About Privacy on the Internet

Description

About the “security ” of ProtonMail Swiss email : https://restoreprivacy.com/protonmail-data-requests-user-logs/

The company is said to have received about 7,000 requests to disclose user data in 2022. Of these, about 6,000 were satisfied.

Briefly about ‘privacy’ on the internet:

1. E-mails:

Unless self-hosted, no E-mail service, no matter what they claim, is private in any way. E-mail was never designed to be private. Even when self-hosted many vulnerabilities exist. I’ve long discussed that ProtonMail is likely a honeypot. Now, I don’t have evidence to that, but some of the claims they make simply aren’t true. It’s highly suspicious that ProtonMail’s website lets you access it through an Onion site, but redirects you to a standard one without notification when setting up an account. So if you’re SBU and are planning a terrorist attack, don’t use E-mail.

We don’t have access to your emails:

They do, no country’s authorities would let a service run if they didn’t. A logical question also arises, how did you open those 6,000 email accounts then? Even for simple security reasons, they definitely have access to your account and thinking otherwise is naive at best.

We don’t log your IP address:

That’s impossible. In order for two accounts to communicate, an IP has to be logged and saved. You can easily check this using programmes such as WireShark (comes pre-installed with some Linux distributions).

We don’t reveal your information:

That’s illegal when ordered to do. Your 5.99$ per month won’t save you. Case has been noted when an email was revealed to police simply because a teenager missed classes. Again, this is naive to believe.

1. VPNs

VPNs are glorified proxy servers, which translates to “someone else’s computer”. Their claims too are often simply not true.

We don’t log your IP address:

Again, impossible.

Military grade encryption:

While true, this isn’t anything special. The HTTPS encryption has been in use for years and you’re likely using it right now to read this.

Hide your traffic:

Not true. Even a simple internet tool will reveal you are using a VPN and tools like WireShark (also free) will reveal every single “handshake” your computer makes, including servers you connect to, regardless of whether or not you use a VPN. Furthermore, the vast majority of VPN providers are owned by a single advertising company. What better way to track someone’s internet traffic than to channel it through a single server… If you need a proxy server, just use a proxy server.

Anonymity:

Tell me, how am I anonymous if I enter my credit card details when purchasing your service…?

1. Conclusion

All tools are useful in certain scenarios, but complete internet anonymity/privacy is an excruciating process that isn’t worth it for most people and, is practically impossible, unless you never want to use your computer or jump through so many hoops you’ll regret having one. Don’t believe claims of companies that are currently riding the privacy train. At best it’s a way to get your money in exchange for nothing, at worst it’s a honeypot.

#Source