The hidden Facebook privacy settings you should know about!

Author : Cat

Date : February 12, 2014

If you have a Facebook account then likely you have visited a website and found it already knew something about you. Perhaps you saw a section showing pictures of other people who 'like' that page and some were your friends. Maybe it knew your location. How did the site know that? You never even signed in! You may be giving away more public information than you think. Or your friends may be doing it for you with your permission. Let's investigate.

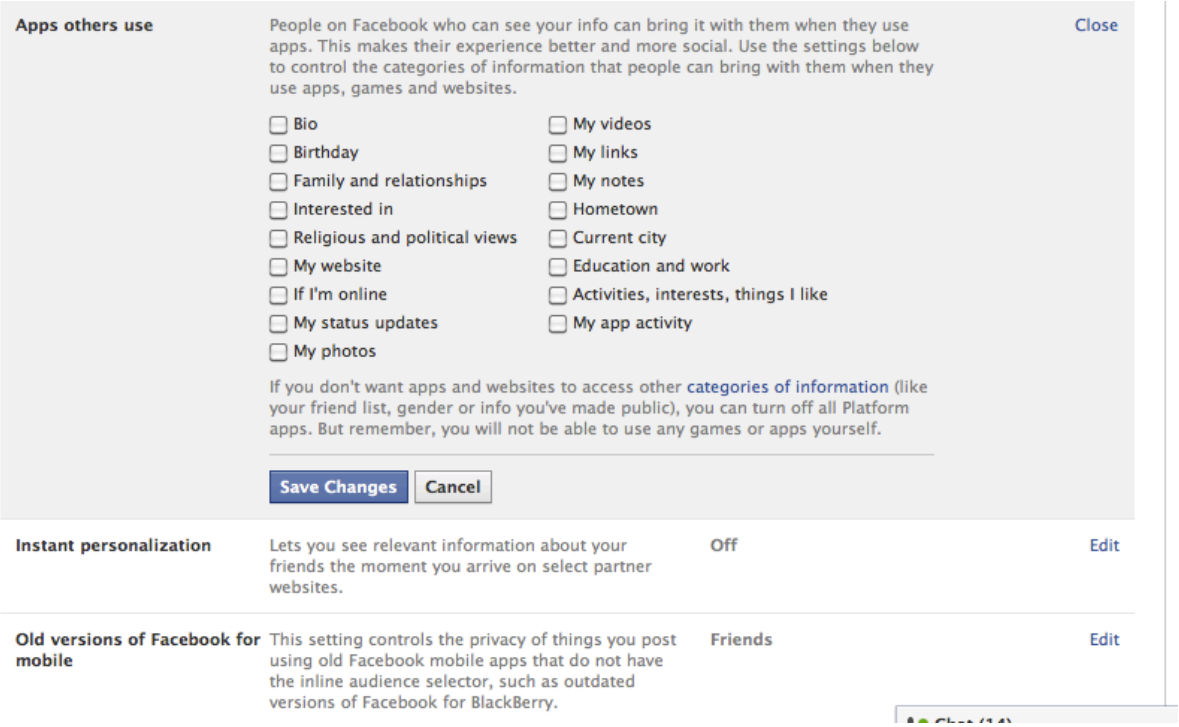
First, you need to know that every Facebook account has 3 pieces of public information: Your name, your profile picture and your Facebook UserID. Your UserID is not publicly tied to your email address or phone number but public sites can access this ID against your picture and name.

Let's say that John Doe and Jane Doe are on Facebook and Jane has user ID 100. John logs in to Travelocity using his Facebook account. Travelocity now has access to John's friend list including the fact that he is friends with User 100. The site records John's name linked to User 100. Later Jill visits the page. Though she has not logged in, her browser knows she is user 100 so it presents her a list of people who like Travelocity and includes John's picture in that list.

App Settings - I agreed to what??

The **Apps Settings** page in Facebook allows you to control how external Apps interact with your data. It also controls how external sites use your data when your friends log in. This is key so I will

repeat it, *even if you have never visited the site, these settings also indicate what a site can take from you via your friend who has signed in.*



- **Apps you use**: Here you will find a complete list of Apps that you have interacted with. If you see any that you do not use or do not remember signing up with then open the App description, delete data associated with the app and remove the app from the list.
- **Apps others use**: This is the area where you decide what information websites and apps can take from you through your friends. Uncheck anything you would not want an outside party to know without your knowledge. My humble opinion: if you have marked the item "Friends" in your profile, likely you do not want it shared outside that circle so probably best to uncheck everything that applies. Make sure to save changes.
- **Instant personalization**: Options here are *on* or *off*. If you want to know all about your friends who have visited this site, you will want this on. Be aware though that you are also permitting the site to look for your Facebook userID and associate any information it can find on your computer with what it has stored on your ID.
- **Old versions of Facebook for mobile**: I am happy to see this feature because it allows you to pick a default audience for posts. Older versions of the mobile app do not allow this choice and everything could be public. A special note for parents, who tend to hand down old devices to teenagers, that this setting should be used. Options here are the standard (Public/Friends/Only Me).

WHAT YOU CAN DO

Make sure you are comfortable with your apps settings. Get to your Apps Settings page by using this link: https://www.facebook.com/settings?tab=applications

Cookies ... and not the chocolate chip kind

In the simplest terms, networks use two main pieces of technology to track what you are doing online.

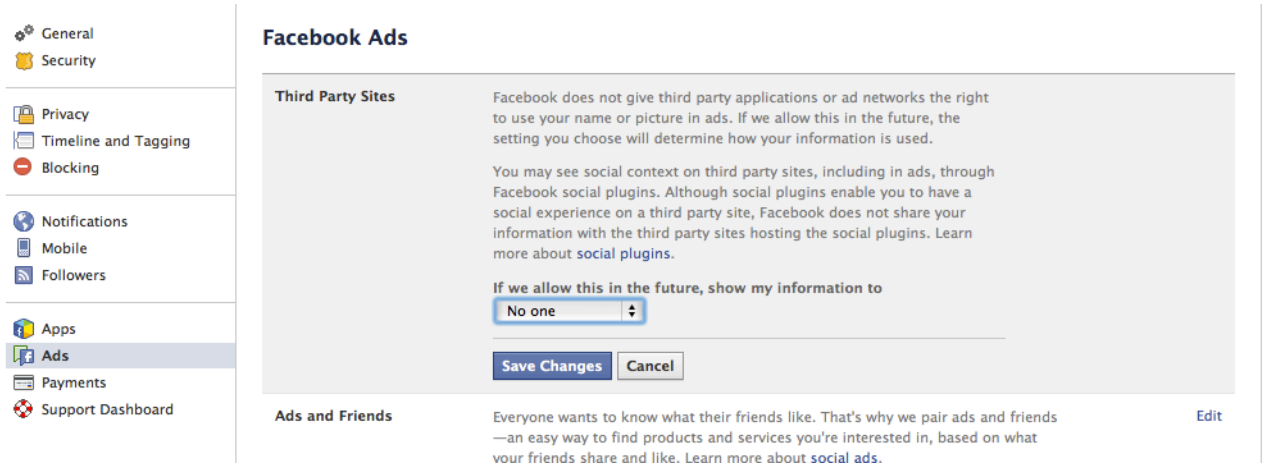
- **Cookies**: Files that contain information about you and your computer use. If you have logged into Facebook in the past on that computer and not subsequently logged out, that cookie (and your User ID) can be shared with any other site you have open.
- **local storage:** Data kept on your computer or device storage for caching (saved views of the websites) for faster loading or offline use.

Networks and their partners will tell you several different reasons why keeping this information is in your best interest:

- For security, to know if someone is doing something that violates the network's terms
- To improve your social experience, give you the information that is relevant to your friends and circles.
- To help Facebook and corresponding companies offer you ads that matter most to you.

These are valid and helpful. I have said before that if I search "winter tires" in Google I would much rather have local stores show up then a random listing. I appreciate ads for items I may actually buy rather than getting ads for diapers and kitty litter. And I would rather stay at a hotel that I know my friend went to and liked. That said, sometimes more information is passed around than I am comfortable with. I went through the cookie list for Facebook. It was typical of a public site - nothing more concerning.

What is worth noting is that Facebook has added a new section in the settings for how they will handle the use of your name and picture for Third Party Sites 'in the event' that they change their policy. You need to opt out or you will be automatically included. That means if you 'like' the fan page for Pizza Hut, which is public, then Pizza Hut could display your picture and/or name on their page.



WHAT YOU CAN DO

For the new Third Party Sites policy, you can find the 'opt out' page under the *Ads* menu (see image above) or use this link:

https://www.facebook.com/settings?tab=ads

The use of cookies have been a part of the web for years so if you enjoy the tailored experience then keep them. If you are uncomfortable with their use, you can chose to disable cookies altogether in your browser settings.

Signing in with Facebook Connect

Rather than creating a new login, some sites will offer a sign-in via Facebook. By using ‘FaceBook Connect’ you are allowing the company you are singing in with to have access to your social information. They like it because it allows them to show your name and picture on reviews and comments. It also allows them to target ads and search results to you. Here is what you are sharing in this case:

- **by default:** location, gender, favourites (that are public), friends list, followers, relationship status, network and schools attended.
- **By requested permission:** email address, activities, status, events, family relationships
- **Request to Post on your behalf**: This requires a separate screen that you OK, but allows the app or site to post messages to your wall or your friend's wall

When you provide information on the new site, it does not pass it back to Facebook. Also, any individuals you may have blocked within Facebook will remain blocked on your connected site.

WHAT YOU CAN DO

When you log into Facebook via these sites, look for www.facebook.com in the address bar to avoid phishing (sites that are looking for your login but are not legit). Only agree to the information and permissions that make sense to that app - some apps ask for far more than they need.

In Summary

- Check your Apps Settings for info you are giving away through friends
- Check your Ads Settings for info you allow third parties to use
- Be aware of what you are sharing when using Facebook Connect