The Complete Guide to Social Media Privacy

Table of Contents

Social media privacy and you

Social media is about sharing.

It's a place where we can communicate our thoughts and feelings, not to mention show off the great things happening in our lives. But sharing these interesting and unique parts of ourselves doesn't mean we have to open up to the point that our privacy is compromised.

The fact is, social platforms are notorious for lax privacy settings that can compromise your privacy in unintended ways. For example, many sites make your personal details public by default, and this information can appear in search engine results. Meanwhile, apps can expose information in hidden ways or collect data, which is later sold to third parties. Even the things you post can make you more vulnerable to outside threats.

With so much at stake, here's a closer look at the top privacy concerns on social media, and how to change your settings on the most popular sites.

The top 4 social media privacy concerns

1. Security breaches

Google the name of your favorite social media site plus the words “security breach,” and you’re bound to find thousands, if not millions, of hits. So, it’s perhaps not surprising that over one in five Americans report having a social media account hacked in 2018. While steps have been taken to provide greater protections on social sites, it’s impossible to know how safe we really are. This leaves it up to us to decide what we’re willing to risk, and what we need to protect.

2. Data collection

Social media companies collect a lot of data. What are they doing with it? The answer is, no one really knows. What is clear is that there’s a lot of buying and selling of our personal data going on behind the scenes. Toss in the fact that everything you do online can be traced back to your IP address, and it’s a recipe for massive privacy invasion. Unfortunately, that’s the hidden price for having access to “free” services.

3. Location-based services

Location-based services and apps are some of the biggest privacy foes. Give a smartphone app permission to access your location data, and you're effectively giving it permission to shadow your every step and move. These apps can track where you work, where you ate lunch, and where you bought a gift for your partner. If that's not bad enough, the app very likely turned around and sold that data to a third party for profiling and marketing purposes.

Given the shocking degree to which we can be surveilled, there's been some rumblings about a "Geolocation Privacy and Surveillance Act" in Congress and the Senate (for years now actually). But until a law like this passes, it's the Wild West as far as geo-tracking goes — and it's not going to stop any time soon.

4. Account hacking

Social media sites are mostly unregulated playgrounds that criminals can target to spread malware and conduct identity theft. With the information they glean from social profiles (names, addresses, workplaces, etc.), they can steal your identity or open lines of credit. Some criminals even monitor social media to keep tabs on people's activities — especially vacation plans — so they can "pay a visit" to a house later.

Controlling your privacy on social platforms

For all of the talk about fixing social media privacy, it's naive to think that it will be fixed, either now or in the future. It's up to us to take back our privacy where we can. Here's how to control your information on four of the most popular networking sites: Facebook, Instagram, Twitter, and LinkedIn.

On Facebook

Facebook offers some fairly robust tools for protecting personal privacy on their site and your Facebook profile on search engines. The bad news is, they're sometimes hard to find. To help you, we've broken down some of the most important settings here.

To lock down your privacy settings:

In the dropdown on the top right, select **Settings**. Using the options on the left **(Privacy, Timeline and Tagging, etc.)**, you can limit who sees your personal information and posts. At a minimum, you should **Limit Old Posts** and set **Do you want search engines outside of Facebook to link to your profile?** to **No**. Both of these settings are located in the **Privacy** section.

To limit the information shown in your profile:

On your personal page, go to the **About** tab. In this section, you can edit and limit the amount of personal information displayed about you. At the bottom of each section, change the default audience (it's **Public** by default).

To change your photo albums privacy:

- On your personal page, go to the **Photos** tab.
- Select **Albums**, then choose the album you want to edit.
- Click the **Edit** button to set the **Privacy** level (it's **Public** by default).

To turn off location services on the Facebook app:*

On Android:

- Go to the home screen.
- Tap **Settings**, then tap **Applications**.
- Scroll through the list and tap **Facebook**.
- Below **Permissions**, tap **Location**, then tap **Location Services** off.

On iOS:

- Go to the home screen.
- Tap **Settings**, then scroll down and tap **Privacy**.
- Tap **Location Services**, then scroll to the Facebook app and tap to set Location Services to **Never**.

To view your location history:

- Go to **Settings** at the top right, then click **Location** on the left.
- View your location history under **View your Location History**. To turn off location services, you'll need to do it from the app.

*Source: How do I turn Location Services on or off for Facebook? https://www.facebook.com/help/275925085769221

LinkedIn

LinkedIn can be a great place to network and even find a job. But even so, you may not want to expose your entire career history to the world via search engines. By default, your public profile is set to on, with many identifying details open to public viewing. Here's how to change it.

To lock down your public profile:

- Go to **Me**, then select **View Profile**.
- Click **Edit Public Profile & URL**
- From the **Public Profile Settings** page, you can turn your profile's public visibility to on or off. Should you choose to leave it on, you can lock down what the public sees (e.g. your education, experience, website, etc.) to make it more private.

Instagram

Facebook owns Instagram, but luckily the privacy settings are much easier to understand here. Like an on/off switch, you can either let the entire public see your photos or just a select list. To edit your photo privacy settings, you must do it from the app (the desktop version doesn't allow it).

To limit who can see your photos:

- On your mobile device, go to your **Profile** page by tapping the icon at the bottom.
- Click the hamburger menu at the top and then **Settings** at the bottom.
- Tap **Privacy** then **Account Privacy**, and turn Private Account on or off (when set to on, only your approved users can see your photos).

Twitter

Most people on Twitter want to reach a public audience. However, if you would prefer to limit your audience to folks you know, you can choose to "protect" your Tweets. By selecting this option, only the people you approve will see your Tweets.

To limit who can see your Tweets:

- Click your user icon, and select the **Settings and Privacy** option.
- Go to the **Privacy and Safety** tab.
- Where it says **Tweets**, you can opt to **Protect Your Tweets**.

Besides understanding your social media settings, we recommend using a strong password for all of your social media accounts (and changing them regularly). We also suggest using encryption software on all of your devices whenever you want greater security and privacy online.

Control is in your hands

At FigLeaf, we don't think you should need to have a law degree to protect your social media privacy.

For that reason, we've created some pretty powerful privacy tools that you can use to protect your identity and activities on the World Wide Web. We strongly believe you should have the power to control how much information you give out at any time — it should always be your choice.

With FigLeaf, the power to take back control is in your hands


figleaf