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 Internet[2)]. 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

SSL[3] 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.

VPNs[4] 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 services[5],

- 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 slower[6)].

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.

TOR network

zone 3

TOR is a protocol that allows for a very high level of ASP, but it comes with significant constraints. It is not a solution for everyday use or a typical threat model.

TOR, also known as the *onion network*, routes your internet traffic through several servers (or "nodes") before it reaches its final destination. This makes it much more difficult, if not practically impossible, for anyone to identify the source of the traffic. You may have heard of it in the context of the *dark web*, for which TOR is one of the main protocols. The term is clearly intended to demonize anonymous and secure internet usage, but the phenomenon it describes—parts of the internet inaccessible to both private and state surveillance—does indeed exist.

This solution is by far the most secure and anonymous for connecting to the internet. However, it comes with significant constraints:

- You can expect **a substantial slowdown in your connection**,
- Some sites and services blacklist TOR exit nodes, either to prevent anonymity or avoid abuse,
- Although TOR is highly secure by default, **it's easy to make a mistake that will ruin all your efforts** for anonymity, for instance, if you log into a service that holds information about you (your bank, your email, Google, Facebook...),
- Besides human errors, there are attacks that TOR does not protect against, such as traffic correlation attacks. These attacks are, however, rare, particularly difficult to carry out, and require uncommon resources.

In short, TOR is the most technically effective solution for security and anonymity but requires a good understanding of the underlying issues to use it safely. I may create a dedicated page on TOR in the future, but for now, it's enough to know that it exists, and it's not suited for everyday situations.

Choosing a Browser

The browser is the window through which you access the internet. Google Chrome, Safari, Firefox... obviously, **it is a crucial piece in our approach**.

Most people use either the default browser on their system, such as **Edge** or **Safari**, or **Chrome**, Google's browser.

These three browsers are proprietary software, difficult to audit, and they collect private data about you without any way to stop it. Anyone concerned with ASP should avoid them entirely[7].

Brave

zone 1

Brave is an open-source browser based on Chromium, the open-source foundation of Google Chrome, and provides an excellent default level of ASP.

If you're looking for an easy replacement for Chrome, Edge, or Safari without worrying about configuration, it's probably the best solution.

However, there are reasons you might not want to choose Brave, starting with its integration of a cryptocurrency system[8]. Some users prefer to avoid Chromium-based solutions, so as not to contribute to the near-monopoly of WebKit[9] on the web, much like the days of Internet Explorer.

Firefox

zone 2

Firefox is the quintessential open-source browser. Less secure and collecting more data by default than Brave, it can easily be configured to achieve as good or even better levels of protection.

Firefox also has the advantage of promoting web diversity and interoperability, as it is based on a different engine than Chromium/WebKit.

Its default configuration is insufficient (from an ASP perspective). Here are some configuration tips to optimize your situation, along with a few useful extensions for this purpose.

I place Firefox in zone 2 because it requires a bit more configuration than Brave, and switching to a different rendering engine will likely have some visual impacts on your usual websites. Still, it's a very accessible option.

Specialized Browsers

zone 3

Several other options exist: specialized browsers whose main goal is to provide a particularly secure and anonymous experience.

- **TOR Browser**: This is a [10] browser preconfigured for maximum security and anonymity, with all traffic routed through the TOR network. Extremely secure and extremely restrictive at the same time, it makes it easier to access the TOR network for situations that require it.
- **Mullvad Browser**: Developed jointly by the TOR project and Mullvad, a VPN provider[11], it's essentially TOR Browser without TOR.
- **Hardened Firefox, Arkenfox, Librewolf…** Several projects aim to provide more secure and anonymous versions of Firefox. They all have different priorities and methods, but they are projects worth exploring if Brave or Firefox doesn't suit you.

Other Browsers

Many other lesser-known browsers exist, both open-source and proprietary. Some are, of course, legitimate tools, so don't hesitate to read about them. However, beware of two proprietary browsers:

- Opera should be avoided like the plague. It's proprietary, poorly configurable, and full of telemetry.
- Vivaldi is a security-oriented browser and quite respectable. However, since its source code is

private, you must trust it blindly, which is contrary to our basic principles.

Authenticating and Protecting Your Identity

One of the main security challenges we face online is protecting our identity. If it hasn't happened to you personally, you've likely witnessed Facebook accounts being hacked, with the owner losing control, or passwords being stolen from a compromised site and used elsewhere to access other accounts.

The problem is complex, but good security practices can dramatically reduce the risk of falling victim.

Password Manager

zone 1

A password manager is essential, easy to use, and dramatically improves your security.

Protecting your identity, on paper, is fairly simple: it *"just"* requires:

- **Strong passwords** (not `MyDog'sName`, nor `MyD0g'sN4m3!`, but rather `3&m7wz$Eqq88&26hZ6DH!#&4`)
- **Unique passwords** for each site (or rather, each account). Otherwise, one security breach on a site can compromise all accounts using the same password.

In practice, this means it's impossible to remember all your passwords, and you need to use a **password manager** to do it for you. These are tools that store passwords securely, encrypted, and allow you to access them when needed.

Once again, **avoid proprietary software**: trust relies on open code. **Also avoid your browser's internal password management**, as its security is suboptimal.

For most people, Bitwarden is ideal: Free, open-source, easy to use, full of practical features, and integrated into browsers and mobile devices. If you're looking for an alternative, Keepass and Pass are projects worth exploring.

You'll need to protect access to this password manager with a… password, called a *master password*, which is also strong and unique. Fortunately, **this is the only password you'll need to remember** from now on. Ideally, this password should include numbers, lowercase and uppercase letters, special characters, not resemble dictionary words, and have no logical connection to you.

Get Cyber Safe gives the following excellent advice for choosing a secure and memorable password:

> *A trick we recommend: create a sentence, such as “The best time to play basketball is in June.” Take the first letter of each word, some in uppercase, some in lowercase, and add numbers you’ll easily remember. You’ll get the following result: Tbtpbij2366. That’s a password only you can remember.*

Once you’ve chosen a password, I suggest testing it on How secure is my password?

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

7)

Special mention to Safari, which is far more secure by default than Edge or Chrome. However, privacy is a different matter

8)

which can easily be disabled

9)

the underlying web rendering engine

10)

free and Firefox-based

11)

widely regarded as one of the most reliable