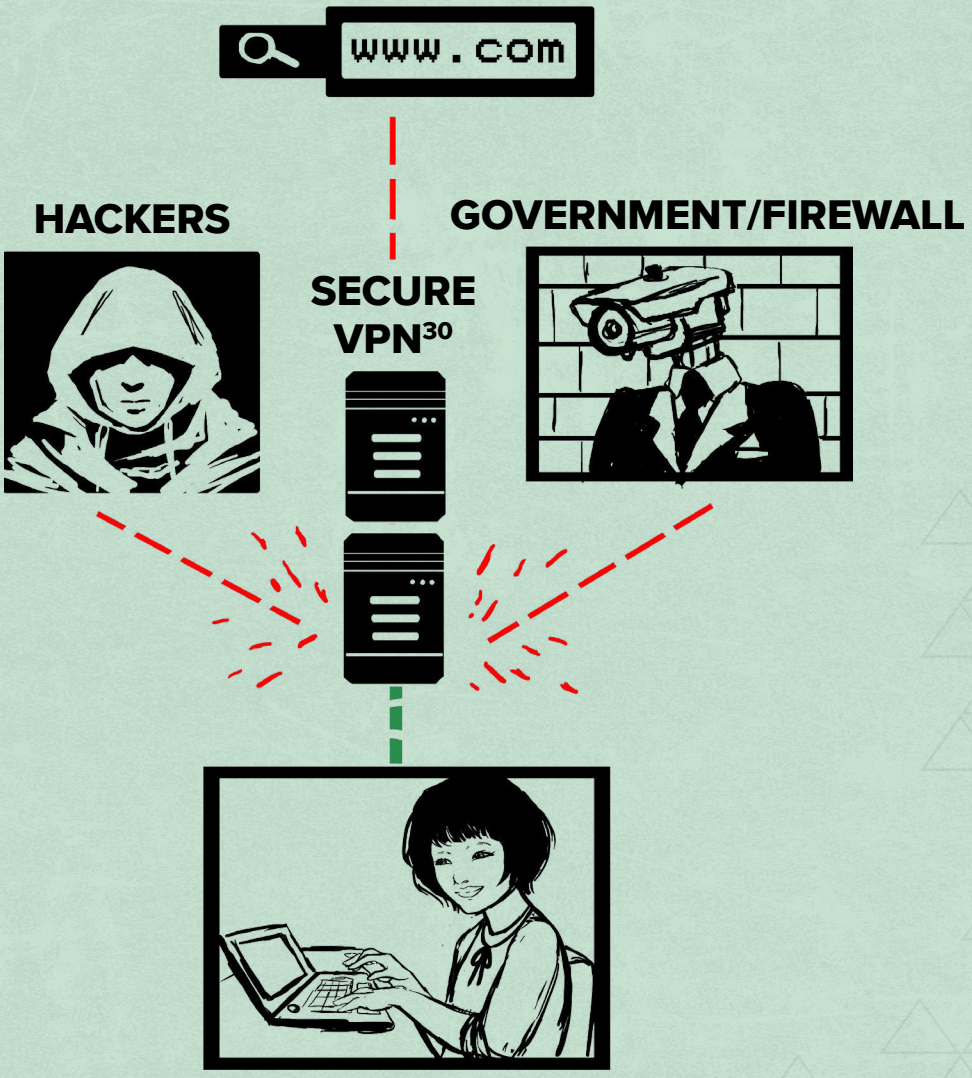
CONNECTING TO THE INTERNET—HOW DOES IT ALL WORK?



The first step to connect to the Internet is typically made through an Internet Service Provider (ISP) at your home, office, cafe, library, or Internet cafe. Common ISP's in the US are Verizon Fios, Xfinity, and Time Warner Cable.

[30] https://securityinabox.org/en/lgbti-mena/anonymity-and-circumvention

The ISP then assigns your computer an IP address, which various Internet services can use to identify you and send you information, such as the emails and webpages you request.

Anyone who learns your IP address can figure out what city you are in. Certain organizations in the country, however, can use this information to determine your precise location.

Using your IP Address, your ISP will know which building you are in or which phone line you are using. Additionally, your internet and phone providers will know which device you were using at a given time, as well as which port or wireless access point you were connected to. Government agencies may know all of these details, as a result of their influence over the organizations above.

Your data funnels through ISP's which operate on the network infrastructure in your country. ISP's connect you to wesites that exist all over the world.

On the other end of your connection, the website or internet service you are accessing has gone through a similar process, having received its own IP addresses from an ISP in its own country.

This summary, even without all of the technical details, is super helpful when considering the various tools that allow you get around filters and remain anonymous on the internet. If you feel comfortable and now grasp this overview, read on to see how you can best protect your network access!

HOW WEBSITES ARE BLOCKED OR CENSORED

Essentially, when you go to view a webpage, you are showing the site's IP address to your ISP, and asking it to connect you with the webserver's ISP. And, if you have an unfiltered internet connection, it will do precisely that. If you are in a country that censors the internet, however, it will first consult a blacklist of forbidden websites and then decide whether to comply with your request.

In some cases, there may be a central organisation that handles filtering in place of the ISPs themselves. Often, a blacklist will contain domain names, such as www.jhalkaribai.com, rather than IP addresses. And, in some countries, filtering software monitors your connection, rather than trying to block specific Internet addresses. This type of software scans through the requests that you make and the pages that are returned to you, looking for sensitive key words and then deciding whether or not to let you see the results.[31]

To make matters worse, when a webpage is blocked you may not even know it. While some filters provide a 'block page' that explains why a particular page has been censored, others display misleading error messages. These messages may imply that the page cannot be found, for example, or that the address was misspelled.

In general, it is easiest to adopt a worst-case perspective toward internet censorship, rather than trying to research all of the particular strengths and weaknesses of the filtering technologies used in your country. In other words, you might as well assume that:

Your internet traffic is monitored for keywords.

- Filtering is implemented directly at the ISP level.
- Blocked sites are blacklisted by both their IP addresses and their domain names.
- You may be given an unclear or misleading reason to explain why a blocked site fails to load.

[31] https://www.eff.org/torchallenge/

BROWSE THE INTERNET ANONYMOUSLY AND BYPASS CENSORSHIP

TOR

Tor[32] is used by political activists, whistleblowers, journalists, domestic violence survivors, and average people around the world who need to shield their identities as they read and write online.

It helps you hide your **IP address** and prevent browser fingerprinting, making it more difficult for online trackers and even governments to surveil you.

In countries where huge swaths of the Internet are blocked, people use Tor to **access the open, uncensored web**. Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content.

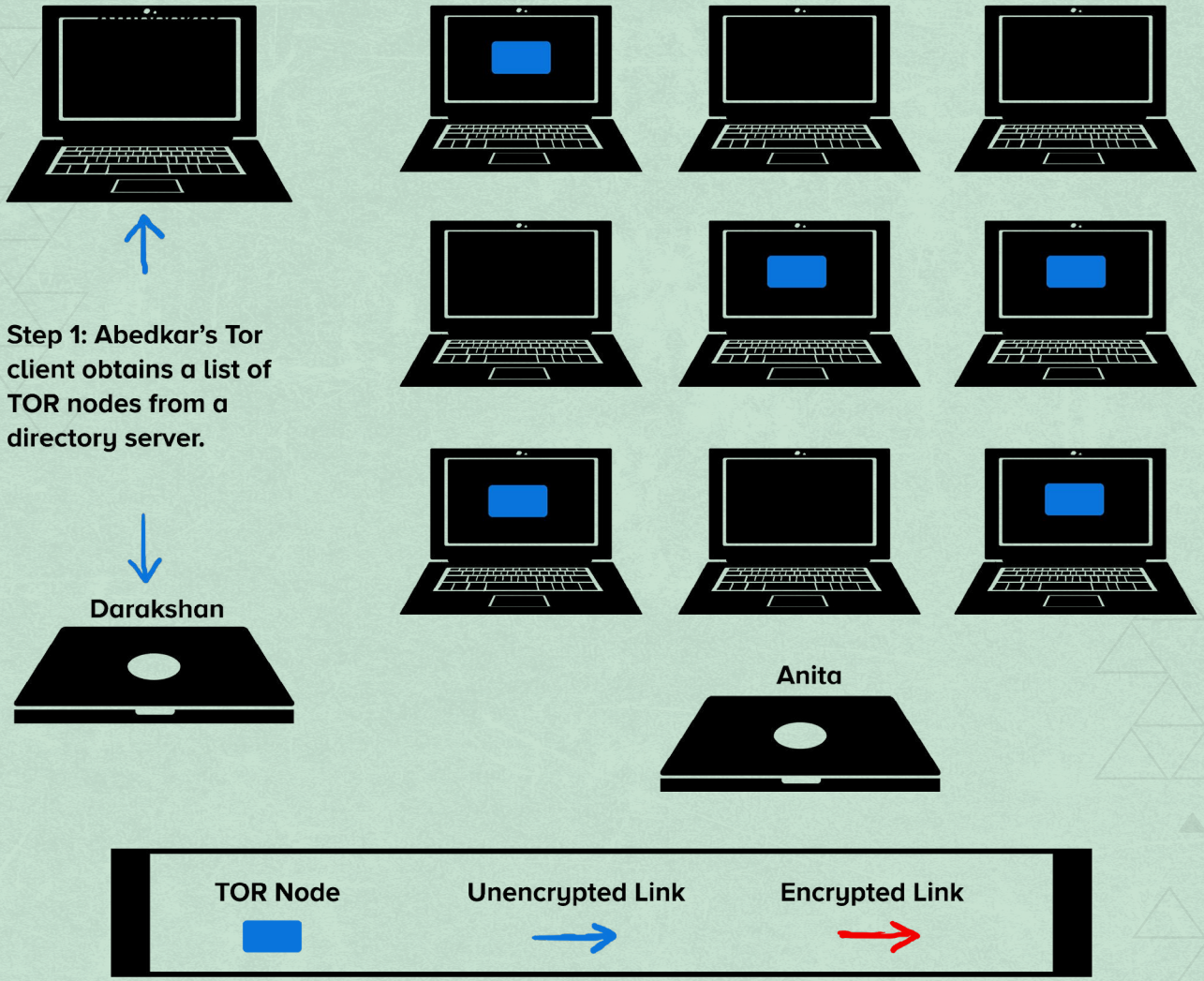
The range of people who use Tor are actually part of what makes it so secure. Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is, the more your anonymity will be protected.[33]

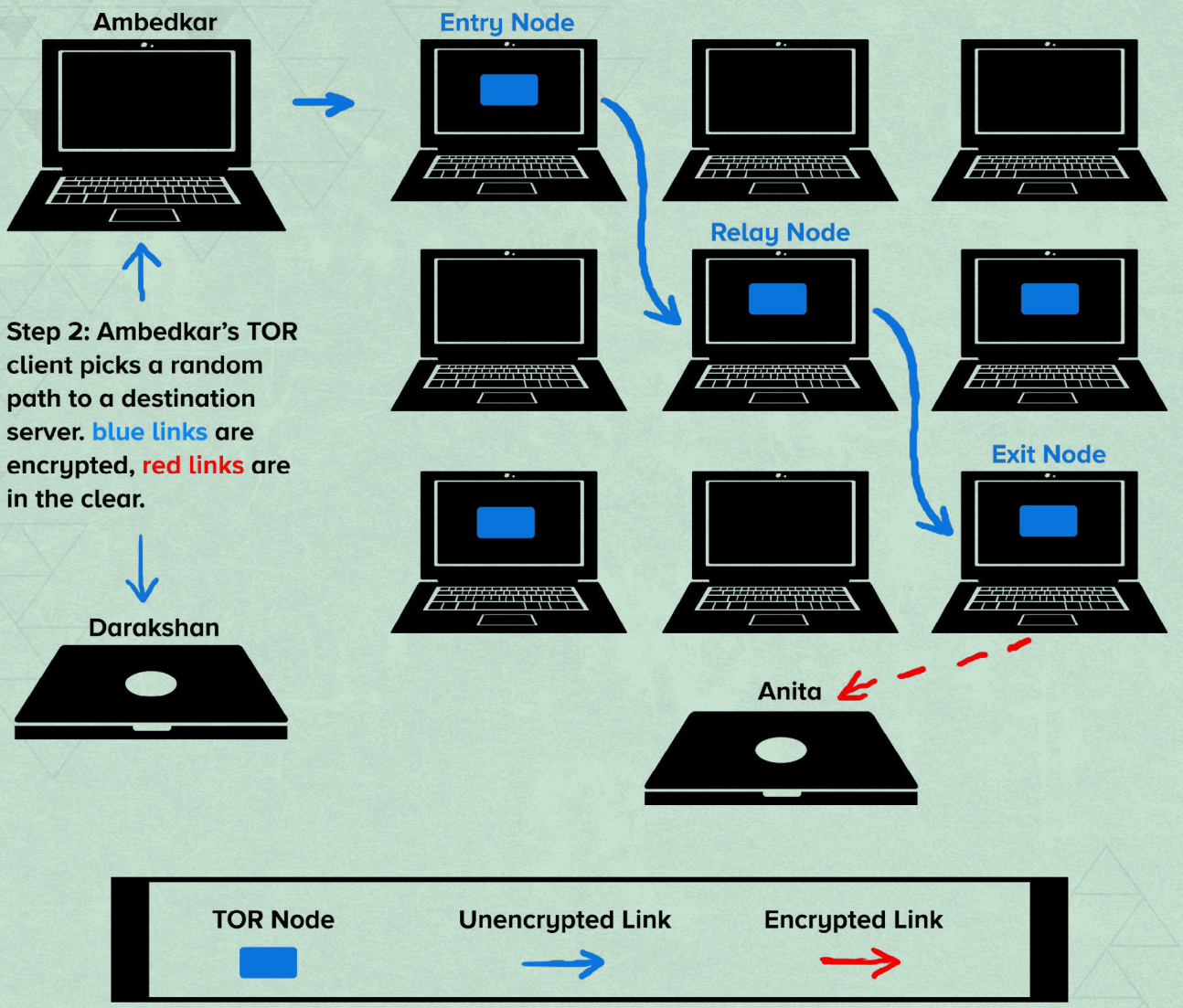
[32] https://www.eff.org/torchallenge/
[33] https://www.torproject.org/about/overview

There are lots of reasons you might want to use Tor. They can include:

- You have sensitive information and you don't want people to know that you are the person who sent it and where you are sending it from.
- You need to search politically sensitive content and you do not want to reveal your identity and geographic location when looking for such information.

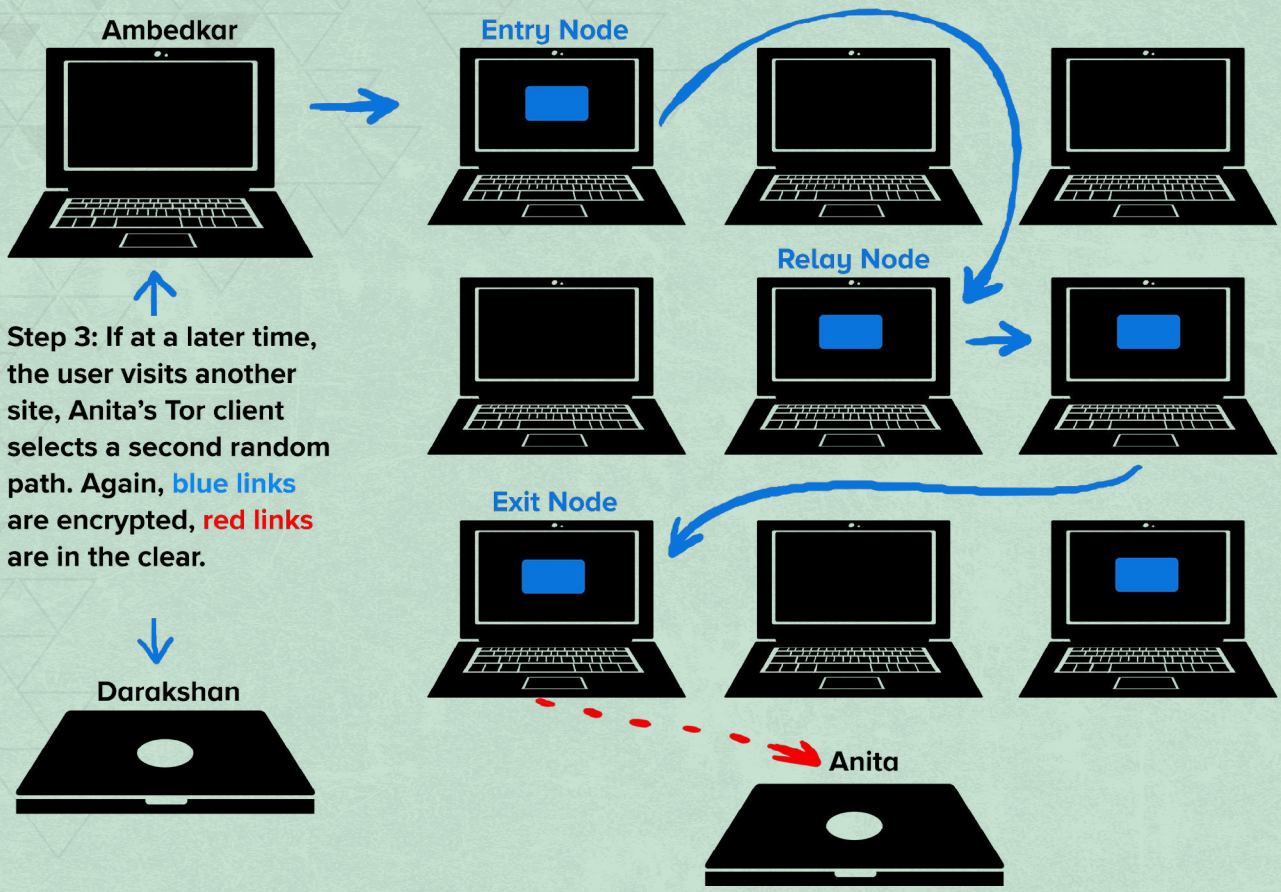
To better understand how Tor works below is a series of diagrams that wil help you understand the Tor process. In these diagrams our friend Ambedkar wants to send e-mails to his friend Anita.





In this next step Ambedkar's client now picks a random path through multiple Tor servers across the world. The first computer is the entry node, and the second computer is the relay node, and the third computer is the exit node. That node is the IP address that is seen by the websites you visit, which recognize the country of origin where the exit node is located.

What is important to know is that the path between Anita and the exit node is UNENCRYPTED so please make sure you use the https protocol between sites.



Step 3: If at a later time, the user visits another site, Anita's Tor client selects a second random path. Again, blue links are encrypted, red links are in the clear.

WARNING: Tor is only protecting the network access. If your computer is communicating with a final destination site that is not using HTTPS then the content sent by the final node through the intermediate Internet route to the destination server will be UNENCRYPTED! YOU MUST USE HTTPS TO REMAIN PROTECTED. So check your URL's and use HTTPS EVERYWHERE as your browser extension.

Tor is only as good as the more diverse communities use it. If you want to learn more about Tor or even join the Tor community please visit www.torproject.org

VIRTUAL PRIVATE NETWORKS (VPN)

Another option for securely accessing the internet is a Virtual Private Networks or VPN. VPN's allow you to connect to the internet via a server run by a VPN provider. All data traveling between your computer, phone or tablet, and this "VPN server" is securely encrypted. As a result of this setup, VPNs:

- Provide privacy by hiding your internet activity from your ISP and the government.
- Allow you to evade censorship by school, work, your ISP, or the government.
- Allow you to "geo-spoof" your location in order to access services unfairly denied to you based on your geographical location(or when you are on holiday.
- Protect you against hackers when using a public WiFi hotspot.
- Allow you to Peer to Peer download in safety.
- Keep in mind a VPN protects one's right to privacy on the internet by creating anonymity. This anonymity is crucial to guaranteeing that none of your data will be divulged without your consent.

HOW DOES IT WORK ?

Normally, when you connect to the internet you first connect to your Internet Service Provider (ISP), which then connects you to websites (or other internet resources). All your internet traffic passes through your ISP's servers, and can be viewed by your ISP.

When using VPN you connect to a server run by your VPN provider (a "VPN server") via an encrypted connection (sometimes referred to as a "VPN tunnel"). This means that all data traveling between your computer and the VPN server is encrypted so that only you and the VPN server can "see" it.

This setup has a number of important consequences:

1. YOUR ISP CANNOT KNOW WHAT YOU ARE UP TO ON THE INTERNET

It cannot see your data because it is encrypted. It cannot know which websites (etc.) you visit because all internet activity is routed through the VPN server. Your ISP can only see that you are connected to the VPN server.

2. YOU APPEAR TO ACCESS THE INTERNET FROM THE IP ADDRESS OF THE VPN SERVER

If the VPN server is located in a different country to you, then as far as the internet is concerned you are located in that country (most VPN services run servers located in many different countries). Anyone monitoring your internet activity from the internet will only be able to trace it back to the VPN server, so unless the VPN provider hands over your details (more on this later), your real IP address is hidden. This means that websites etc. cannot see your true IP address (just that of the server).

3. IT IS SAFE TO USE PUBLIC WIFI HOTSPOTS

Because the internet connection between your device and the VPN server is encrypted. Even if a hacker somehow manages to intercept your data, for example by tricking you into connecting to

an “evil twin” hotspot or packetsniffing your WiFi data, the data is safe because it is encrypted.

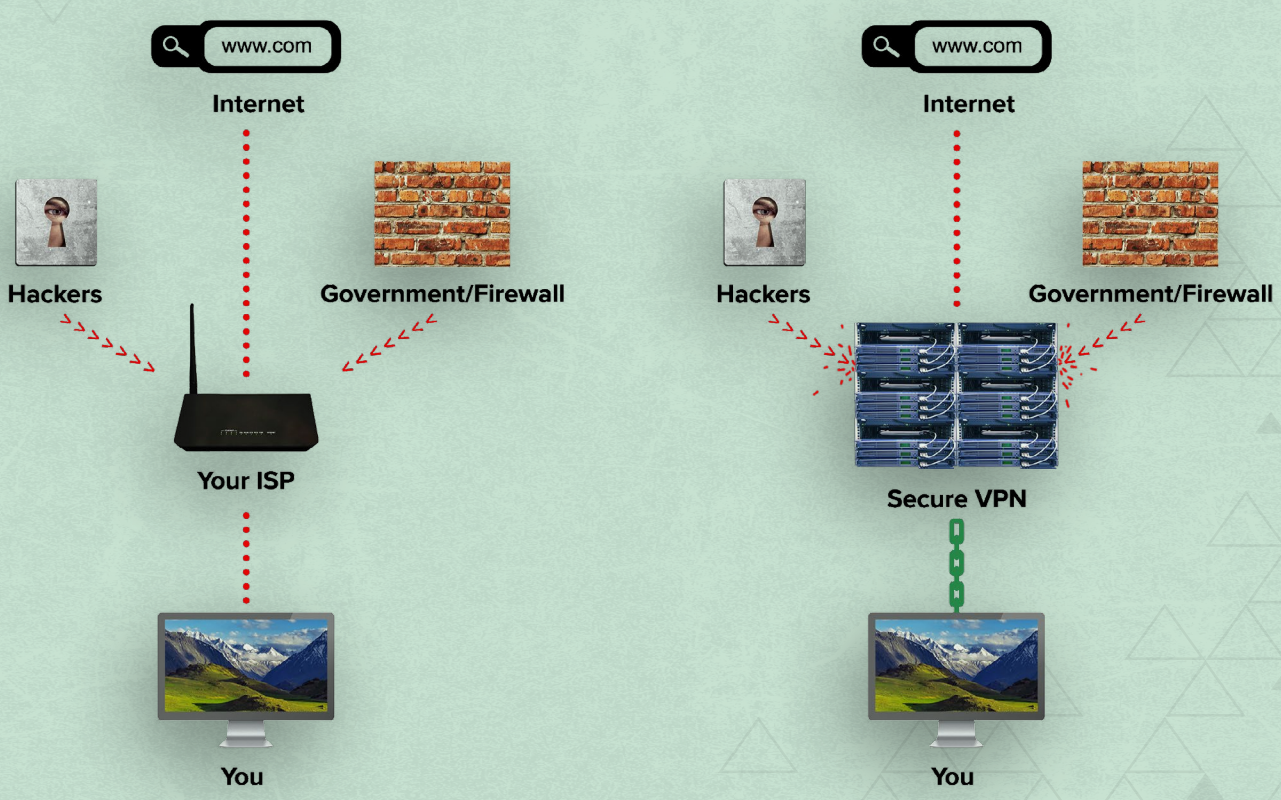
4. YOUR VPN PROVIDER CAN KNOW WHAT YOU ARE UP TO ON THE INTERNET

Your VPN protects your internet traffic from surveillance on the public network, but it does not protect your data from people on the private network you’re using.[34] This means whenever you are looking for a VPN, you want to see what their data sharing policies are and if they are dedicated to doing VPN’s or have only recently started. This can be an indicator to the expertise and seriousness of the service with regards to User privacy.

You are therefore shifting trust away from your ISP (which has no interest in, or commitment to, protecting your privacy) to your VPN provider who usually promises to protect your privacy. More privacy-minded VPN services mitigate this issue by employing various technical measures to know as little as they can about you. More on this later.

5. YOUR INTERNET WILL SLOW DOWN

Encrypting and decrypting data requires processing power. This also means that, technically, the stronger the encryption used, the slower your internet access. However, given the power of modern computers, this issue is relatively minor compared to the extra distance traveled by your data. Using VPN always introduces another leg to the journey that your data has to travel (i.e. to the VPN server), and thanks to the laws of physics, the further your data has to travel, the longer it takes.



[34] https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

If you connect to the VPN server located geographically nearby in order to access a website that is also located nearby, expect a 10% decrease in internet speed. If you connect to a server half way across the planet, you should expect a much greater decrease in speed.

We encourage you to always look through the privacy policies of all VPNs that you work with. Some VPN's we recommend include VyprVPN by Golden Frog. Not all VPNs are transparent about what they share about you and where. Vypr currently has a minimal amount of data stored about you and your usage and they also hold all servers in house. The downside of Vypr is that it is a paid service. You can find it here: https://www.goldenfrog.com/vyprvpn

TOR VS VPN

There are subtle, but important differences between using Tor and a VPN:

	TOR	VPN
ORGANIZATION	Tor is a network run by global volunteers	A VPN is usually run by a private company unless you are using your own activist VPN
RESILIENCY	Tor nodes are distributed and harder to shutdown	A VPN company can be a target for legal requests to shut down or divulge data. You will have to trust your VPN partner to have good business practices
SPEED	Traffic through Tor is going through several parties and usually has a significant slowdown	Traffic is going only through your VPN and is much faster than Tor
EXIT NODE IP ADDRESS	You cannot guarantee the exit node IP Address will be the same between requests and sessions	You can choose a fixed IP Address from which your traffic will originate from
END-TO-END ENCRYPTION	Tor has encryption between all of the nodes, but does not have guaranteed end-to-end encryption	All traffic between you and the exit node is encrypted
LOGGING	Nodes are usually configured not to log traffic	A VPN company may log your traffic without your knowledge or consent

In short, Tor is slower but offers more privacy, and a VPN is necessary when dealing with sites that will not open in Tor. In either case, always check for HTTPS or you will be voiding your secure network access.