# Protecting Yourself on Social Networks

Social networking sites are some of the most popular websites and tools we use on the Internet. Facebook, Google+, and Twitter have hundreds of millions of users each. With social networking platforms come many benefits, such as the unprecedented opportunity to communicate, publish, coordinate, and persuade. Many people use it for their professional as well personal lives. But, this also means that we're sharing a lot about ourselves online, usually more than we realise. In some cases, this can put our operations, our contacts, or us at risk.

When using social networks it is important to consider:

* + What information do I want keep private and who do I want to keep it private from?

Depending on your circumstances, you may need to protect yourself against the social media site itself, against other users of the site, or both.

# Take care registering

* Consider whether you want to use your real name or not. Might you want to share things that could be dangerous if they were linked to you?
* When you register, don't provide more information than is necessary. Do you really need to include your birthday/contact number/employment details?
* If you are concerned with hiding your identity, use a separate email address. Be aware that your IP address may be logged at registration, so for full, guaranteed anonymity you may want to use a VPN or even Tor.
* Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities.
* Choose a strong password, change it regularly and, if possible, enable two-factor authentication.
* Beware of password recovery/security questions whose answers can be mined from your social media details. For example: ?What city were you born in?? or ?What is the name of your pet?? 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 safe. See the [Password lesson](umbrella://lesson/passwords) for more information on how to choose and remember strong passwords.
* Only connect to people you know personally and trust.

# Check the Site's Privacy Policy

Remember that information you post on most social media sites does not belong you ? it is subject to the sites own policies and they can use it or share it with others. We know that reading privacy policies is a near-impossible task, but you may want to take a look at sections on how your data is used, when it is shared with other parties, and how the service responds to law enforcement requests.

Social networking sites often collect sensitive information beyond what you actually post?where you are, what interests and advertisements you react to, what other sites you've visited (e.g. through "Like" buttons). Be aware of what you like and repost if they may put you at risk. It can be helpful to block third-party cookies and use tracker-blocking browser extensions to make sure such information isn't being passively transmitted to third parties.

Some social networking sites, like Facebook and Twitter, have business relationships with data brokers in order to target advertisements more effectively. You can see guides that walk you through how to opt-out of these tracking schemes here:  
? [How to opt-out of Facebook's data broker relationships](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)  
? [How to opt-out of Twitter's data broker relationships](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)

# 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?
* See here for: [How to change your Facebook privacy settings](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)

Remember, privacy settings are subject to change. Be sure to 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.

# Think about what you share

Always ask the questions:

* Who can access the information I am putting online?
* Who controls and owns the information I put into a social networking site?
* What information about me are my contacts passing on to other people?
* Will my contacts mind if I share information about them with other people?
* Do I trust everyone with whom I'm connected?

Be careful about putting too much information into your status updates ? even if you trust the people in your networks. It is easy for someone to copy your information or unintentionally share something.

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have?

# Sharing videos/photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first. As a good rule of thumb, don't post information, images, or updates about people you know if they aren't posting about themselves.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

[Guardian Project](https://guardianproject.info/) has created an open-source app called [ObscuraCam](umbrella://lesson/obscuracam) to detect/select faces on photos and blur them. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

# Check what your friends share about you

Remember that you?re not the only person who can give away potentially sensitive data about yourself. Your friends can tag you in photos, report your location, and make their connections to you public in a variety of ways. You may have the option of untagging yourself from these posts, but privacy does not work retroactively. You may want to talk to your friends about what you do and do not feel comfortable having them share about you in public.

# Think about what you join

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

# Don?t use social media sites for instant chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Never engage in chats with people you don?t know, especially those who want to send you documents or pictures. This is a method commonly used by authorities to put malware in activists? computers.

You should use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the [Sending a Message lesson](umbrella://lesson/sending-a-message) or [Pidgin tool guide](umbrella://lesson/pidgin) to find out how.

## Don?t rely on social media for storage

Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable.

# Access sites securely

Access social networking sites using https:// to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.

Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine.

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Password lesson](umbrella://lesson/passwords)
* [How to opt-out of Facebook's data broker relationships](umbrella://lesson/facebook)
* [How to opt-out of Twitter's data broker relationships](umbrella://lesson/facebook)
* How to change your Facebook privacy settings
* ObscuraCam
* Sending a Message lesson
* [Pidgin tool guide](umbrella://lesson/pidgin)

### FURTHER READING

* + [EFF - Protecting yourself on social networks](https://ssd.eff.org/en/module/protecting-yourself-social-networks)
* [Security in a Box - Social networking tools](https://securityinabox.org/social_networking_tools)