5 Simple Steps to Increase Your Privacy Online (2019)

Privacy does not mean a lot in today's world. We have all searched up some item on google and then seen ads targeted to us based off of that search. Many have talked to friends on the phone about some product or item only to see ads targeted to them based on that discussion. This happens largely with social media site Instagram but they stand firmly behind the "coincidence" excuse.

Is true privacy lost? Maybe. However, there are ways for each person to increase their privacy on the internet in order to reduce the unethical practices occurring on everyone's data. Here is a list of simple steps to increase privacy on today's internet:

1. Use Privacy Oriented Browsers

Privacy oriented browsers are browsers who focus largely on user security and privacy. One example of this is the chromium-based Brave Browser which has a built-in ad and tracker blocker This blocker significantly increases user privacy in comparison to other browsers and it enables Brave to operate 2-8 times faster than competitors. Like most other browsers Brave has private browsing mode. Something that sets Brave apart is that you can open Tor windows which is a unique and really cool feature. These windows mask your IP address and prevent tracking from Internet Service Providers. Brave also has a reward system with their own cryptocurrency token however, for optimal privacy, I would advise against using this. One minor drawback to Brave is that some web pages will not load correctly due to the ad and tracker blocker.

Brave is available on Windows, Mac OS, Linux, Android and iOS.

Another example of a privacy oriented browser is Firefox. Mozilla doesn’t necessarily advertise Firefox as a privacy based browser however, they do a good job at making it one anyways. The main difference between the two browsers is that Firefox does not come with an ad blocker, you’ll have to download one such as AdBlock Plus. Firefox does have a built in content blocker which can block things such as trackers, cookies, cryptominers and fingerprints. This feature has two settings: standard and strict. I recommend using the strict setting because it blocks all of the things I mentioned above.

Ad-ons such as uBlock, HTTPS Everywhere and Decentraleyes which quickly make Firefox a privacy titan. Brave has these extensions as well but based on my experience they seem to work better on Firefox. Mozilla also makes it easy to configure settings such as enabling your browsing history to never be remembered, cookie deletion and various permission settings. The clear downside to Firefox is that you will have to do a lot of the work yourself but the upside is tremendous.

Firefox is available on Windows, Mac OS, Linux, Android and iOS.

Which to Choose?

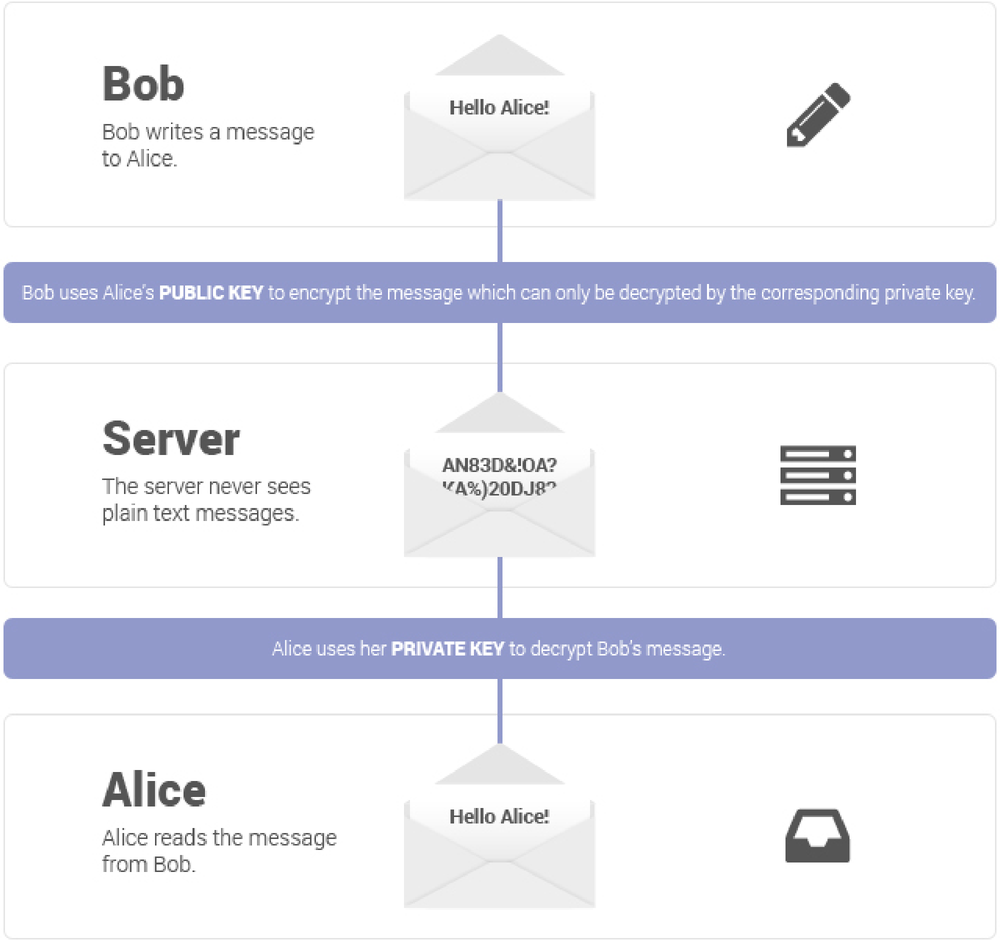
If you are willing to put in a substantial amount of time to optimize your privacy online, I would go with Firefox.

If you want something that just works out of the box and requires little to no configuration then I'd recommend Brave.

It is also worth noting that both mobile browsers are very well made. Brave Mobile & Firefox Focus are each labeled as privacy browsers and work as advertised. Personally, I use Firefox Focus.

2. Send Messages with End-to-End Encryption

End-to-End encryption, simply put, is the use of public and private keys in order to encrypt and decrypt messages solely among users. The application being used does not have access to these keys. Here is an infographic that explains it very nicely on ProtonMail's website:



Bob

Bob writes a message to Alice.

Bob uses Alice's **PUBLIC KEY** to encrypt the message which can only be decrypted by the corresponding private key.

Server

The server never sees plain text messages.

Alice uses her **PRIVATE KEY** to decrypt Bob's message.

Alice

Alice reads the message from Bob.

End-to-End encryption is becoming a standard in the industry and the odds are that you have already used or heard of a service that offers this feature. Here are some recommended services that utilize End-to-End encryption

Email

- ProtonMail
- CounterMail
- HushMail

All of the listed services are well known and well reviewed. Personally, I recommend ProtonMail because of its compatibility among various platforms and the quality of their application.

Messaging & Voice-Calling

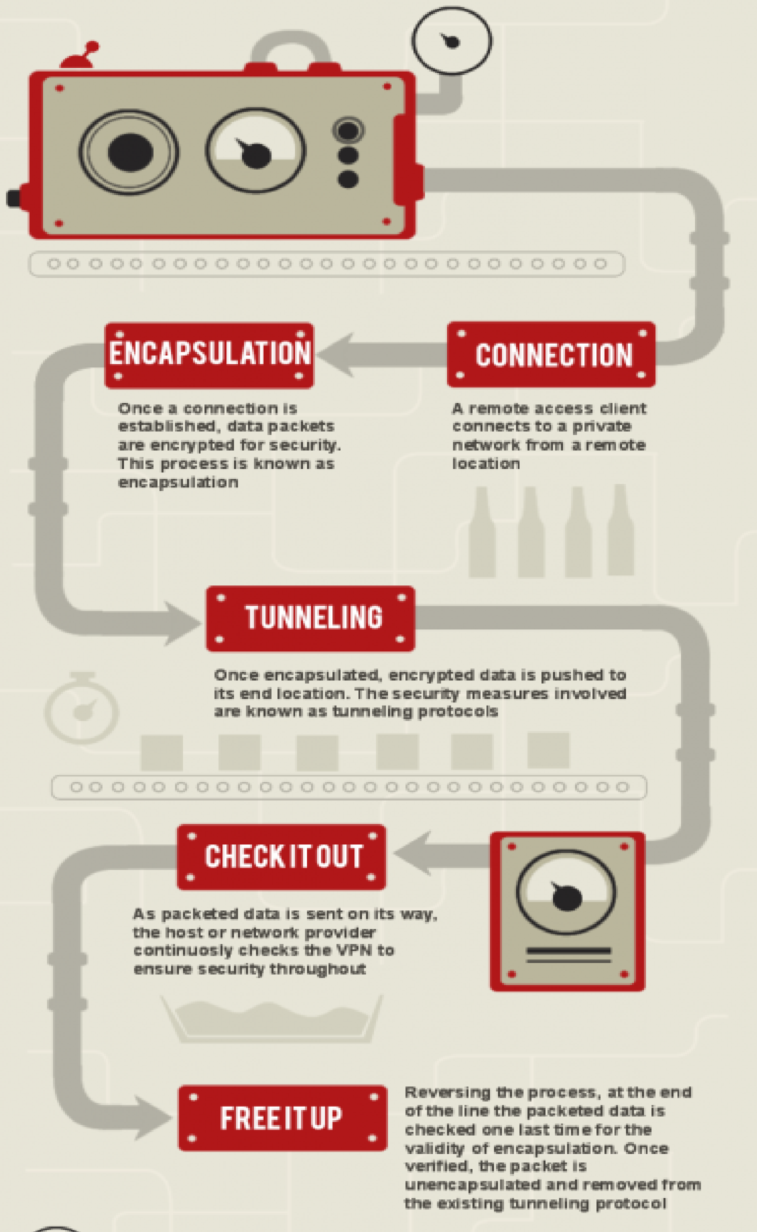
- WhatsApp
- Signal
- Telegram

Each of the applications listed above are valid choices for using an end-to-end encrypted communication system. Personally, I recommend WhatsApp because of its robust encryption and its popularity around the world. Signal is a good alternative and there was nothing wrong with my experience while using it. Telegram is one that I would use with caution because they DO NOT use end-to-end encryption by default. You will have to manually create a “secret chat”. Furthermore, encrypted messaging is not supported in group chats which makes Telegram significantly less secure in comparison to its competitors.

3. Use a Virtual Private Network (VPN)

A Virtual Private Network also known as a VPN, is a private network which allows users to connect to a server from usually a vast selection of countries. Once connected, you are able to browse the internet using this connection. This makes it seem like you are browsing from a certain location when in reality you are not.

Virtual Private Networks: How they Work



CONNECTION

A remote access client connects to a private network from a remote location

ENCAPSULATION

Once a connection is established, data packets are encrypted for security. This process is known as encapsulation

TUNNELING

Once encapsulated, encrypted data is pushed to its end location. The security measures involved are known as tunneling protocols

CHECK IT OUT

As packeted data is sent on its way, the host or network provider continuosly checks the VPN to ensure security throughout

FREE IT UP

Reversing the process, at the end of the line the packeted data is checked one last time for the validity of encapsulation. Once verified, the packet is unencapsulated and removed from the existing tunneling protocol

80%

Of all businesses currently utilize VPN for some segment of their remote access needs

60% - 67% average business cost savings on long distance data plans by utilizing VPN's

VPNs have many benefits and uses, here’s a few of them:

- Bypassing country browsing restrictions
- Streaming content only available to certain countries on services like Hulu and Netflix
- Protecting yourself when connected to public WiFi networks.
- Increasing general privacy

The current VPN market is a very saturated one. It is difficult to determine which ones are trustworthy and which ones are not. This is due to unethical marketing practices by big players in the market. Luckily enough someone created the site https://thatoneprivacysite.net/ which gives users the rundown on most VPNS and makes it easy for users to choose the appropriate VPN for their use case.

Choosing a VPN was a very long process for me. The only recommendations I will make are the following:

- NEVER use a free VPN
- Never use a VPN that has shared user information.
- Don’t use a VPN within the jurisdiction of the fourteen eyes
- Don’t subscribe to a VPN for over one year
- Don’t use a VPN that currently or has previously logged browsing data

Currently, I am trying out NordVPN for one month. The reason I chose Nord is because it checks all of the requirements I listed above. The only problem I have with NordVPN is that their advertising scheme is slightly unethical and many users complain about not being refunded money despite having been promised a 30-day money back guarentee. Additionally, many users claim that after the 30 day money back guarantee expires, their connection and browsing speed significantly decreases, which isn't a good look for Nord. However, despite all of this, I have been having a pretty good experience so far.

4. Pay with Cryptocurrencies

What are cryptocurrencies and why should I use them? Simply put, cryptocurrencies are a medium of exchange that allow people to transact without needing a third party. Cryptocurrencies enable users to conduct cheap (sometimes free) transactions, maintain privacy, and much more.

In fact, when I purchased my VPN subscription I did so with bitcoin. Here’s why:

The whole point of me using a VPN is to help maintain my privacy online. Therefore why would I attach my name, and payment information such as credit/debit card or pay-pal account to this privacy service? It defeats the purpose. With bitcoin however, I was able to purchase this VPN service without needing to share all of that data. It was as simply as scanning a barcode with my phone’s camera. I did need to provide an email address, but I felt comfortable enough using the end-to-end encryption provided by the ProtonMail service.

Many services today have decided to accept bitcoin and other cryptocurrencies as payment. For your reference, here's a list of some of them:

- Microsoft Store (Games, Movies, and Apps)
- Dish Satellite Television
- Expedia
- VPN services (NordVpn, ExpressVpn, TorGuard, AirVPN and more)
- Cloud Hosting (Vultr, Digital Ocean, and RamNode)
- NameCheap Domain Names
- NewEgg Hardware

The list goes on. Cryptocurrencies are still in a period of growth and new retailers decide to accept them as payment every single day.

More Privacy with Cryptocurrencies

Unlike bitcoin, some cryptocurrencies who are fully focused on solving the issue of privacy on the internet. These include

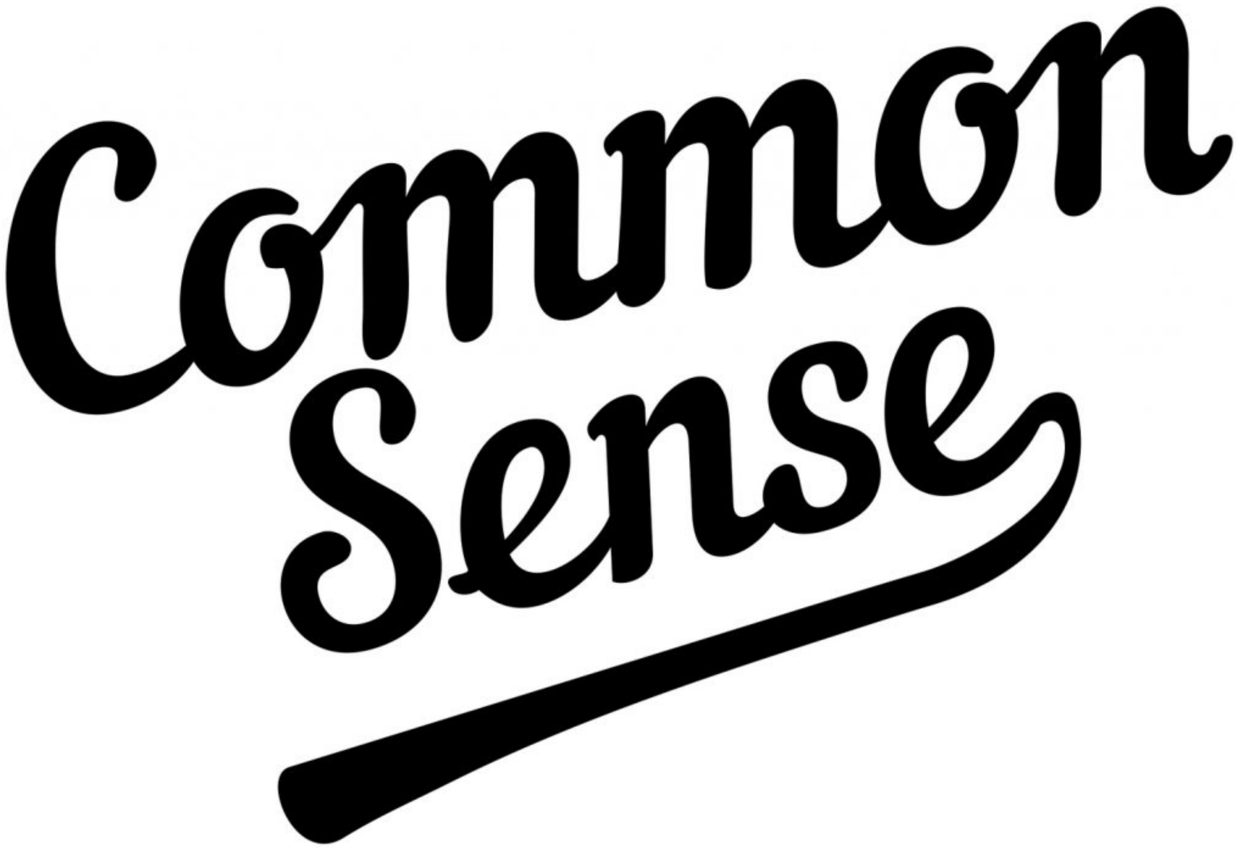
- Monero
- Zcash
- Dash
- Ycash

Which Should You Use?

If you don’t need 100% privacy and you want to use the most credible cryptocurrency possible then I’d recommend using Bitcoin.

If you need to maximize your privacy and you are willing to decrease the amount of available retailers then I’d recommend using Monero.

5. Exercise Common Sense



Common sense does not seem to be all that common in today's world. Everyone makes bad judgement calls but it should never become an acceptable habit, especially online.

Listen, I'm not going to sugar coat it for you. The internet can be a very dangerous place. Reusing passwords, entering your email and passwords onto untrustworthy websites, purchasing off of untrustworthy websites, are some of the most common mistakes people make on the internet and many pay the price for it.

Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds throughout 2019. It's also predicted that cyber crime will cost the world in excess of $6 trillion annually by 2021.

These numbers could significantly decrease if people follow these common sense "internet rules":

- Do not reuse passwords
- Separate your professional and social life (different emails and accounts)
- Check to make sure the URL you're visiting is the correct one
- Do not believe everything written in messages sent to you (Seriously, scammers are crafty.)

There's much more that can be added to that list but you already know that. We must not forget common sense just because we are interacting with people through screens.

Final Thoughts

Above I’ve listed five simple steps to increase your privacy online. These steps will increase your privacy and comfort while browsing the internet. If these steps haven’t quenched your thirst for true privacy, stay tuned for my post on Advanced Steps to Increase Privacy Online.