5 ways to encrypt Internet traffic

Encryption is the process of converting data so that it cannot be read by anyone without the corresponding decryption key. In other words, it's a great way to prevent unauthorized access and increase security.

But is it possible to secure your Internet connection with encryption? The answer is yes, although this requires a multifaceted approach. Here are 5 ways to encrypt your Internet traffic.

1. Use private browsing

Your browser is your main gateway to the World Wide Web. If your browser doesn't protect you from being tracked, anything you do to improve your security won't make much of a difference.

Tor Browser is arguably the only truly private browser available today. Unlike other similar software, Tor redirects your traffic through at least b3 relay and encrypts it at every step. Commonly used to access the dark web, it is an indispensable security tool used by whistleblowers, political activists and reporters around the world. If you want to encrypt your traffic and protect yourself, you really can't find a better choice than Tor.

However, there's one big problem with this browser: It's too slow for everyday use. One solution is to only use it for certain sensitive tasks when protecting your privacy is imperative. In other cases, you can use a browser like Brave or Firefox. To be clear, neither Brave nor Firefox encrypt your traffic like Tor Browser, but they offer much greater privacy and tracking protection than browsers like Chrome or Microsoft Edge.

2. Use VPN

The debate is still unclear about whether and how one should use a virtual private network (VPN) with Tor Browser. However, you should definitely use a VPN with any other browser. In general, using a VPN is a good idea if you want to protect your privacy and make it harder for others to track your online activities.

The problem is that there are many VPN providers today but only a few offer software that actually does what they need. When choosing a VPN, make sure it has strong encryption and a strict no-logs policy, DNS leak protections, a kill switch function, and good performance. There are a few different ways to test a VPN's encryption capabilities, so make sure you test thoroughly after choosing a VPN.

With a VPN, you can encrypt your traffic easily and at low cost or even for free. But remember that you should do this on all devices, not just on your computer. If you are new to this concept, know that there are a few things you need to pay attention to when choosing a VPN service.

3. Use an encrypted messaging app

A secure browser and a good VPN service will go a long way in protecting you, but you need to cover all the bases. You can have the most reliable VPN in the world, but if you use an unencrypted messaging app, you're still at risk. Other than that, there's really no downside to using secure messaging apps.

And what you need is a messaging app with end-to-end encryption. In other words, the software ensures that only you and the recipient can read the messages you exchange. There are several popular encrypted messaging

apps on the market, but Signal is probably the best choice because of its reputation and strong focus on user privacy.

Telegram is another good choice, especially if you're looking for an app with social features. And if the people you communicate with via text don't use these apps, there's always WhatsApp. It may be owned by Meta, but it has end-to-end encryption and is certainly more secure than many other mainstream messaging apps.

4. Switch to an encrypted email provider

What do Google, Microsoft and Yahoo know about you? It's probably a lot, and if you use these providers' email services, they've collected an incredible amount of data from you. When you use an email provider owned by one of these companies, you're not only generating profits for Big Tech, but you're also putting yourself at risk. Here's why you should consider switching to an encrypted email service.

Encrypted email services outperform Gmail and similar products in almost every way. They use strong encryption, apply advanced security measures to prevent unauthorized access, and do not rely on collecting data from users. The only problem is that you may have to pay to use more advanced features (e.g., more storage, more email addresses).

With that said, choosing an encrypted email provider if you've never used one can be a bit daunting. Pay attention to some key features, such as what encryption algorithms they use and whether they store user logs. ProtonMail, TutaNota and Mailfence, to name a few, all have excellent reputations.

5. Invest in encrypted cloud storage

If you want to encrypt your Internet traffic, you can't ignore file storage. Especially in this day and age, when many of us rely on the cloud to store personal and important data.

To protect your privacy, look for cloud storage providers that use end-to-end encryption and maintain strong security measures to keep their customers happy. There are a lot of options, so choosing the right cloud storage for your needs can seem a bit daunting. For example, Icedrive, pCloud, Tresorit and Proton Drive are all safe and reliable.

It should be noted that it is very difficult to find a free encrypted cloud storage provider. This is understandable because the security and infrastructure required to provide this service comes with significant costs. However, it's better to pay with your money than with your data - you definitely want your data to be secure and encrypted.