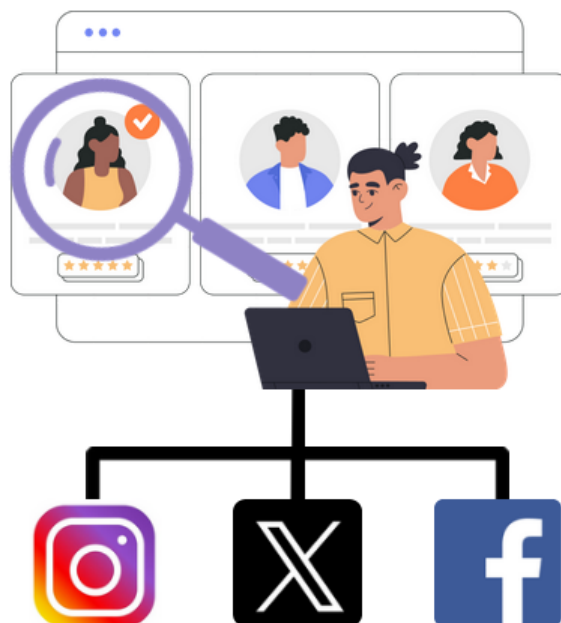


The proper use of social networks

The global success of social networks— first and foremost Facebook - has ushered society into a new era, that of digital exhibitionism. Real phenomena, these social networks provoke extreme reactions. Either you like them or you don't. Yet on closer inspection, social networks often offer as many advantages as they do disadvantages.

The main advantage of these interactive platforms is undoubtedly networking, both social (since they enable their members to keep in touch with friends and family) and professional (since some of them enable useful contacts to be made and jobs to be found).



These sites can also be used to send and receive messages, upload photos and videos, and build public awareness by creating a blog or Youtube channel to generate buzz and a certain number of views and likes.

They are also a highly effective promotional tool for companies, services, products or even sites. Instagram has thus become an essential platform for brands.

[For more information, refer to the factsheet **Presentation of the main social networks**]

On the other hand, the main risks include:

- account piracy, which can go as far as identity theft;
- burglary when a person has given not only his/her address but also his/her vacation dates;
- voyeurism, when purely private information, such as photos or videos, is published and can be reused for purposes not originally intended, for example on child pornography sites;

- online harassment, for example in schools, where teenagers threaten their peers to reveal naughty photos, or hurl insults or even incite the victim to commit suicide;
- undue sharing of sensitive information with complete strangers;
- unwanted use of collected data for advertising purposes;
- the risk of addiction, particularly among the very young who can't go to bed without going one last time on Tik Tok.



And while there's often no middle ground between those who want to go public and those who have chosen to live by the adage “to live happily, let's live hidden”, the solution may simply lie in learning to tame the social networks that have become part of our daily lives, and adopting the right behaviors.

A cats of actors who know everything about you



Remember ! In 2007, **Max Schrems**, a law student, initiated Europe's largest class action against Facebook. The young Austrian's crusade against the exploitation of personal data on the Internet was born after he asked Facebook to send him a compilation of his data collected on the social network. He was shocked to receive a 1,222-page file containing a meticulous list of all his personal data on the site, even those he thought he had deleted.

« If it's free, you are the product »

Social networks collect a great deal of data on their users, **often without their knowledge or informed consent**.

These data are collected **either directly** from the user, for example when a user account is created, **or indirectly**, through the various functionalities offered, such as the ability to “like” a publication.

A wide range of data is collected in this way, from the most obvious, such as identification data (name, profile photo, contact details, etc.) or the list of friends, to browsing data (content posted, sites visited, links clicked, etc.), geolocation data and data on interactions with other users.

These data are then often used for **marketing, profiling or targeted advertising purposes**.

Some major risks for users' privacy

In addition to a definite intrusion into the **private sphere** of users through personalized advertising and a lack, often, of prior consent to the collection of personal data, the **risk of surveillance** of these same users by social networks is also to be taken very seriously.

By analyzing users' behavior, activities and social interactions, social networks can create **extremely detailed** profiles and know the preferences of said users.

This risk is all the greater in that it often leads to data being transferred to **countries that do not offer an adequate level of protection**.

Most social networks belong to American companies such as Meta, which owns Facebook, Messenger, Instagram, Threads and WhatsApp, or in some cases even Chinese (TikTok, for example).

They store the data collected according to the regulations in force in their country, which are **far less protective** for users than the laws in force in Europe.



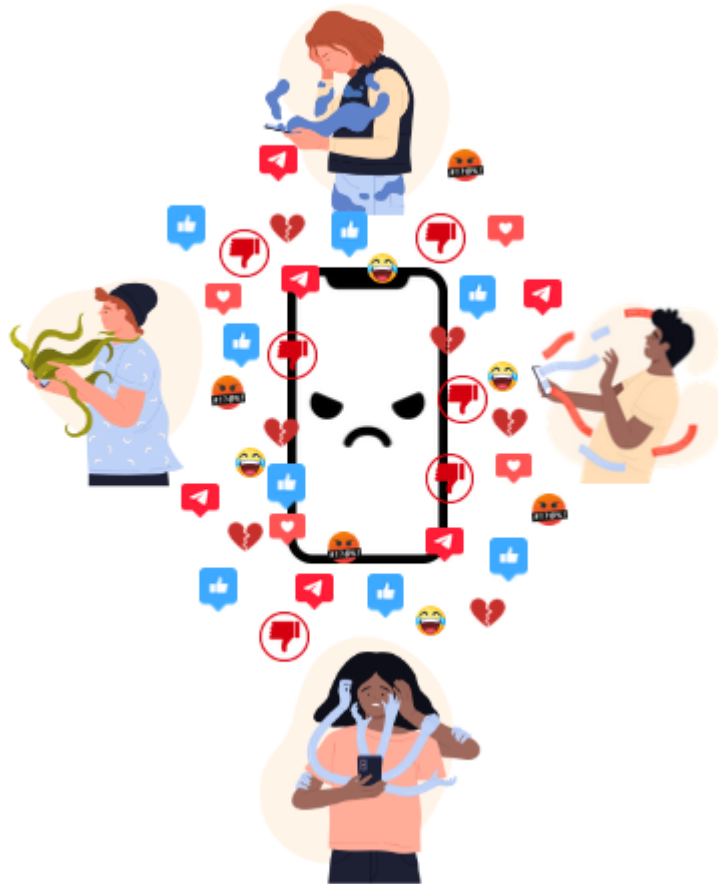
How to behave on social networks

Since the primary purpose of social networking is to exchange information with the rest of the world, **anonymity is virtually impossible**.

However, by adopting the right behaviors, you can protect your personal data and limit the risk of revealing more of your private life than you need to.

Although each network is different, they are all likely to collect 4 types of data:

- profile information (name, age, profession, education, etc.) ;
- traces of user activity ("*likes*", shares, comments, group memberships, etc.) ;
- silent activity (every movement is recorded, even in silent mode);
- device geolocation (used, among other things, to generate targeted advertising).



To prevent these data from being shared without restriction, social networks have set up their own security policies with **privacy settings**. Getting to know and configuring these settings is therefore the first good thing to do to avoid any unpleasant surprises.

Every network strives to improve these settings. They are constantly changing, so it's important to check regularly whether they still correspond to what you want.

And of course, it's a good idea to use social networks sensibly.

It's also very important to keep your personal and professional lives separate on any network.

Finally, don't forget that **nothing published is ever completely erased**.

 NOT TO DO	TO DO 
Never divulge your username or password Don't publish your full date of birth, which can be used by advertisers Don't mention your vacation dates (responsible for some burglaries) Don't constantly indicate where you are Don't accept just anyone as a friend Don't let your friends talk about you about anything and everything Don't tell anyone your political opinions, religion or telephone number. Don't like or relay content without thinking that it reveals your opinions Don't publish content that you wouldn't have made public in real life under your real identity Don't think that simply deleting a piece of content will make it disappear forever, and that there will be no trace of it	Separate “<i>personal</i>” and “<i>professional</i>” profiles Choose a secure, unique password, renewed regularly Have a different password from other accounts (e-mail, bank, etc.) Adapt confidentiality settings to your needs, and don't leave the default conditions. Make sure the correspondent is a friend and not someone pretending to be a friend (check the account, messaging...) Regularly delete inappropriate friends Ask yourself the right questions before publishing potentially dangerous content Ask yourself: “<i>Would I publicly approve this content in writing or in a face-to-face conversation outside the social network and under my real identity?</i>” Check the veracity of the information published, remain vigilant, report problematic content (particularly illegal content) to the authorities, and do not relay it.

Don't comment indiscriminately, because what is written on the net remains even years later	Regularly type your name into a search engine to check what information is circulating about you
Don't post embarrassing photos of yourself and/or your friends and family, because once they're published, they become uncontrollable.	Use antivirus software
Don't think that influencers know everything about everything and are an authority even outside their original field of competence	Install the most recent version of your browser (such as Internet Explorer, Firefox...)
Don't subscribe to third-party applications associated with Facebook (" <i>Like</i> " button, for example)	Delete cookies after disconnecting from the network (via the " <i>Delete browsing data</i> " option), to avoid being tracked, even when disconnected
Don't skip the conditions of acceptance with new versions	Prefer a secure connection (with the prefix " <i>https</i> ")
Don't leave children alone on social networks	Activate connection notifications, which inform you of all connections to your account
Don't click on all shared links, as they may be infected	
Don't connect from public Wi-Fi hotspots	