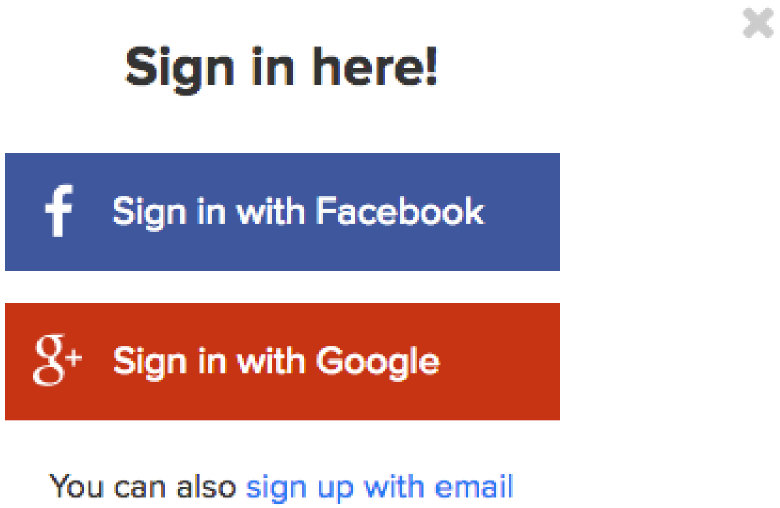
# Signing In Using Social Media Logins

**Author :** Cat

**Date :** February 16, 2015



Sign in here!

You can also sign up with email

If you are like me, you have more online accounts and passwords than you can possibly remember. Every website seems to require a login. When you find yourself needing to sign up for the 59th time, it can be quite exhilarating to be offered the ability to sign on using Facebook, LinkedIn or another network you already have. This seems perfect! No need to re-submit information or create a another password. Now wait a minute, do you know what you are trading for the luxury of one less password? Let's find out.

## How it works

Let's clear up one misconception: When you sign in using a network account you are *not* handing over your network password to the new site. You are allowing the new site to contact the chosen social network site and gain access to your information therein. Let's say you were using Facebook as a log in, you'd select the 'Sign on with Facebook' button and it will pop up a new window with a Facebook address. You are now in Facebook. The URL (website address) should have an 'https' in the front followed by www.facebook.com. You can then enter in your email and password. If the URL is not the site you want, this could be a scam so best not to enter your password here.

If you are already logged in to Facebook on your computer (ie you never logged out, even if the tab is closed) then you may be presented with your profile photo to click on. At this point, if you login to your Facebook account, you are authenticating with Facebook and giving them permission to work with the new site. In some cases you are granting access to numerous pieces of your information. In other cases, you may also be allowing the new site to post on your behalf. The onus is on you to understand what information or actions you are agreeing to specific to the site or application that wants access.

## Information you are giving away

Each social network has a set of user's information that it gives away to anyone connected. The new site or application (aka third party) can get additional information with the user's permission. According to the rules of the social networks, the third party that connects is supposed to have a clear display about which special information they are requesting. It should be as clear as "we would like to access your friend list" but could be as vague "we will also collect information about you".

The user's age range is almost always passed over by the network to ensure that the appropriate ads are shown. The ranges are usually; Age 13-17 (no adults ads), 18-20 (alcohol for non-US residents) and 21+.

Here is a list of what each major network allows connected apps to see:

### Twitter Sign In

Since Twitter is a public site to begin with, most of what a third party site or app can access is what anyone can see. If you do have a private account, be wary that you are giving this away.

- *Automatic information*: Your bio, followers list, following list, posts, and your profile photo
- *By permission:* Ability to post on your behalf

### Google Sign In

Since Google owns the world's biggest search engine, the biggest video service (YouTube) and one of the biggest email systems (Gmail), they have a tremendous amount of information about your searching, shopping, and viewing habits. Be wary when sign in using Google and check what information the connect site is requesting.

- *Automatic Information*: Your Google+ connection list, user's age range, language, public profile information, email address, your profile photo, and people that you have circled.
- *By Permission:* Personal data such as posts and pictures, search history, YouTube video history, gmail and ability to post on your behalf.

### Facebook Login

Facebook has also become a wealth of insight into personal preferences and demographic information. When a development company uses the Facebook API to create an app that connects with Facebook, they can get the automatic information but much of the special requested info (like user actions or personal posts) has to be reviewed by the Facebook team to make sure third parties are using the information ethically.

- *Automatic Information*: profile photo, location, gender, favourites (that are public), friends list (that are public), followers, relationship status, network and schools attended.
- *By Permission:* user-friends, email address, age, mailbox, analytics on fan pages, likes, actions (shares, comments etc), pictures, posts, and ability to post on your behalf.

### LinkedIn Sign In

LinkedIn should likely contain your least private information but none the less, third parties can take a lot of it.

- *Automatic Information*: first name, last name, unique LinkedIn ID, maiden name, headline, number of connections, industry, last posted item, summary.
- *By Permission:* Additional sections of your profile, company pages you manage, messages (InMail), and ability to post on your behalf.

## When to use it

Every time you use a sign in you are essentially adding that company or app as a 'friend' to your account. Ask yourself, if this third party were a person, would I want them to have access to this information? Do I trust them with it?

I highly recommend that you only connect via another network when you need it. For instance, if you use an app that manages one of your social sites, then you will have to login with the network. One example is a scheduling app, like Tweetdeck or Hootsuite, where the purpose is for that third party app to post updates to your feed on your behalf. If you want to write a comment on the Wall Street Journal website, you do not need to use access via your social sites. In this instance it is better to create a new account or post anonymously.

**Recommendations:**

- **Only connect when you feel it is needed**
- **Think of the third party app like a person. Do you trust them with all your information?**
- **Look for a line detailing what information the network is asking for and make sure you are comfortable with it**
- **Make sure the sign-in screen lists the network URL that you want to access and it uses https**