

Making the Most Out of  
Facebook's Privacy  
Settings



# How to Configure Your Account's Privacy Settings

Rik Ferguson, Vice President Security Research



## Making the Most Out of Facebook's Privacy Settings

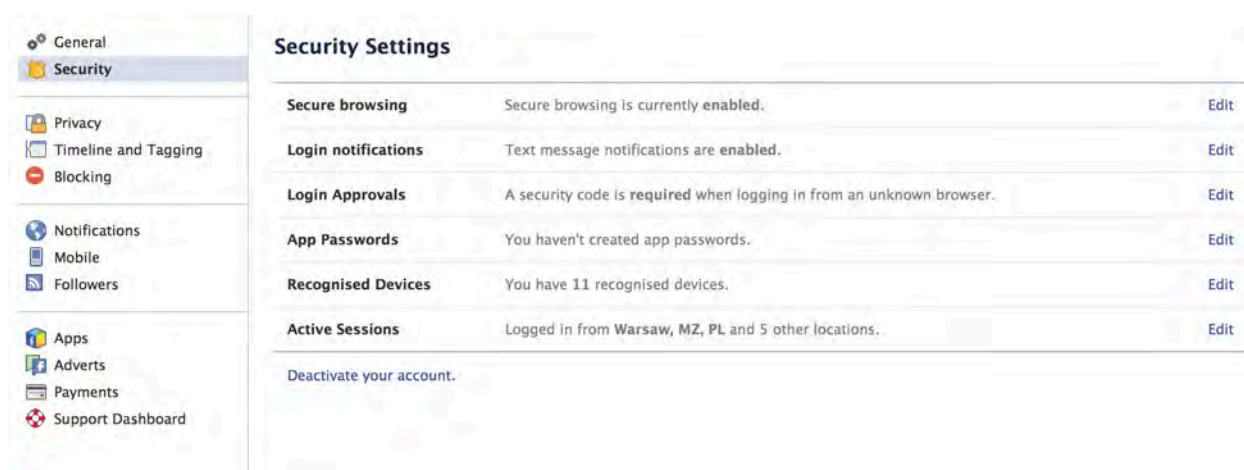
As a result of the constant stream of updates and refinements to Facebook's security settings; I have been receiving ever-increasing amounts of questions from friends, colleagues and *CounterMeasures* readers concerned with how their online privacy can be optimised. So I have put together this guide to **Making the Most of Facebook Privacy in 2013**. Of course the very act of publishing this guide is sure to prompt yet more layout changes and feature enhancements from the biggest social network on the planet, so get it while it's hot!

## Don't Get Facejacked

Facebook has built in some great features to stop even a person who has your password from accessing your account. This stuff isn't new, it's just underused and underpublicized. If you regularly log in from the same device or devices, you can train Facebook to recognize those machines. You can ensure that if someone tries to log in from an unrecognized device you are immediately notified. You can even make that person enter a code that will be sent as an SMS to your registered mobile phone. So unless the snooper has direct access to your PC and to your mobile phone, he/she won't be "facejacking" (or the less salubrious term, "fraping") you. But if he/she does have that kind of access, well, your problems might be bigger than just Facebook.

**To ensure you don't get facejacked, follow these steps:**

- Log in to Facebook and in the top-right drop-down gear wheel menu, select **Account Settings**.
- In the Settings page that appears, click the Security section over on the left hand side. Then make the following changes:



- Click the **Edit** link next to **Secure Browsing** and put a tick in the box. This will ensure that

your communication with *Facebook* is always encrypted when possible and will guard against password-stealing tools like *Firesheep*.

- Under **Login notifications**, select whether you would like an email or text message/push notification whenever an unrecognized device tries to access your account.
- Under **Login approvals** tick the box to have a security code sent to your mobile device, follow the on-screen instructions depending on whether you use an Android, iPhone or other device and you're all set. Even if someone knows your password, he/she still won't be able to log in without the security code.

## Turn on Security Codes

Activate Code Generator to get security codes on your phone. [?]

1. Open the Facebook app on your phone
2. Tap the menu button in the top left corner
3. Scroll down and tap **Code Generator**
4. Tap **Activate**

When Code Generator is activated, click **Continue**.

[Having trouble?](#)

**Continue**

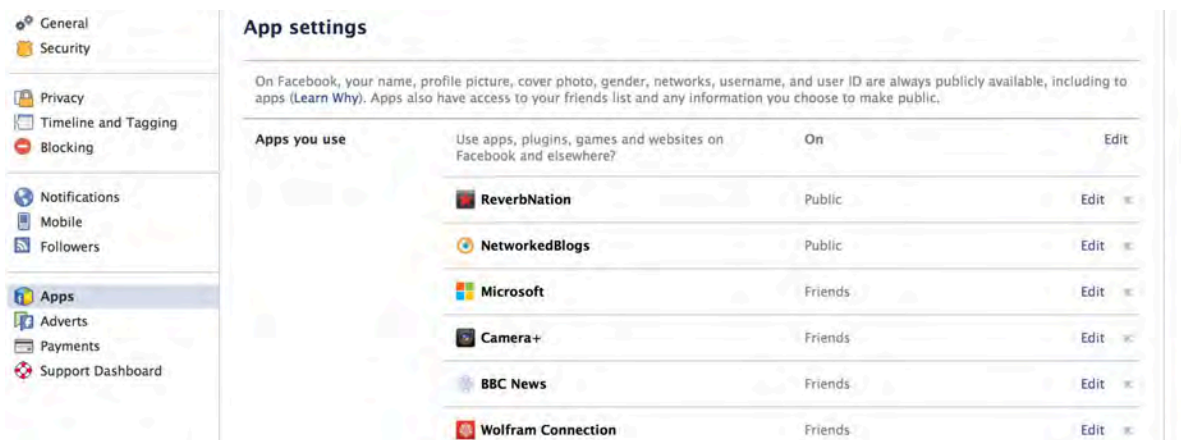
**Cancel**

## Lock Out Leakage

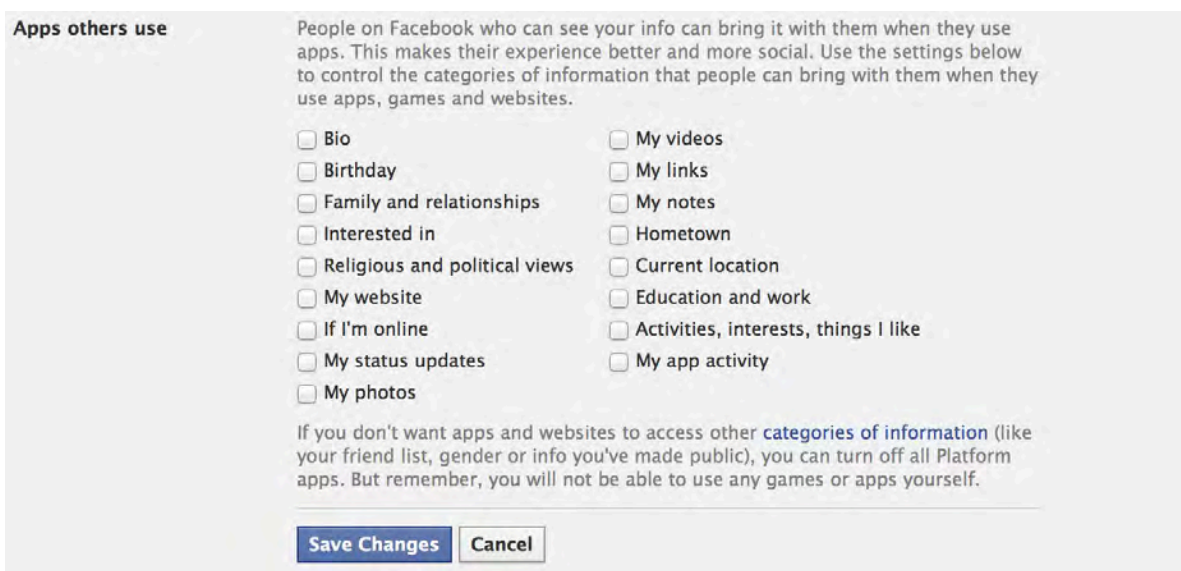
With that out of the way, let's go on to tweak your account and privacy setting to better protect the content you share and control the audience with whom you share it. Let's look at **Account Settings** which can be accessed through the drop down menu on the top right of your *Facebook* page.

## Apps

In this menu you should review the individual permissions that you have allowed the Apps that you have installed. Have a first pass through this list and remove any apps you no longer use. Then review individual permissions by clicking the **Edit** link next to each remaining App. Some permissions are required for an App to work but many optional permissions can be revoked here. At the same time, ensure that the App itself is not giving out too much information by changing the setting **Who can see posts and activity from this app** to **Friends** unless you have specific Apps that you wish to grant greater visibility.



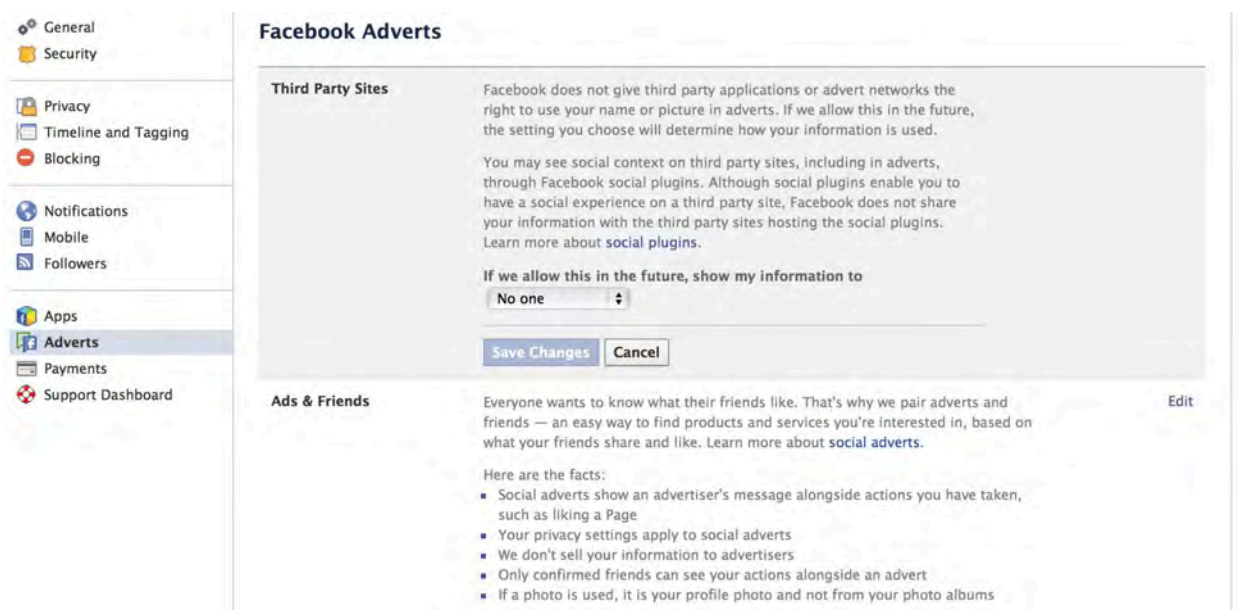
The section **Apps** others use controls how much information from your profile is visible to Apps that your *Facebook* friends may have installed. I think you'll be unpleasantly surprised by just how wide open this leaves your information to unknown third parties, and recommend that you deselect every tick box in this section



Finally, in the *Old versions of Facebook for mobile section*, ensure that you set the default sharing for new posts to *Friends* only, just in case.

## Adverts

The *Facebook Adverts* section controls how your data, **including your name and photo**, may be shared now or in the future with third party sites and apps. Modifying these settings means that you can safeguard your data from future commercial use as much as possible. Change the *Third Party Sites* and *Ads & Friends* settings to *No one*.

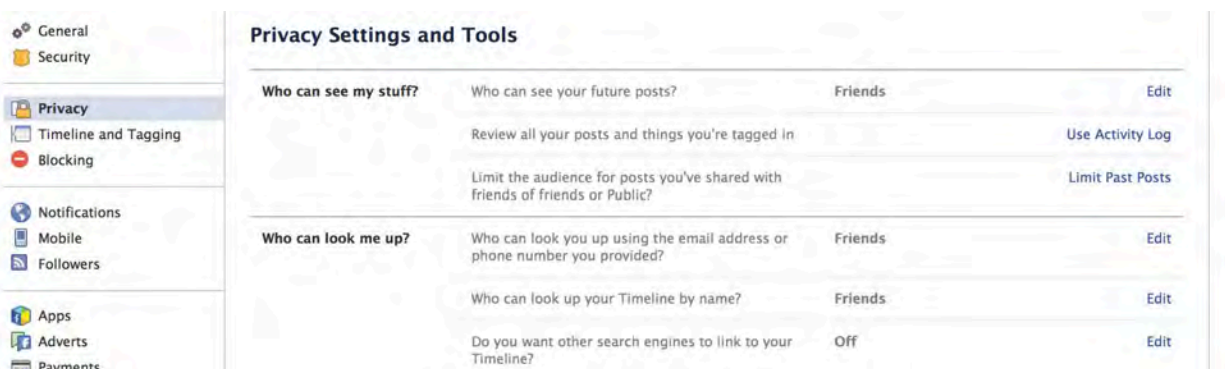


The screenshot shows the Facebook Adverts settings page. On the left is a navigation menu with options: General, Security, Privacy, Timeline and Tagging, Blocking, Notifications, Mobile, Followers, Apps, Adverts (highlighted), Payments, and Support Dashboard. The main content area is titled "Facebook Adverts" and is divided into two sections:

- Third Party Sites:** Explains that Facebook does not give third party applications or advert networks the right to use your name or picture in adverts. It offers a dropdown menu to select how information is shared in the future, with "No one" selected. There are "Save Changes" and "Cancel" buttons.
- Ads & Friends:** Explains that everyone wants to know what their friends like, so Facebook pairs adverts and friends to help find products and services. It includes a list of facts:
  - Social adverts show an advertiser's message alongside actions you have taken, such as liking a Page
  - Your privacy settings apply to social adverts
  - We don't sell your information to advertisers
  - Only confirmed friends can see your actions alongside an advert
  - If a photo is used, it is your profile photo and not from your photo albums

## Protect Your Privacy

The changes to *Facebook* have radically changed the ways in which we can share content with our friends, friends of friends and the general public. There are two main ways to configure this privacy; when you post through the *Facebook* interface or when you post through a device or App that doesn't allow per post privacy settings. To configure these settings select **Privacy Settings**, which is accessed through the same drop down menu as previously.



The ***Who can see your future posts*** setting in the ***Who can see my stuff?*** section controls which audience your new posts will be shared with by default. I recommend setting this to **Friends**, the default setting here is **Public**. You have to remember though, if you change this setting on a per post basis at the time of posting an update, **Facebook will remember your choice and use it as the new default** in this section and for every subsequent post until you manually change it back.

While you're in this section, it's a good idea to hit the **Limit Past Posts** link, then the **Limit Old Posts** button, to ensure that any information you may have inadvertently over-shared in the past is now restricted to just your Friends.

***Who can look me up?*** controls how visible your profile is to people who are not already friends of yours, restricting these settings to **Friends** means that only people to whom you are already connected will be able to find you in search results. It certainly locks down the visibility of your profile, but it kind of defeats the object of a social network, where one of the aims is to be able to make new connections. I would recommend opening these up to at least **Friends of Friends**, if not **Everyone**. There is one little gotcha here, which the more observant of you may notice, comparing the screen shot above and the one on the next page. Opening up the setting ***Who can look up your timeline by name?*** is a one way ticket. If you had this locked down in the past, as I did, then **changing the setting will remove this option from your settings permanently**.



Finally, under ***Do you want other search engines to link to your timeline?*** make sure you disable this functionality, stopping any of your content inadvertently appearing in other people's search results.

## Timeline and Tagging

This section controls who can post to your timeline, who can see certain specific content on your timeline and how the audience for certain posts may be expanded.

Unless you don't want to allow anyone at all to post to your timeline then ***Who can post to your timeline?*** should be left at the default setting of ***Friends***. If for any reason you want to silence your timeline for a while, changing this setting to ***Only Me*** will ensure that you get no incoming posts, from anyone.

***Set Review posts friends tag you in before they appear on your timeline?*** to ***On***. This does not stop you from being tagged in posts and those posts and tags will still appear in others' searches, news feeds, tickers and other timelines if they are connected to the originator or to someone else tagged in the post, but they won't appear on your own timeline until you approve them. By default this is turned off.

***Who can see posts you've been tagged in on your timeline?*** should be restricted to ***Friends*** unless you're entirely at ease with your friends being able to tag you in a post and that part of your timeline being shared with a wider audience than your own posts, possibly including people you do not know at all. ***Who can see what others post on your timeline?*** exerts a similar control but this time over posts that do not contain a mention of you. The same restrictions should apply, ***Friends*** only.

***Review tags people add to your own posts before the tags appear on Facebook?*** is a sneakily important setting. Remember, when any person is tagged in a post, they and possibly their friends will be able to see the content of that post, whether they are connected to you or not. For this reason it is

wise to enable the reviewing of tags before they are added to *Facebook*, it maintains your control over the audience for your posts. Set this to **On**.

**When you're tagged in a post, who do you want to add to the audience if they aren't already in it?** represents the other side of this equation, here you need to decide whether posts in which you are tagged are further shared with your own friends, even if they are not connected to the original poster. I can't give you any better advice here than, think carefully about the kinds of posts your friends enjoy tagging you in before you select either **Only Me**, or **Friends**. If you chose **Only Me**, then no one other than the original audience for the post will be able to see it.



## Lists - Control privacy when you post

Use the *Facebook* lists feature to divide your friends into lists. This is a great for protecting your privacy because it allows you to select an individual audience for each one of your posts, be aware though it is not possible to specify the audience for your “Likes”

*Facebook* offers three default lists; **Close Friends**, **Acquaintances** and **Restricted**, dividing friends between **Close Friends** and **Acquaintances** will influence how much or how little they show up in your news feed. Adding a friend to the **Restricted** list means they will only be able to see content that you make **Public**. *Facebook* has also introduced the concept of Smart Lists, these could be related to where you live, where you work, or where you went to school for example.

If you add a friend to any of the **Close Friends**, **Acquaintances** or **Restricted** lists, they will not be informed. However, be aware that if you add a friend to a Smart List that is related to a place of work or college for example, they will receive a notification that you have done so and will be able to



approve that information for posting to their own timeline. You can also create custom lists and again your friends will not be notified if they are added to these lists. It is worth noting that when you share content with a specific custom list of friends, your friends will not see the name of the list you have shared it with, if you choose to share with a Smart List, the name of the list will be visible. In addition, the audience in both cases **will see that you have chosen a restricted audience for your post and they will be able to see every individual name in that group.**

## Followers

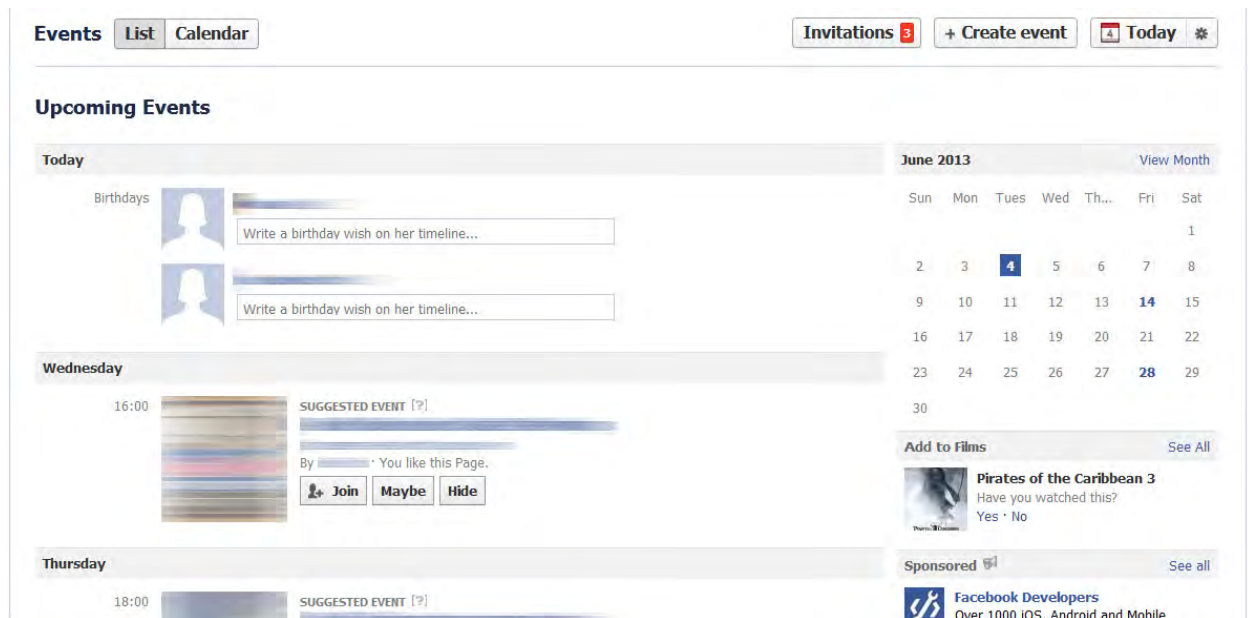
Following allows you to follow the public activity of someone on *Facebook*, without having to add them as a friend. Of course this means that the possibility exists for people to follow your content, without you having *accepted* them as a friend as well. It's one more reason to tightly control your privacy on *Facebook*. For example, default behaviour on *Facebook* if you unfriend someone who is also following you, is that they will remain a follower and able to see any public content and perhaps content that is shared by mutual friends too, unless you do something about it. If you want to enable or disable the permission for other users to subscribe to your content, this is also controlled from the same settings screen as previously, in the *Followers* section.



## Events

Any **Public** event you have responded to will feature on your timeline and will be shared with the public, meaning that *anyone* viewing your *Facebook* timeline will be able to see these events. To hide these events from your timeline, view your timeline by clicking your name in the top right of your browser, click the **Activity Log** button and select **Events** from the activity type list that appears on the left of your screen. You may then hide any events you wish from being displayed on your timeline; your attendance at these public events will still be visible to anyone on the event page itself.

The same rule also applies to any other activity type in the list, if the original activity is public, your reaction to it will also be public, even if you do not allow it on your own timeline.



### Check yourself out!

If you want to check how the changes you have made have affected the information you share you can view your own timeline as another Facebook user would see it, or as it is visible to the general public.

To do this, select the downward pointing arrow just to the right of the **Activity Log** button on your own timeline, select **View As...** Your initial view will show you how you look to the general public, people who are not your friends.

If you want to see how a specific person sees your timeline, click **View as specific person** in the top left and type that person's name. This is a great way of identifying those last few pesky events, photos, videos or stories that may still be publicly visible. You can then find each unique event in your **Activity Log** and refine the audience to whom it is visible or remove it entirely from your timeline.

## 5 rules to remember

1. If you post on someone's wall then you cannot control the privacy of your post. The visibility of the comment is defined by the original post which may be less restrictive than you want, for example, **Friends of Friends**.
2. If you restrict the audience of a post in order that certain friends cannot see it that restriction should not be considered final. If someone later posts a comment that tags a *Facebook* user who was not a part of the original audience, then the entire thread and original post will be visible to that person. Be careful what you post.
3. If you post on, or respond to an invitation to a public event or a public page; you cannot control the privacy of your post. You can only hide it from your timeline after the post has been made.
4. If you post on a friends wall where *their* privacy setting is **Friends of Friends**, then any of *your* friends who are on your **Restricted** list will be able to see that post, because **they are your friends**.
5. This means that anything you post which is **Public** or **Friends of Friends**, either by your own settings or those of the recipient, may show up in the ticker of people you do not necessarily know, have restricted or have unfriended.



Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

• TREND MICRO (EMEA) Ltd  
• IDA Business & Technology Park  
• Model Farm Road , Cork  
• Ireland

©2013 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. .