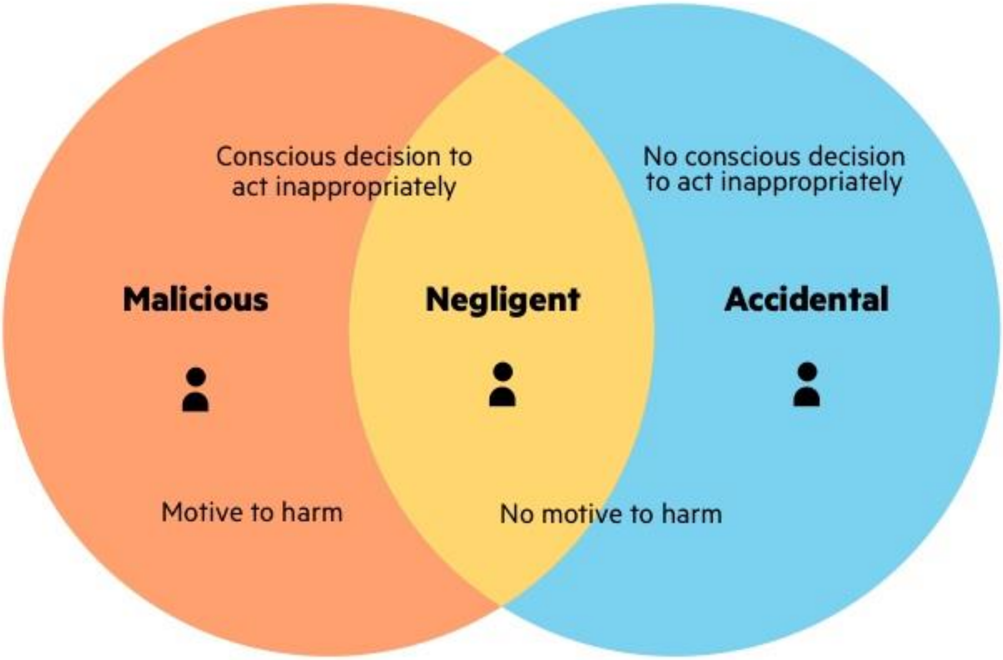

Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

Image source: https://www.imperva.com/learn/application-security/insider-threats/

I know I already provided a loose example of an intentional threat earlier with the sticky note example, but let's apply a different type of threat, one that not alot of people may have even heard of. Social Engineering is a type of a potential threat or attack that can happen at any company big or small. Social Engineering: A hacking technique whereby the hacker gains useful information about an organization by deceiving its users or by exploiting their unsecure working practices. (Example: Phishing, Phone calls pretending to be someone legitimate etc.)
Various ways that Social Engineering can take forms is:

- Attacker gains insider knowledge
- Attacker often carries out multiple small steps to gain access
- Attacks depend on human factors
- Attacks come in a variety of ways:
  - In person
  - Email
  - Phone
- Often targets non-technical users and users who need assistance

Common Social Engineering Exploits:

- Impersonation
- Phishing
- Spoofing (spoof an IP address, email address or MAC Address)
- Dumpster diving (someone going through trash to find sensitive information; such as thrown out documents or disposed hard drives)

- Shoulder surfing
- Tailgating (when you follow someone into a building without authenticating yourself via an access card or key card)