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.

Une version française de cette page se trouve ici

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

![warning] 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.
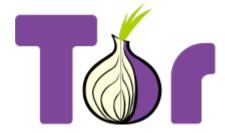
TOR network

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 Blink[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/Blink.

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?

Two-Factor Authentication - 2FA

<mark>zone 2</mark>

Two-factor authentication[12] is a technique used to enhance the security of an account. To authenticate, it's no longer enough to know the account's password, which could be compromised, but you must also **prove possession of a secret**.

You've likely encountered this before, for instance, when websites send you a code via SMS when logging in. This is an extremely effective technique if implemented properly, and **you should enable it whenever possible**.

There are several implementations of 2FA, and while **all are more secure than single-factor authentication**, they are not equally effective:

- **SMS**: Often imposed, especially by banks, this is the weakest form of 2FA. The security and privacy of SMS are a joke, and it's easy for an attacker to gain access. This method could also cause problems when trying to log in from an area with no cell network or if you lose your phone. It's favored[13] by institutions because it's an easily accessible and familiar technology for most people.
- **Email**: Working on the same principle as SMS-based 2FA, it's much less popular but significantly more secure.
- **TOTP**: You might be familiar with Authenticator, the app developed by Google[14], which gives you 6-digit codes for each registered service that change at regular intervals. This implementation, known as **TOTP**[15], is **much more secure than SMS or email**, while still being fairly widespread. Moreover, you're not required to use Google's app. Though open-source, it's not very ergonomic. I recommend 2FAS, which is open-source, more user-friendly, and gives you greater control over your secrets.
- **Physical keys**: You can also use physical keys with the U2F[16] or FIDO[17] protocols, such as those sold by Yubico. This is undoubtedly the simplest and most secure method to use, but it's not supported everywhere. Be sure to **have a backup key**, just like with your house keys!

> **To summarize:** Use 2FA whenever possible. Prefer physical keys and TOTP where available, but email and SMS are better than nothing.

> 💡 You can use **a physical key or a TOTP token in Bitwarden**.

Communicating

Emails

Email is **one of the oldest internet protocols**. As such, it was designed in a completely different context than the one we know today—a world where data theft, identity theft, and spam hardly existed—and is absolutely not built to address these challenges.

However, **email is at the heart of our digital identity**: we use it to authenticate with banks or governments, receive confidential data, reset passwords… For most people, **a security breach on their primary email is a potential disaster**, putting all important accounts at risk.

Beyond the security issue, privacy is also crucial with email. Without going as far as this grim story of Yahoo Mail technicians accessing intimate photos, **all the content of your emails is scanned to gather data about you, sell it, target you, and profit from it**.

There are several ways to protect yourself from this intrusion, such as self-hosting your email or encrypting them systematically (`zone 3+`), but these are usually cumbersome and difficult to implement.

Secure Providers

`zone 1`

A simpler solution is to switch to **a secure email provider that respects your privacy**. These are few in number and often paid, but they make **a significant difference** to your ASP.

- Proton Mail is a service that automatically encrypts your emails, enabling end-to-end encryption between users of the platform[18], based in Switzerland[19], and does not require personal information to sign up[20]. They offer a free plan, likely sufficient for most people, as well as several paid plans, with more storage, the ability to use your own domain name, and other features. It's an **excellent service**, easy to migrate to from another provider, especially *Gmail*, and very simple to use.

- Tutanota is a similar service, also offering a limited free plan. It's slightly more innovative[21] but also a bit harder to access, making fewer concessions to user-friendliness.
- Riseup is an activist collective, with anarchist leanings, that provides free, secure communication services for activists (on the left!). It's probably the only free provider robust enough to be recommended here.

Anonymous and Secure Email

`zone 3`

Using the providers above places you in an infinitely better situation, from an ASP standpoint, than any mainstream provider, but **this does not guarantee complete anonymity**. For instance, Proton was recently in the news for logging the IP address of a French environmental activist at the request of authorities.

This doesn't give authorities access to the content of their emails, but it can still endanger a person or their activities. If you're concerned about this type of anonymity and want **something more absolute** than what the above providers offer by default, here are a few tips:

- With the **TOR browser**, connect to Proton Mail's onion service and create a free email account. Choose an identifier with no connection to you[22] and a strong password, which will immediately be stored in a password manager,
- **Do not reveal** this email's existence to anyone, let alone its connection to you,
- **Never** use this email outside of TOR, and **always** use the onion service to access it,
- **Never** use this email for any activity related to you, even remotely.

Such an email account won't be useful for everyday life, but if you need **a truly secure and anonymous means of communication**, this is probably one of the easiest and most effective methods.

Instant Messaging

The other major axis of online communication is instant messaging: Messenger, WhatsApp, Telegram, Signal, to name the most well-known.

The situation has greatly improved over the past few years in this area, with **end-to-end encryption** being integrated into all major services. However, not all these services are equal: **some collect metadata about you, others retain the encryption keys to your data**, or rely on proprietary software for encryption.

To keep it simple, as much as possible, **use Signal**, the only one of these services that collects no metadata, and relies entirely on open-source software on both the server and client side. The only real

issue with Signal is that it requires a phone number to create an account, which excludes true anonymity.

If you can't use Signal (for example, if your contacts don't use it), make sure to enable end-to-end encryption in the settings of your messaging app.

Backing Up and Managing Personal Data

zone 2

Backing up your data online, using services like Google Drive, Dropbox, or OneDrive might seem like a good idea from a security standpoint. These services offer several useful features on top of the security provided by backups.

However, there are several problems with this approach:

- **All your data will be scanned**, indexed, and used to profile you and generate profit,
- **A synchronization service is not a backup**, and cannot replace one. If you accidentally delete an important file, it will also be deleted from your online sync. If ransomware encrypts your files to extort money in exchange for the decryption key, this encryption will also be propagated to your online sync.

That being said, **maintaining an up-to-date backup of your data is crucial for security**, unless you have no important data stored digitally.

Several approaches can help circumvent these issues:

- Making backups on **physical media**, such as external hard drives or USB keys. This is a viable approach, but it becomes quite complex when considering the need for regular backups, stored off-site to protect against risks like theft or fire. **This approach requires a lot of discipline and regular rotation of media**, making it a fragile and difficult strategy to implement.

- Using an online service, such as those mentioned above, but **encrypting your data** before uploading it to the service. This is a perfectly viable approach, though somewhat complex. You won't be able to rely on the built-in sync features of mainstream services, and you'll lose access to features that require unencrypted files (such as sharing or online editing). If you choose this route, it's better to use a "bucket" service like AWS, which will cost less and be better suited for this use case. I personally use Backblaze B2,

.

```
* <wrap danger>zone 3</wrap> Self-hosting your own data storage,
synchronization, sharing, and editing service, using a tool like
[[https://nextcloud.com|NextCloud]]. This solution is by far the most complex,
but it's also the one that gives you the best of both worlds: complete control
over your data security, along with sharing and editing features. However,
this route is **far more technically demanding** than the previous two.
```

Going Further

These general tips cover the essential daily concerns regarding ASP, and applying them will place you in a far better position than you likely are by default.

However, if these issues are important to you, many other stones deserve to be turned.

A Secure Operating System

The operating systems of our computers and phones can have a major impact on our security and privacy:

- **Windows is notoriously insecure**, though the situation has improved considerably. Its code is also almost entirely proprietary, and it spies on you without hesitation. In short, avoid it if you care about these issues,

- **Mac OS is relatively secure by default**, and far more so than Windows. However, in terms of privacy, Apple's practices are just as questionable as those of Microsoft.

- zone 2 Linux is uncommon on desktop computers, and it has a reputation for being difficult[23]. It's open-source, which gives it a structural advantage, but **it's not particularly secure by default**. However, **it's an excellent starting point** for securing your system and controlling your data, for example by encrypting the entire installation.

- zone 3+ Some **Linux distributions are specialized in security and anonymity**, such as Tails or Qubes OS, **both extremely secure systems that allow for advanced anonymity**, at the cost of significant constraints.

- **On smartphones**, the situation is a bit more complex:
  - By default, **iOS is more secure than most "stock" Android systems** provided by manufacturers,
  - "Stock" Android, as distributed by Google on Pixel devices and occasionally by some third-party manufacturers (One+, Oppo, Motorola), is on par with iOS in terms of security, but gives you more freedom to do more,
  - zone 3 There are **third-party Android ROMs** that can be installed on certain devices and are focused on security: **GrapheneOS and CalyxOS** are particularly notable. These systems

are generally more secure than stock Android, but being small projects, they expose you to delayed updates or the risk of disappearing without notice,

- ○ **The cellular network itself is a security flaw**, as it **constantly tracks your location**. This location data is not hard to obtain and is available to anyone for a small price,
- ○ `zone 2` A *dumb phone* protects you from the software profiling of apps and services on your smartphone but does not protect you from being located through the cellular network,
- ○ `zone 3+` If you need an anonymous phone that's hard to track, you can consider using a **prepaid phone**, keeping the number secret, and using the SIM card only to access the data network. You can then use a **VoIP service** over this data network. Note that you are still fully locatable; this just makes it harder to associate you with your cellular number.

Self-Hosting

`zone 3`

To avoid entrusting your data and its security to third parties, **one possible approach is to self-host**[24] **all the services that handle your data**, from email and backups to streaming movies or music.

This is an approach that's **very effective but requires a lot of time and work**. For most people, it's impractical—too difficult, too time-consuming, and perhaps even too risky, as the security of these systems depends entirely on your own knowledge and diligence.

If this is a path you want to take, I recommend sharing the efforts with a few friends to distribute the work and responsibilities. You'll learn a lot along the way, but you'll also likely experience some lonely moments :)

> `zone 3+++` Do not attempt to self-host your email without solid experience with Linux, hosting other web services, command-line tools, strong programming knowledge, and a tested, proven backup plan.
>
> This is an especially hostile sector, and any configuration error will be exploited faster than you think, potentially within minutes of your mail server going live. **Likely causing significant damage to both you and third parties**.

Everything Else

I've tried to cover the main issues of online security and anonymity, but each application and service we use is likely to expose us to new risks.

Applying these tips should give you a solid foundation and a good sense of online security, enabling you to generalize them to other situations. The core principles remain the same, and similar techniques apply:

- Prioritize **open-source software and protocols**,
- **Limit the permissions** granted to third parties to the bare minimum necessary,
- **Minimize exposure** of your data as much as possible,
- Identify your needs, **model the risks** you face,
- **Know the limitations** of the security measures you rely on,
- **Formalize and systematize** your security practices to minimize human error.

Modeling Risks and Developing Appropriate Strategies

These tips are broad, and you may be wondering what is relevant or not in your situation. I won't delve deeply into risk modeling here, but here are three profiles to help you identify your position:

General Public

`zone 1`

You don't have anything specific to hide, don't handle sensitive data, and don't want to invest a lot of time, effort, or money into these issues. You have no reason to be specifically targeted, either by a government or a private actor. **Your main concern is to avoid overly intrusive profiling and protect yourself from criminal attacks**.

- Use a password manager and activate 2FA where available,
- Use the Brave browser, or configure Firefox if you prefer to support web diversity,
- Move your email to Proton Mail,
- Think about a backup system for your data, keeping in mind that backups and syncs are not the same.

Increased Security Needs

`zone 2`

You are involved in **activism**, handle **sensitive data**, or for some reason, are at risk of being **targeted by malicious actors**:

- In addition to a password manager, ensure you only use services compatible with 2FA and that offer either TOTP or physical keys,
- Besides transferring your email to a secure service, learn to use GPG and the concept of asymmetric encryption. Ensure your correspondents also use secure services.
- Keep up-to-date, encrypted backups, with at least one stored off-site.

Healthy Paranoia

`zone 3`

If you suffer from healthy paranoia, whether justified by your activities or the surveillance you're under, or simply by your own twisted mind, the tips on this page are, of course, applicable but probably not enough. At a minimum, you should:

- **Encrypt all your data**, even locally,
- Master GPG, asymmetric encryption, and apply a strict policy of encryption and signature,
- Have **an anonymous email** created and accessed exclusively via TOR,
- Use **a free operating system**, such as Linux, **and** harden its default security settings with TOR, SELinux, and various hardening techniques,
- Consider using **a security and anonymity-focused OS, like Tails**,
- Leave or at least severely compartmentalize social networks,
- Learn to use **anonymity-oriented cryptocurrency**, like Monero,
- Stay actively informed about technologies that keep you secure. If an encryption algorithm or service you use is compromised, you want to know about it before a malicious actor exploits it against you.

Resources

If you're looking for relevant resources on these topics, you can check out:

- The Electronic Frontier Foundation is probably the most important organization addressing these issues,
- They provide several practical tools:
  - Atlas of Surveillance,
  - Surveillance Self-Defense,
  - Cover Your Tracks,
- You can also take a look at Techlore, which aims to document and simplify security and privacy for the general public.

Web, Cryptography, Security, Linux
[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

12)

commonly referred to as "2FA", for *Two-Factor Authentication*

13)

wrongly, in my opinion

14)

but entirely open-source

15)

Time-based One-Time Password

16)

Universal 2nd Factor

17)

Fast IDentity Online

18)

and with any recipient, as long as they know how to use GPG

19)

which has much more protective privacy laws than the USA

20)

It's possible to pay anonymously if necessary

21)

the encryption used does not rely on GPG and seeks to overcome its limitations

22)

for example, a random word and a number between 0001 and 9999: `glacis9456`

23)

it's not really that hard, but it certainly requires learning a new paradigm

24)

yourself or a trusted third party

From:
http://2027a.net/ - **/dev/null**

Permanent link:
http://2027a.net/tech/privacy_and_security_online?rev=1728153893

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