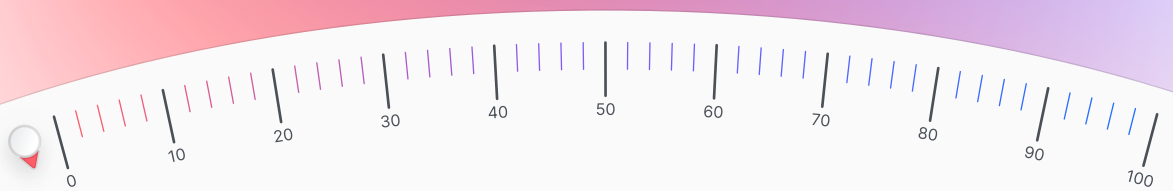
Privacy Guide

How to protect your privacy on the Internet ?

Qwant, Proton, Olvid and Murena give you the keys to understand and implement solutions to protect your personal data on the web.



The guide proposed by :

Qwant Proton Olvid murena

In the era of more ethical and responsible digital services, **Qwant, Proton, Olvid** and **Murena**, major players in Europe **offering ethical digital services** without collecting personal data, give you the keys **to understand why you should protect your privacy online and how to keep your data truly private**. Definitions, tips and solutions, this is THE guide that will accompany you in your transition to a world where you will be free and incognito.

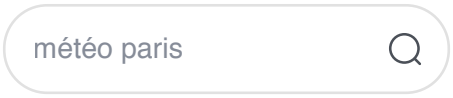
Have you ever felt like you were just accepting cookies when you arrived on a website? Are you tired of finding advertisements for sneakers, under the pretext that it was the object of your last search? You systematically accept the sharing of your geolocation, even if the site or the application does not require it? Are you tired of having no choice but to share emails, files and private information with companies and want to take back control of your online identity? Do you feel like your smartphone is spying on you?

If you recognize yourself in at least one of these situations, then **this guide is for you!** We will give you the keys to better understand how the internet knows everything about you. We will also share with you **tips and solutions** to limit the data you leave behind when you surf the web.

1 Review and learn the basics

Each time you connect to the internet, you leave a trace of your passage: information searched for, products bought, comments posted, emails sent, posts commented on, connection to sites, use of an application..., everything is listed! This may seem harmless to you, it doesn't matter that we know what you like. **But what about the data transmitted without you wanting it?** How do sites use it?

As you log on or use third-party applications, this data is accumulated and forms your digital profile. Your **digital profile** reveals **your relationships, your opinions, your habits, your movements, in short, your entire private life**. This digital profile is often sold and resold to multiple companies for profit. How is this possible? How does it work? Here are some explanations that will help you better understand this subject.



What is the difference between a browser and a search engine?

A browser is a software that allows you to consult web pages, such as an e-commerce site or that of your favorite media for example. Today, the most commonly used browsers on the market are Firefox, Safari and Chrome.

The search bar present on the browser allows both to access a web page via its URL (*www.exemple.com*) but also to search via the search engine defined by default on the browser.

A search engine is a website that allows you to search for other websites. A search engine is therefore accessed via a browser.

Today, the most used search engines are Bing, DuckDuckGo, Ecosia, Google, Lilo, Qwant, or Yahoo.

You make a request, for example "weather in Paris" and the search engine will suggest several sites that could meet your request.

The search engine guides you to the right site while the browser is just a connection to the digital world.

To illustrate the difference between these two terms, the browser is the vehicle that transports you while the search engine is the GPS that shows you the best way to find the best web page corresponding to your request.

What is a cookie ?

Surely, you have already seen an advertisement on social networks and asked yourself "how can they know that I have already searched for this product on another website? "The answer to the question is ... "thanks" to cookies!

But what is a cookie?

It is a small **text file that is deposited by the browser**, on your computer when you visit a website. This cookie will track your navigation on the web. This cookie has an expiration date, that is to say that it is deleted after a certain period of time.

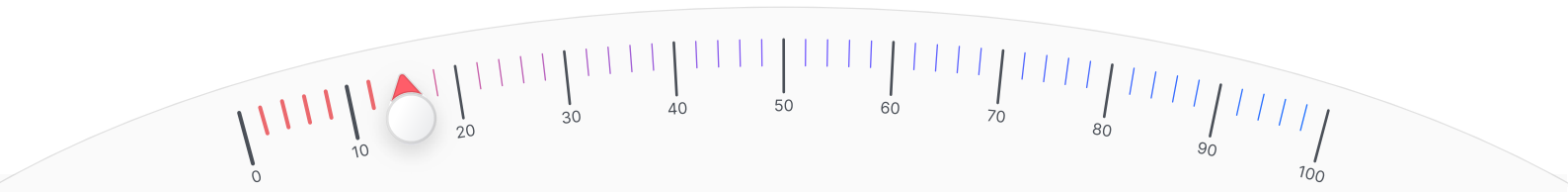
This cookie, deposited on your computer, can have several uses:

Functional cookies:

They record your preferences on a website, i.e. automatic login to the account, location, language and other settings you choose. This helps to improve your experience as a user of a site.

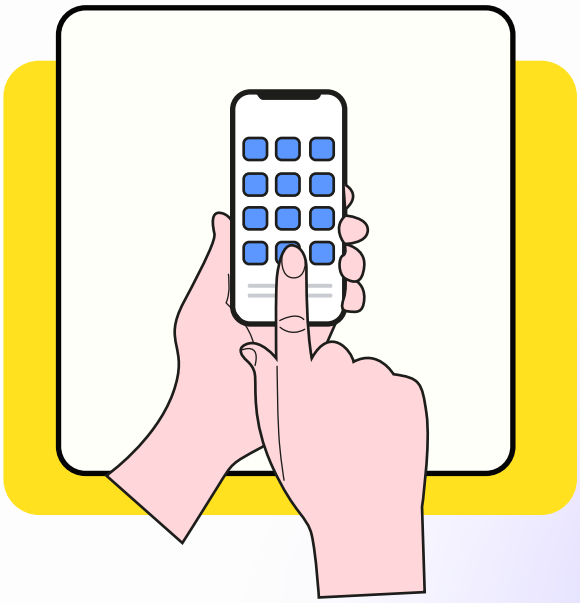
Third-party cookies or advertising cookies:

They primarily record user behavior and the visitor's path through the Internet in order to create **a user profile** that is enhanced as the visitor logs on. On the basis of this user profile, it is then possible to place personal advertising. This user profile can then be **sold to third-party sites** and social networks, for example, which will then present you with advertisements for brands or products you have previously searched for. This is how you end up with an advertisement for a pair of shoes you searched for a few days or weeks before, without having asked anyone.



What is a tracker?

Trackers can be found **in the mobile applications** that you download on your smartphone. These trackers are **code libraries** (called Software Development Kit or SDK), **in charge of collecting information** about the person who uses an application, or about the uses or the environment of this person. These SDKs allow to save time in the development of an application by using already existing code. They can be used to analyze the audience or the path taken by the user on the application, but also to locate and profile him. This tracker will therefore **collect information about you**, your usage, just like cookies, but on your smartphone.



What are web beacons?

Web beacons are widely used by businesses and marketers, especially in newsletters and promotional emails. They are simple **images hosted on an external server** that are inserted into your emails. Once they are loaded for display in your e-mails, these web beacons **collect and share personal information** such as the date and time of opening, the type of device used and the operating system, or your IP address and geographical location. This information can then be collected and used to profile you and target you with personalized ads. Some of these trackers are almost invisible - they appear as small transparent images that are only used to collect additional information about you.

How does online advertising work?

We see advertisements every day: on social networks or on television, whether it's to offer us discounts on our next trip or for a product that we've been wanting to buy for weeks! But do you know how it really works?

Online advertising involves 3 actors:

- **Advertisers** who **promote their product,**
- **Advertising platforms** on which the ads are **displayed,**
- **Tracking companies** that **collect a lot of information about you**

As we have seen in a previous paragraph, every user leaves traces on the Internet. These traces can be collected by tracking companies that place the famous advertising cookies on our computers and smartphones to retrieve data. These data can be sold to advertising platforms. Brands then use these platforms to advertise their products. The role of advertising platforms is to connect users to the product to be sold, thanks to the profile established from their personal browsing data.

As we have seen in a previous paragraph, every user leaves traces on the Internet.

These traces can be collected by tracking companies that place the famous advertising cookies on our computers and smartphones to retrieve data. These data can be sold to advertising platforms. Brands then use these platforms to advertise their products. The role of advertising platforms is to connect users to the product to be sold, thanks to the profile established from their personal browsing data.

Not very convenient when the purchase is personal, or when it is a gift, no?
GAFA (Google, Apple, Facebook, Amazon) are the most important advertising platforms on the market.

What is an algorithm?

If we schematize, an algorithm is **a set of operations that allows to solve a problem**. For example, a cooking recipe is surely one of the simplest algorithms: it is a sequence of instructions that allows to obtain a result. Of course, there are more complex ones.

Search algorithms, for example, are **sequences of instructions that allow you to obtain a result based on a request**. This result can be an object in an image, a word in a text, or a list of web pages. We can see an algorithm a bit like a production line: we provide information in input, and we obtain a result in output.

This is how search engines work. You enter a query and the search engine will use a series of algorithms to fetch all the web pages that might answer your question.

There are **two types of search engines**:

Those whose search results are influenced by your personal information, your geolocation, your culture, your search history (recipes searched, news consulted, favorite sites etc.). This is the case of Google for example.

Those that do not use this information because they do not collect personal data, such as Qwant for example.
The proposed results are therefore impartial in the sense that they are the same for everyone, regardless of your profile.

Some algorithms have been designed in such a way that their behavior evolves over time, depending on the data they have been provided with. These "self-learning" algorithms are part of the research field of expert systems and artificial intelligence. They are used in a growing number of fields, from traffic prediction to medical image analysis.

holidays

What is a filter bubble?

The filter bubble is the concept in which **algorithms bias users' opinions by recommending content based on user preferences**. User preferences are known thanks to the cookies deposited by the sites, when browsing the Internet.

The content that is then proposed to you as you search is over-personalized and can generate a kind of confinement, isolation in an intellectual and informational bubble, which is called a filter bubble.

Concretely, some search engines can show different **results to two users who make the same request**.

For example, a search for vacation accommodation may yield results for 5-star hotels rather than campings or bed & breakfast based on search and browsing history. This is also true for the news you are offered or the prices advertised. Your browsing habits put you in boxes that define your profile. The news you are offered will then be related to this profile, thus limiting your critical sense. The Internet user is thus locked in a filter bubble.

The only way to avoid **being trapped in this bubble** is to limit as much as possible the traces you leave on the Internet, to limit as much as possible the collection of your personal digital data.

What is encryption? What about end-to-end encryption?

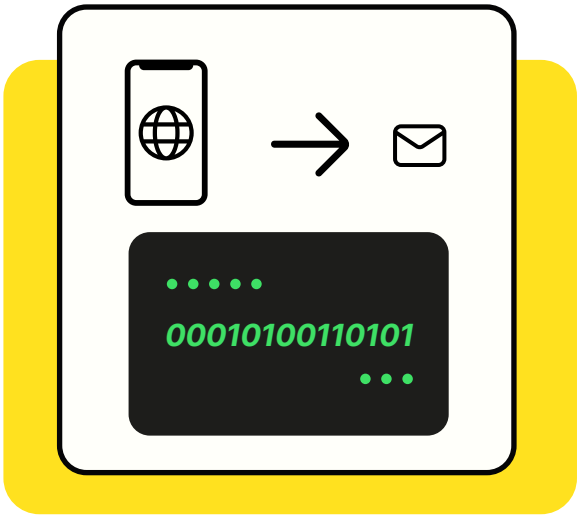
When you communicate over the Internet, your data potentially travels hundreds or even thousands of miles before it reaches its destination. Cables, routers, servers are needed to carry your data. But does this mean that all these elements necessarily have access to everything you send, even though they are not the final recipients? No! It is possible to protect your data from eavesdroppers with **cryptography,** the science of secret codes, through a process called "**encryption**".

Let's take an example: when you connect to *https://www.qwant.com/* and perform a search, your request is automatically "encrypted" by your browser before being sent to Qwant's servers, where it will be "decrypted" so that Qwant can prepare a list of relevant sites to send you. Of course, this list is also encrypted by Qwant before being sent to you. Your browser then decrypts this result just before displaying it to you. That's it!

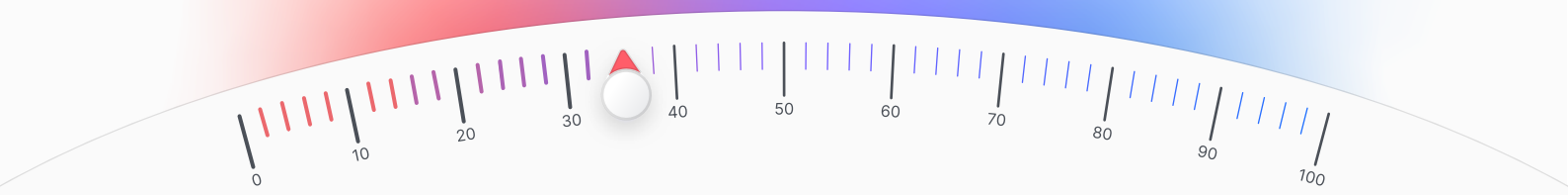
Through encryption, your searches are known only to you and to Qwant, which does not know who is behind the search.

We have seen how encryption allows you to secure your communications with a server offering a service, such as Qwant. But what about communications between you and another physical party? This is where "**end-to-end encryption**" comes in.

When you send a message to a correspondent via a traditional public messaging service, it is usually encrypted between your device (smartphone or computer) and the server of the operator offering the messaging service, which decrypts it in order to store it "in clear" while waiting for the recipient to come and get it. This message is then encrypted between the server and the final recipient. This is called "**point-to-point encryption**". The problem? The problem is that the service provider has access to everything you communicate, even though they are not the final recipient. Fortunately, there is a solution: **end-to-end encryption**. This technology e**nsures that your messages will be encrypted on your device before leaving it and will only be decrypted in one place:** on the recipient's device. In between, your messages remain encrypted, even when stored on the service provider's server. It's that time again!



Unfortunately, few email services offer end-to-end encryption by default. This is not the case with Gmail (for email) or Telegram (for instant messaging). This may seem surprising: in the end, end-to-end encryption only **reproduces in a digital world what we have been doing for centuries with our physical letters**: we put them in envelopes before sending them!



The right habits to adopt to control your data

"Today it's decided! I control the traces I leave when I surf the Internet". You don't know where to start? We can help you! First step: spring cleaning. Once everything is cleaned, we equip ourselves. 3, 2, 1 ... let's go!

2 Do the cleaning

Delete cookies and browsing history

Cookies record your actions, in other words your navigation on the Internet. So the first thing to do is to clean up and **delete your cookies**.

How do you do it? It all depends on your browser!

If you use Firefox:

1. In the menu bar at the top or bottom of the screen depending on your device, click on Firefox and select *Preferences*.
2. Select the *Privacy & Security* panel and go to the *Cookies & Site Data section*.
3. Click the *Clear Data* button and the Clear Data window will appear.

   The boxes for *Cookies and Site Data* (to delete site connections and site preferences) and Cached Web Content

   (to delete cached images, scripts and other web content) should be checked.
4. Click on *Delete*

If you are using Safari:

1. In the Safari application on your Mac, choose *Safari*, then *Settings*, and click *Privacy*.
2. Click *Manage Website Data*.
3. Select *one or more websites*, and then click *Delete* or *Delete All*.

On iPhone, to delete your cookies, but keep your history,

1. Go to *Settings* > *Safari* > *Advanced* > *Site Data*,
2. Click > *Delete Site Data*.

If you use Chrome:

1. On your computer, open Chrome.
2. At the top right, click *More* and then click *Settings*.
3. Click *Privacy and Security*, and then click *Cookies* and *Other Site Data*.
   Click on *View all site data and permissions* and then click on *Clear all data*.
4. To confirm, click on *Delete*.

-

Review your geolocation settings

Not all applications need to track your movements to function. A quick trip to the location settings is therefore necessary to make sure that your settings are defined according to your wishes and not systematically by all the applications that have asked for your permission.

To do this, follow these procedures:

On Android :

1. Go to > Applications
2. Application Permission
3. Location

On iPhone :

1. Go to > Settings
2. Privacy
3. Location services

Now it's your turn to choose the applications for which you accept or not the location!

Clean up your social networks

Don't like all the pictures of you? Want to limit access to them? It's time to check what people can know or see about you on social networks.

On Instagram, TikTok and Facebook:

↪ **Step 1 :** Switch your account to private if it isn't already.

↪ **Step 2 :** Sort through the people who subscribe to your account. Old acquaintances, strangers, it's time to sort out the people you want to share your content with.

↪ **Step 3 :** Was your account created a few years ago? Maybe it's time to take a look at your old posts to see if you're still comfortable sharing all those photos.

↪ **Step 4 :** Think before you post content and before you accept a subscription request.

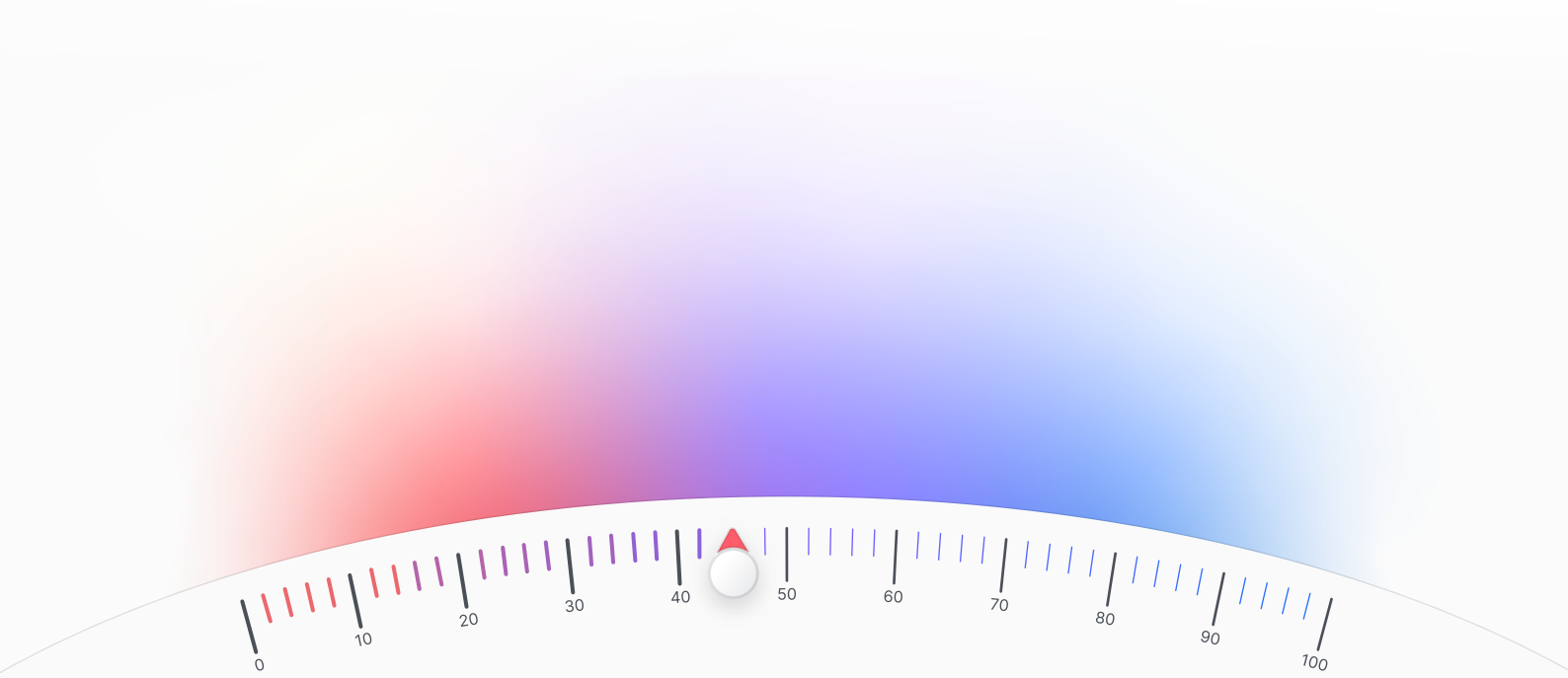
Monitor your e-reputation and assert your right to be forgotten

Friends' publications, names associated with works, events, sports performances, former activities... but **what does the web know about you?** To find out, all you have to do is regularly type your first and last name, your e-mail address or other data that you may share online and that allow you to be identified on any search engine.

What should I do if unwanted content is posted on the Internet?

When possible and if it is not malicious, you can request deletion directly from the person who posted it, or if you are not satisfied with the response, you can exercise your right to be forgotten. T**he regulation on the protection of personal data (RGPD)** allows any person to request the deletion of data concerning him. To do this, you must contact the website that published the information directly, specifying the URL, the information to be deleted and the reason that leads you to make this request. These contents can then be removed.

At the same time, you can ask the search engines to no longer associate content that may be prejudicial to your name.



3 Equip yourself, protect yourself

Now that the cleaning is done, here are some habits to adopt.

Activate location only when the use of the service requires it

Not every application or site you visit needs to track your movements and know your location at all times. Take the time to decide when the service asks you for access: why does this site need to track my movements? Does entering my location myself give me a satisfactory user experience?
Adapt your answers accordingly!

Use a browser and search engine that are more respectful of your personal data

Your gateway to the web is through a browser and a search engine. So you need to change your habits, right from the start of the experience, by choosing a browser and search engine that are more respectful of your personal data.
This is the case with Firefox as a browser, or Brave or the Qwant application.

For search engines, try Qwant (French search engine) or DuckDuckGo, search engines that do not collect your personal data and therefore do not sell it.

Use private browsing

Private browsing is a feature available on browsers that allows you **to browse without having browsing data like history or cookies stored** on your device.

With private browsing, once you log out, neither your browsing history nor cookies are saved. However, this does not prevent sites from depositing cookies on your device. It is therefore a first step before switching to the tracker blocker.

To browse in private mode, simply go to your browser settings and open a "new private browsing window".

Refuse non-essential cookies

If you don't have cookie blockers, most sites will ask you to accept or decline cookies. Try to refuse them systematically, or accept only those essential to the use of the service.

This is restrictive, which is why we suggest the following step: "Install a cookie blocker".

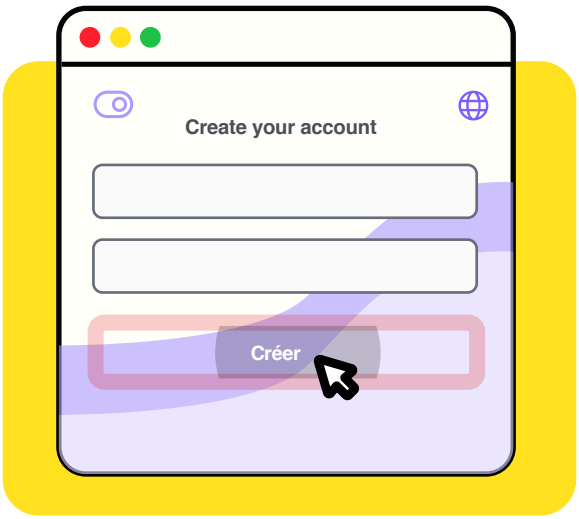
Install a tracker blocker

In order to navigate safely, we recommend that you install **a cookie and tracker blocker.** This blocker will allow you to surf the web in complete confidentiality. We recommend installing the **Qwant VIPrivacy** browser extension, which will block cookies and trackers while you are browsing, and install Qwant as your default search engine. You can also use a tracker protection tool or use **an email service that automatically blocks trackers**. Proton Mail's enhanced tracking protection is enabled by default for all users on the web and on the **Proton Mail** app for iPhone and iPad. This feature protects your privacy from tracking attempts in your emails and gives you greater peace of mind. Safe and confidential browsing from one end of your search to the other! By installing **/e/OS on your smartphone**, you can use **Advanced Privacy tool to control all trackers in your applications** with a few clicks.

Choose your email and instant messaging

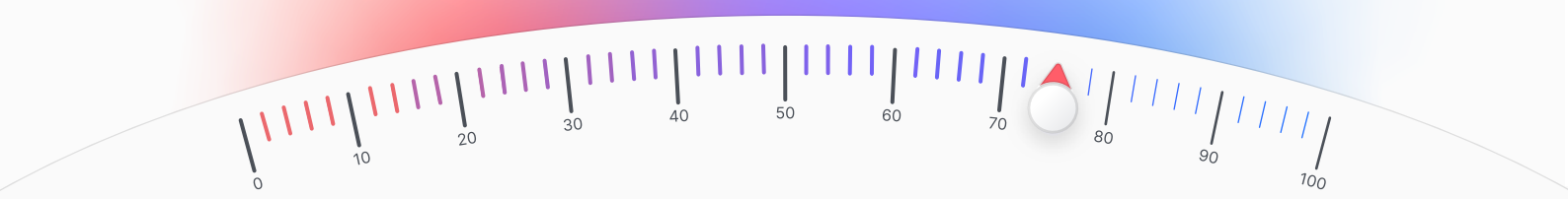
In order to secure your emails, your calendar or your drive, we advise you to create an account on the **Proton** website.

For your instant messaging, we recommend installing **Olvid**, the first private messaging service for everyone, free on iOS and Android.



In both cases, the protection of your personal data is a priority. In the case of Olvid and Proton, for example, you won't even have to give the publisher a single phone number, address or name... In the case of Olvid, there isn't even an "account" on a server somewhere on the planet. This is because Olvid **does not require any personal data to operate**! Your data (like your name for example) is only shared with the Olvid users you decide to invite.

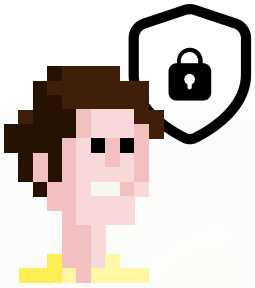
As a result, Olvid is the only messaging service that can guarantee that you will never receive spam. Using email services that guarantee, by design, that they do not have access to your personal data is the only way to ensure that a service that advertises itself as free is really free. Such services exist. Why go without them?



Use a VPN

A **VPN (Virtual Private Network)** is software that is installed on devices connected to the Internet and creates **a secure tunnel between you, as a user, and the Internet**.

When you connect to the VPN, all of your internet traffic is redirected through the VPN server before it reaches the final site. Connecting to a VPN server will result in your IP address being hidden and changed to that of the server. Finally, the VPN server acts as an intermediary. Thus, your original IP address will not be revealed to the website you are visiting and your privacy will be respected.
Here are some trusted products that you can easily install on your computer or mobile: **Proton VPN**, Express VPN, CyberGhost, Mozilla VPN and NordVPN.



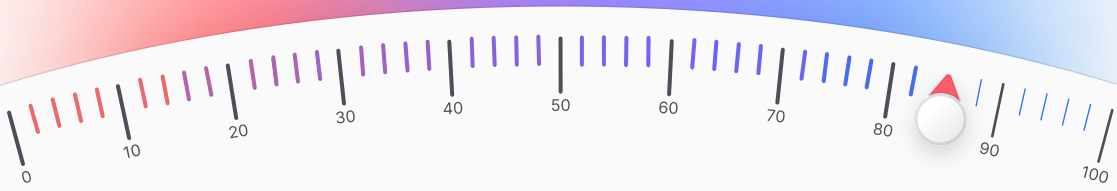
You now have all the cards in your hands to protect your online privacy: now it's time to play!

Choose a smartphone that does not use your personal data

It is very likely that **your smartphone is spying on you without your knowledge**. The majority of conventional smartphones collect a huge amount of data from your device, be it your contacts, your activity, your movements, and send all this data to servers at Google, Apple, Facebook and other tech giants.

Murena smartphones were designed to offer a different approach to privacy-conscious users who want to protect themselves from data-hungry phones. They are based on the open source operating system "/e/OS" which is fully "deGoogled": by default, **it doesn't send any data to Google and doesn't collect your usage data or your location**.

Not only does /e/OS allow you to consult a "Privacy Score" for each Android application before installing it, it also allows you to block trackers hidden in the applications and thus block micro-targeting.



This guide is presented by Qwant, Proton, Olvid and Murena; major European players that offer digital services that respect the privacy of their users.

Qwant

About **Qwant**

Developed in France and leader in Europe, Qwant is the search engine that respects the privacy of its users by not collecting any personal data. Qwant develops its own web indexing technology, designed to provide unbiased, exhaustive and unprofiled search results. Qwant provides a search service with zero tracking of searches, zero tracking of advertising and zero sale of personal data.

In addition to Qwant Search, Qwant Maps, a mapping service, and Qwant Junior, a search engine dedicated to 6-12 year olds, Qwant offers Qwant VIPrivacy, a browser extension that allows users to browse the web without being subject to ad tracking.
Qwant is available on the web: www.qwant.com, or through browser extensions. The Qwant browser is available on iOS and Android mobile applications.
Qwant has 6 million monthly users.

Qwant knows nothing about you, and that changes everything!

www.qwant.com

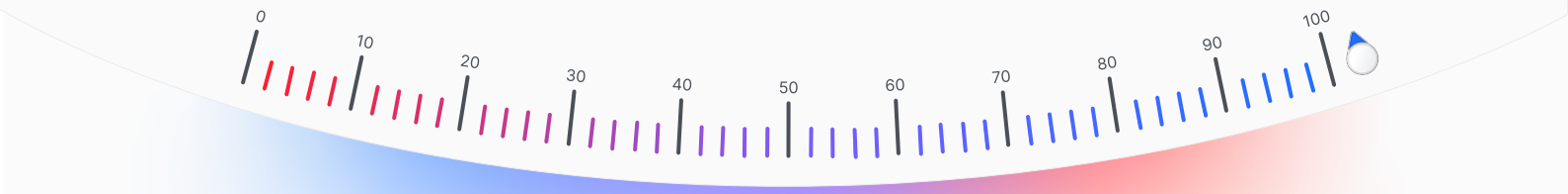
Proton

About **Proton**

Proton was founded in Switzerland in 2014 by scientists who met at the European Organization for Nuclear Research (CERN). Our vision is to create an internet where privacy is the absolute rule, through an ecosystem of services accessible to everyone, everywhere, all the time. Our first product, Proton Mail, is now the largest encrypted messaging service in the world. The products that followed, Proton VPN, Proton Calendar and Proton Drive rely on the same end-to-end encryption that gives our users complete control over how and with whom their data is shared.

Our products are open source, developed by a team of 400 people and supported by an active community in over 180 countries. Today, Proton makes privacy accessible to everyone with over 70 million user accounts, from journalists to some of the world's largest organizations and individuals.

https://proton.me/fr



About Olvid

Olvid is the first private instant messenger for everyone, available for free for iOS and Android.

In addition to the systematic end-to-end encryption of all your communications, Olvid guarantees end-to-end authentication of all your interlocutors. This protects you from any form of spam and ensures that only the users you choose will be able to communicate with you. Since Olvid does not require any personal data to operate (and therefore does not ask you for any), it is fundamentally free.

Create groups with your family, friends and key collaborators. There's no need to build a virtual network of 5,000 "friends". Olvid was designed to be the best place to talk about the things that matter, with the people that matter.

https://olvid.io

About Murena

Founded in 2018 by open source veteran Gaël Duval who created “Mandrake Linux”, Murena is a startup committed to privacy with outstanding transparent products and services that help people escape digital surveillance.

Murena believes that open source technologies are the only way to deliver on this promise, remaining fully auditable for maximum transparency. Murena designs /e/OS, a mobile operating system with pre-installed apps, and Murena Cloud, a set of online services to complement /e/OS.

Murena also develops Murena phones, with /e/OS preinstalled, ready to buy, shipping in the USA, Canada, Europe, UK, and Switzerland.

https://murena.com

Contact : dataprivacyday@qwant.net