

# PROTECTING YOURSELF ON SOCIAL MEDIA

Social networks are among the most popular websites on the Internet. Facebook has over a billion users, and Instagram and Twitter have hundreds of millions of users each. Social networks were generally built on the idea of sharing posts, photographs, and personal information. For some, they're a good way to stay in touch with family, friends, and your support system. Any of these activities can rely on privacy and pseudonymity.

The following questions are important to consider when using social networks: How can I interact with these sites while protecting myself? My basic privacy? My identity? My contacts and associations? What information do I want keep private and who do I want to keep it private from?

## **Tips to Keep in Mind When Creating an Account**

Do you want to use your real name? Some social media sites have so-called "real name policies," but these have become more lax over time. If you do not want to use your real name when registering for a social media site, do not.

When you register, don't provide more information than is necessary. If you are concerned with hiding your identity, use a separate email address and avoid giving your phone number. Both of these pieces of information can identify you individually and can link different accounts together.

Be careful when choosing a profile photo or image. In addition to metadata that might include the time and place the photo was taken (hint: turn off GPS / location services in your phone's settings), the image itself can provide some information. Before you choose a picture, ask: Was it taken outside your new home or workplace? Are any addresses or street signs visible?

## **Choose a strong password and, if possible, enable two-factor authentication.**

Beware of password recovery questions such as "What city were you born in?" or "What is the name of your pet?" because your former partner probably nose the answers. You may want to choose password recovery answers that are false. One good way to remember the answers to password recovery questions, should you choose to use false answers for added security, is to note your chosen answers in a password manager.

## **Check the Social Media Site's Privacy Policy**

Information stored by third parties is subject to their own policies and may be used for commercial purposes or shared with other companies, like marketing firms. While reading privacy policies is a near-impossible task, you may want to read the sections that describe how your data is used, when it is shared with other parties, and how the service responds to law enforcement requests.

Social networking sites are usually for-profit businesses and often collect sensitive information beyond what you explicitly provide—where you are, what interests and advertisements you react to, what other sites you’ve visited (e.g. through “Like” buttons). Consider blocking third-party cookies and using tracker-blocking browser extensions to make sure extraneous information isn’t being passively transmitted to third parties.

### **Change Your Privacy Settings**

Specifically, change the default settings. For example, do you want to share your posts with the public, or only with a specific group of people? Should people be able to find you using your email address or phone number? Do you want your location shared automatically?

Even though every social media platform has its own unique settings, you can find some patterns.

Privacy settings tend to answer the question: “Who can see what?” Here you’ll probably find settings concerning audience defaults (“public,” “friends of friends,” “friends only,” etc.), location, photos, contact information, tagging, and if/how people can find your profile in searches.

Security (sometimes called “safety”) settings will probably have more to do with blocking/muting other accounts, and if/how you want to be notified if there is an unauthorized attempt to authorize your account. Sometimes, you’ll find login settings—like two-factor authentication and a backup email/phone number—in this section. Other times, these login settings will be in an account settings or login settings section, along with options to change your password.

Take advantage of security and privacy “check-ups.” Facebook, Google, and other major websites offer “security check-up” features. These tutorial-style guides walk you through common privacy and security settings in plain language and are an excellent feature for users.

Finally, remember that privacy settings are subject to change. Sometimes, these privacy settings get stronger and more granular; sometimes not. Pay attention to these changes closely to see if any information that was once private will be shared, or if any additional settings will allow you to take more control of your privacy.

### **Keep Separate Profiles Separate**

For a lot of us, it's critical to keep different account's identities separate. This can apply to dating websites, professional profiles, anonymous accounts, and accounts in various communities.

Phone numbers and photos are two types of information to keep an eye on. Photos, in particular, can sneakily link accounts you intend to keep separate. This is a surprisingly common issue with dating sites and professional profiles. If you want to maintain your anonymity or keep a certain account's identity separate from others, use a photo or image that you don't use anywhere else online. To check, you can use Google's reverse image search function. Other potentially linking variables to watch out for include your name (even nicknames) and your email. If you discover that one of these pieces of information is in a place you didn't expect, don't get scared or panic. Instead, think in baby steps: instead of trying to wipe all information about you off the entire Internet, just focus on specific pieces of information, where they are, and what you can do about them.

### **Familiarize Yourself With Facebook Groups Settings**

Facebook groups are increasingly places for social action, advocacy, and other potentially sensitive activities, and group settings can be confusing. Learn more about group settings, and if participants are interested in learning more about group settings, and work with others to keep your Facebook groups private and secure.

### **Privacy Is A Team Sport**

Don't just change your own social media settings and behavior. Take the additional step of talking with your friends about the potentially sensitive data you don't wish to be revealed. Even if you don't have a social media account, or even if you untag yourself from posts, friends can still unintentionally identify you, report your location, and make their connections to you public. Protecting privacy means not only taking care of ourselves, but also taking care of each other.