MAKING THE MOST OUT OF
FACEBOOK'S PRIVACY SETTINGS
HOW TO CONFIGURE YOUR ACCOUNT'S PRIVACY SETTINGS

Rik Ferguson

A 2011 Trend Micro White Paper
Since the long list of new features recently unveiled has begun to be rolled out for all Facebook users, I have been receiving an ever-increasing number of questions from friends, colleagues, and CounterMeasures readers concerned with how their online privacy may be affected. So I put together this guide to help them make the most out of Facebook’s privacy settings in 2011. I referred to the forthcoming Facebook feature, Timeline a lot in this guide but don’t be fooled, as these settings are available right now even if you haven’t enabled Timeline yet.

**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 (if you’re logged in). 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 won’t get facejacked, follow these steps:

1. Log in to Facebook and in the top-right drop-down Account menu, select Account Settings.

2. In the Settings page that appears, click the Edit link next to Account Security. Then make the following changes:
   - Tick the box to enable secure browsing. 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 SMS 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 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.

**Lock Out Leakage**

With that out of the way, let’s go on to tweak your account and privacy settings to better protect the content you share and to control the audience you share it with. Let’s look at Account Settings, which can be accessed through the drop-down menu at the top-right corner of your Facebook page.
In the *Apps* menu, you should review the individual permissions that you have allowed for the apps that you have installed. Have a first pass through this list and remove 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 for *Who can see posts and activity from this app* to “Friends” unless you have specific apps that you wish to grant greater visibility to.

Meanwhile, in the *Facebook Adverts/Ads* section, change the third-party and social adverts/ads sharing settings to “No one” from the default option, “Only my friends.”
**Protect Your Privacy**

The changes to *Facebook* have radically changed the ways in which we can share content with our friends, with our friends’ friends, and with the general public. There are two main ways to configure your account’s privacy settings—when you post through the *Facebook* interface or when you post through a device or through an app that doesn’t allow per-post privacy settings. To configure these settings, select *Privacy Settings*, which can be accessed through the same previously mentioned drop-down menu.

The default privacy settings only apply to posts made through the *Facebook* interface or through an app that doesn’t support inline-sharing controls. I recommend changing this to “Friends” from “Public.”

In the succeeding parts of this guide, I will go into more detail on some of the more specific settings to control how you share information and, perhaps more importantly, how information about you is shared.
To better protect your privacy, let’s take a more in-depth look at each Privacy Settings option.

**How You Connect**

Change the settings for *Who can look up your Timeline by name or contact info*, *Who can post on your Timeline*, and *Who can see posts by others on your Timeline* to “Friends” from “Everyone.” The default setting for this last option is “Friends of friends,” which has been the cause of much of the oversharing in the ticker that upset so many Facebook users.

Your settings for *Who can send you Facebook messages* and *Who can send you friend requests* are just a question of how easy to contact you want to be based on your personal preference. The default setting for this again is “Everyone.”

**How Tags Work**

- **Set Timeline Review to “On.”** This does not stop you from being tagged in posts. Those posts and tags will still appear in others’ feeds if they are connected to the originator or to someone else who has been tagged but they won’t appear on your Wall/Timeline until you approve them. By default, this is turned off.
- **Set Tag Review to “On.”** When someone tags your content, you must review it before it is posted. This is useful because once a person is tagged in a picture, a post, or a comment, both that person and his/her friends can see the content, which you may not want to share more widely. By default, this is turned off.
- **Set Maximum Timeline Visibility to “Friends.”** This controls the maximum extent of who can view posts to your own Timeline. Don’t forget that this content may have initially been posted on someone else’s Wall/Timeline and you can’t restrict the visibility of the original post. By default, this is set to “Friends of friends.”
- **Set Tag Suggestions to “Off.”** This feature will suggest your name when someone uploads a picture that Facebook thinks looks like you. By default, this is turned on.
- **Set Friends Can Check You Into Places to “Off.”** That way, you’re not going to get checked in to a place you would rather have kept secret or even to some place you never went to. By default, this is turned on.
Apps and Websites

The *Info accessible through your friends* section controls which content about you can be accessed by apps that your friends may have installed. Deselect every check box in this section. You will find that by default, almost all of them are allowed.

*Instant personalization* shares Facebook data with certain partner websites. If the option is available, uncheck the box to turn it off. If it is greyed out, it means that it is not yet available for your account. Note that it is turned on by default so try to remember to keep an eye on it because you are not able to turn it off until the feature is already enabled for your account.

If you’ve been following the recommendations so far, the *Public search* feature should already be turned off because you changed your settings for *Who can look up your Timeline by name or contact info* to “Friends.”

Limit the Audience for Past Posts

To limit the audience for your past posts, click *Manage Past Post Visibility* then click *Limit Old Posts*. This will ensure that any post you have made in the previous years on Facebook will be restricted to “Friends.” Unfortunately, no indicator tells you whether you have previously done this. So, if you’re unsure, just do it again.

**CONTROL YOUR PRIVACY WHEN YOU POST**

Lists

Use *Facebook’s Lists* feature to divide your friends into categories. This is a great feature to protect your privacy because it allows you to select an individual audience for each of your status updates or *Wall* posts. Remember though that it is not possible to individualize the audience for your *Likes*:

*Facebook* offers users three default lists—“Close Friends,” “Acquaintances,” and “Restricted.” Dividing your friends between “Close Friends” and “Acquaintances” will influence how much or how little they show up in your *News Feed*. Adding someone 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*, which could be related to where you live, where you work, or where you went to school, among others.

If you add a friend to any of the “Close Friends,” “Acquaintances,” or “Restricted” lists, they will not be informed. Note, however, that adding people to a *Smart List* that is related to a place of work or to where you took up college, for example, will notify them that you have done so. They will be able to approve that information for posting to their own *Timelines*.

You can also create custom lists. Your friends will not be notified if they have been added to these lists. It is worth noting, however, that when you share content with a specific list of friends, they will not see the name of the list you shared it with but they will see that you have chosen a restricted audience and will be able to see every individual name in that group.
Subscriptions

Subscriptions is a new Facebook feature that allows you to follow the public activities of people on Facebook without having to add them as friends. This means that the possibility exists, if you have subscriptions enabled, for people to follow your content without need for your acceptance as friends as well. It’s one more reason to tightly control your privacy on Facebook. For example, even if you de-friend someone on Facebook, he/she will remain subscribed to content you post and will be able to continuously see public content about you. This content may include information your mutual friends share unless you do something about it. If you want to enable or disable the permission for other users to subscribe to your content, go to your Timeline and click the arrow to expand the view of your Favorites boxes. You will see the Subscriptions box, click the box and you will be able to either click the Allow Subscribers box or better yet a Settings button, which will let you turn it off.

Events

Any “Public” event you have responded to will appear on your Timeline and will be shared with the public. This means that anyone viewing your Facebook profile will be able to see these events. To hide them from your Timeline, view it, click View Activity and select Events from the activity type drop-down menu that appears on the right. You may then hide any event you wish to from your 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 seen by another user. This will let you see what is visible to the general public. To do this, select the downward pointing arrow to the right of View Activity. Select View As... and type the name of the friend whose account you want to use to view your profile or click the Public link. This is a great way to identify 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.
**Five Rules to Remember**

1. If you post on someone’s Wall, you can’t control the privacy of your post. The visibility of the post is defined by your friend’s privacy settings. The same is true for your comments on other people’s posts. The visibility is determined 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 so that certain friends can’t 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, 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 post something on a public page, you can’t control the privacy of your post. You can only hide it from your Timeline after it has been made.

4. Posting something on a friend’s Wall if his/her privacy setting is set to “Friends of friends” allows any of your friends, even those in your Restricted list, to see that post because they are your friends.

5. Anything you post using the setting “Public” or “Friends of friends” (either by your own settings or by those of the recipient) may show up in the ticker of people you do not necessarily know, have restricted, or have de-friended.