

Anonymity, Security, and Privacy on the Internet

Our lives are increasingly dependent on the internet and the data we associate with our identities. **Many of us still approach this situation naively**, without a clear understanding of what their online identity represents, the data connected to it, or the risks involved.

Use the information found here at your own risk: **my advice and suggestions should never replace your understanding of the issues** and a strategy tailored to your particular situation. I believe them to be relevant, but **applying them without understanding could lead to more insecurity** than anything else.

This page aims to provide a simplified overview of the main issues, tools to establish a healthy baseline of ASP ¹⁾, and directions to explore further, based on a few [fundamental principles](#).



This is not an exhaustive guide guaranteeing security and anonymity on the Internet²⁾. These are simply some tools and tips for using them, which help to move towards these goals.



Improving security, privacy, and anonymity sometimes has significant consequences on browsing habits:

- **zone 1**: Easy, negligible impact, everyone should do this
- **zone 2**: Noticeable impact, new habits to adopt, loss of secondary functionality
- **zone 3**: Difficult, significantly transforms and/or limits your use of the internet

Risks and Challenges

Even without anything to hide, everyone is affected by issues of online security, anonymity, and privacy.

Whether they realize it or not, people face several serious challenges in this area. Here are some of the most important:

- **Protection of personal information**: The information you share online, intentionally or not, is exploited for profit and may be used abusively. This includes data collected about you unknowingly

during internet browsing, such as your IP address, browsing habits, people you communicate with...

- **Cybercrime risks:** Phishing, malware, ransomware, and other forms of cybercrime are serious threats. Poor online security can lead to personal data theft, including financial information,
- **Surveillance and tracking:** Governments, corporations, and even cybercriminals can monitor your online activity for various reasons, but probably none that you would approve of,
- **Data-based discrimination:** Companies sometimes use the data collected online to make decisions that may affect you, like insurance rates, loans, etc. These decisions can sometimes be discriminatory,
- **Intrusive targeted advertising and profiling:** Based on your online behavior, companies can target specific ads at you. This can be perceived as intrusive and may also lead to impulsive consumption decisions.

Being aware of these challenges helps you better protect yourself. Beyond these generalities, some individuals, particularly activists, are more likely to be directly targeted by surveillance, profiling, or online attacks from hostile entities, primarily governments.

Of course, not all situations involve the same risks and countermeasures. The following sections of this guide provide general advice for improving security and anonymity, but we will also see **some strategies available for those who need a higher level of security and anonymity**, and ways to go further.

Accessing the Internet

As soon as you're connected to the internet, you interact with third parties and risk exposing private data against your will.

https (SSL)

zone 1

SSL³⁾ is an encryption protocol used to secure communications between a client and a server. If you want to know more, [the Wikipedia page](#) is a good starting point.



In practice, you mainly use it with the **https** protocol, which encrypts the connection between the user's browser and the website they have requested, meaning that **all information transmitted between the user and the site is encrypted and can only be read by them.**

This is the basic level of security on the internet, and you should ensure you only browse secure https sites, and especially, **never submit personal information or passwords on a site that does not use it.**

Modern browsers have configuration options or extensions that allow you to [automate secure https connections](#).

VPN

zone 2



VPNs can be useful, if you understand how to use them. They are **by no means turnkey solutions guaranteeing ASP**, contrary to what their sellers claim.

VPNs⁴⁾ are marketed at every corner. This tool, potentially very useful for security, is often misunderstood.

It creates a private tunnel between your computer and the VPN server. All or part of your internet traffic is routed through this tunnel, meaning that no one on your local network or ISP can see what you're doing online, and the websites you visit see the VPN server's IP address instead of yours. The traffic in this tunnel is encrypted. **The VPN server operator can see everything that passes through this tunnel.**



This technology has various uses. In a context where you are connecting to a remote private network (e.g., your employer's network), and sharing private data between you and this network, your organization controls the VPN server, and this is undoubtedly the most secure solution.

However, in the context of your personal online security and anonymity, we're generally not talking about this usage, but rather the service provided by companies selling it as a turnkey and complete solution for security and anonymity. **These promises are mostly marketing, and while such VPNs have legitimate uses, it's important to understand the relevant cases and their limitations.**

When using a public VPN:

- Your **internet provider**, or the operator of the **public or private Wi-Fi** you're connecting to will not be able to know what you're viewing online or read your passwords and other private data. But this is also true with simple https encryption, and a VPN offers only marginal security from this perspective,
- **Your IP will be hidden from the websites you visit**, and you will appear to be browsing from the IP of the VPN server you're connected to,
- As such, **a VPN can help bypass geographical restrictions** on some services⁵⁾,

- However, **you must have a great deal of trust in your VPN provider**. They potentially have access to all your transactions and data, and **can hand them over to authorities or sell them**. Most VPNs, of course, swear they don't do this or even claim not to keep logs, but several have been caught lying about it,
- You'll also need to deal with minor inconveniences: your geolocation will be incorrect, and your connection will be slower⁶⁾.

Choosing a trustworthy provider

I personally use [ProtonVPN](#) for the rare cases where a VPN seems like the right tool. It's a paid service linked to Proton Mail, but **audited, doesn't require personal information to subscribe, is composed of free software, and seems to take security seriously**. Don't take this as a guarantee. It's simply the provider of my emails, and the VPN is included ([Mullvad](#) would be my first choice if this service were important to me, and [IVPN](#) also ranks well).



In general, **avoid free services like the plague**, which will probably be financed by selling your data. However, for occasional use, and if you can accept a reduced speed (it's slow!), **Riseup is a militant project**, offering several secure and privacy-respecting services, including a free VPN, without collecting any information about you.

¹⁾
Anonymity, Security, and Privacy: this is not a common acronym, but it will save me from repeating myself throughout this page

²⁾
The internet is not limited to the web and the http protocol: Email, torrent, ftp, DNS... usage and protocols are diverse, and all must be considered from a security and privacy standpoint

³⁾
Secure Sockets Layer

⁴⁾
Virtual Private Networks

⁵⁾
Note that many VPNs are blacklisted by many streaming services, if that's your goal

⁶⁾
More or less, depending on the provider you use

From:
<http://2027a.net/> - /dev/null

Permanent link:
http://2027a.net/tech/privacy_and_security_online?rev=1728149780

Last update: **2024/10/05**

