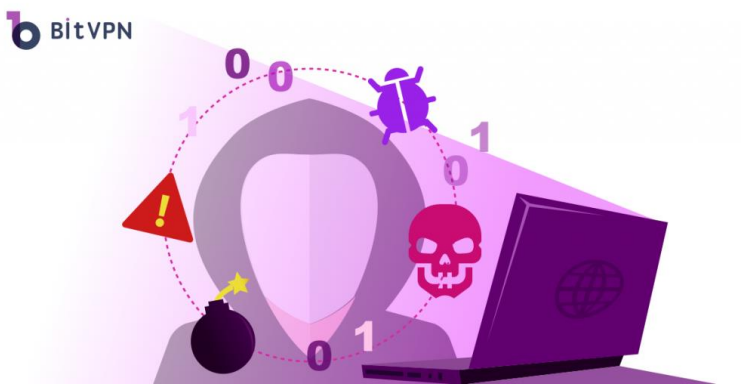
How Should You Encrypt Your Internet Traffic in a Decentralized Way?

by Edward Laba

Everyone should encrypt their internet traffic but not everyone knows that.

As you use the Internet, your online tracking isn't what can be seen only by you. Internet fraudsters and third-party organizations are keeping tabs on your internet activity. Your Internet activities are always monitored by those people who have been striving to get more profits. Therefore, it would be weird and dangerous not to get some protection when you use the Internet for anything.

There are multiple ways out there that can be used to protect your Internet connection from snooping eyes. Well, what this article focuses on is those with low cost and high convenience. Let's go for them.



Something You Should Know About Internet Traffic Encryption

As you try to understand an issue, it's the best idea to start by understanding it from a literate range.

What is Internet Traffic and How does It Work?

Based on the introduction by Wikipedia, Internet traffic is the flow of data within the entire Internet, or in certain network links of its constituent networks. Common measurements of traffic are total volume, in units of multiples of the byte, or as transmission rates in bytes per certain time units.

Now that "traffic" is used in this phrase, it's sensitive to understand internet traffic from the perspective of traffic. The traffic we usually refer to indicates the number of vehicles going on the street. Locations play roles as websites on the internet. Internet traffic isn't evenly

distributed on the internet, which is the same as in real traffic. You know, I hate Sunday Walmart since I have to spend more time looking for a parking lot.

Time often arouses the uneven distribution of internet traffic as well. It's so easy to understand that since traffic jam isn't a new term. Now, it's not difficult to understand internet traffic pressure during COVID-19 pandemic that slows down Netflix streaming and YouTube. After all, a sudden high number of people are forced to stay at home and the Internet can be their only true friend with whom social distancing can be totally ignored.

Internet Traffic vs IP Traffic, How Different are They?

Internet traffic indicates the range of the whole internet while IP traffic indicates that of a certain IP address. An IP address clarifies where on earth either a website stays in the Internet world or a device (also individual, you) are sending out a searching request.

What is Encryption?

Encryption is a method to protect information by using secret keys to decode. The keys are used to encrypt data and transform data into random strings that share NO similarities with original strings. Anyone who wants to check original data can never make it unless a decryption key is obtained. Otherwise, what can be seen by them is just garbled that can never be understood.

Once your internet traffic is encrypted, even if hackers, your Internet Service Provider (ISP), local government, or any third-party organization that is interested in your browsing habits or tries to gain illegitimate profits from you won't have access to your real data you just transmit and receive between your device and the Internet.

Dangerous Internet! Why Should You Encrypt Internet Traffic?

For your CYBERSECURITY

The first and most obvious reason for encrypting your internet traffic is SAFETY. You might not know this, but as long as you are opening tabs and using services from large corporations, your browsing patterns and information are being tracked and recorded. That personal data could end up in the hands of government bodies, ad campaign runners, or even scammers.

For your PRIVACY

The second reason is privacy. Even if your personal data does not end up as part of some ad algorithm for entrepreneurs, it can still feel very uncomfortable to have your personalized searches scrutinized by any person who happens to pick up your phone. Encrypting your internet traffic covers you on all fronts and prevents unexpected leaks from ever happening.

To stay away from HACKERS

Never say you'll never be hackers' target just because you're neither a celebrity nor government VIPs.

Whenever there are computers, there will be hackers around, all kinds of. Up to now, the internet is still the most valuable tool to make money as far as hackers are concerned. Some hackers monitor internet traffic by joining unpublic WiFis so that they can get valuable data such as password and credit card information. If encryption fails to be done on internet traffic, all your personal data will fall into the reach of hackers easily. Worse still, you will possibly keep unaware during the whole process. That would be so bad and late.

Remember, hackers, keep constantly refreshing their capability to get access to your data like phishing emails, Bluetooth hacking, pharming attacks, etc. while you still keep the same way when using the Internet and you depend on it more and more. How should you think ahead of them instead of trying to follow them?

To prohibit from being monitored by ISP

Your internet costs a lot. It is charged by your ISP. Behind your screen, ISP does a lot of things based on your internet service and activities to increase their profits. For example, your ISP may monitor your network traffic data to throttle when necessary. In addition, your ISP may sell your online data to business parties who then release commercials that are "fit" for you. Coeus, one of my friends, once bought a set of diapers because he'd like to visit her sister and her newborn. In the next days after his order completion, he had received tons of spam ads about diapers. Does Coeus need more diapers? Of course not. Nevertheless, just once purchase brought forward huge callouts. That all derive from the summary about your browsing habits collected by ISP. Besides, ISP also sells your data to the government for political causes.

How to Encrypt Your Internet Connection?

Encrypting your internet traffic is not necessarily an overly complex or expensive process. You can browse safely and securely by tweaking certain settings or exploiting unique features you are not aware of already. Listed below are a couple of the most common ways of encrypting your internet traffic at a low cost.

Encrypt your Wi-Fi network

This is one of the easiest ways how to secure your internet traffic. Once you set a password that you are comfortable with, you have officially encrypted your network traffic. The easiest way to tell if a network is encrypted is the padlock icon that is usually present beside the Wi-Fi signal. There are numerous types of wireless encryption protocols you can use. The most common are WEP, WPA, and WPA2.

WPA2 encryption is the updated version of the WPA security protocol. WPA2 encryption is currently the most secure type of wireless encryption protocol available on the internet today. It adds the Counter Mode Cipher Block Chiang Message Authentication Code Protocol onto the already existing layer of security and makes it difficult for someone to break through and access your data. When choosing an encryption security protocol, it is recommended that you make use of WPA2 encryption.

You can set up the encryption protocol on your Wi-Fi router easily. Some routers require a more complicated process, but most home routers only require you to log in to your router, enable WPA2 encryption, and set a password you are comfortable with.

Use a VPN

Using a VPN or Virtual Private Network to encrypt your internet traffic is one of the most popular low-paid avenues of protecting your personalized browsing data. VPNs secure your personal data by redirecting your connection through servers all around the world. In basic terms, VPNs provide secure encrypted tunnels for your internet connection to pass through. Usually, VPNs are provided by private internet security companies. Upon payment and registration, they will walk you the process of securing your internet access and will encrypt it as long as you choose to pay for their services.

Use HTTPS

VPNs and encrypted routers are great, but if you cannot afford that and you still want an extra layer of security, you should consider using HTTPS instead of HTTP. Hypertext Transfer Protocol Secure is a more secure version of HTTP used popularly on the internet. While it cannot ensure that your data won't be recorded and used by the organization or parties you are reaching out to over the internet, it can ensure that your data does not leak in transit. An HTTPs connection ensures bidirectional encrypted communication. This means that the website or entity you are communicating with has signed a digital certificate proving that they are legitimate. If a website does not have an HTTPS certificate and asks for payment for a service, they are most likely not legitimate.

This method of encryption won't completely protect your data, but it will prevent it from falling into the wrong hands while you browse. It is recommended that you use a browser extension like HTTPS everywhere to help you always load a site with HTTPS encryption.

Use a Tor browser

A Tor browser is an internet browser that offers complete anonymity while browsing on the internet. Unlike simple browser functions like incognito or private tabs that wipe your history alone, this type of browser leaves no data whatsoever. Your location, Ip address, cookies, and everything else will remain a complete mystery with this type of browser.

A tor browser encrypts your internet access by connecting you at random to a public node, bouncing the signal through another random middle node, and finally exiting at yet another node. The three layers of protection tor provide are often referred to as the onion protocol. Tor switches out your IP address numerous times during the encryption process, and in most cases, it will spit out location information from halfway across the world. Tor browsers are best coupled with other secure search engines like Bing, Duckduckgo, Privatelee, and searX.

It's optimal to use a Tor browser together with a VPN although a Tor browser is different from a VPN in many aspects. However, there's one common goal that is to protect your online security and privacy.

Encrypted messages

Encrypted messages are messages that cannot be read or access without some sort of password or clearance. Encrypted messages don't technically encrypt your internet access, but they can keep conversations and data private. There are tons of encrypted messaging platforms on the internet; you can use to convey your messages privately. Apps like iMessage, Telegram, and Threema are popular encrypted messaging platforms you can try if you want to communicate with someone discreetly.