Tighten your Facebook privacy settings

By Scott Mace

In their hunt for market dominance, social networks Facebook, Google Buzz, and Microsoft Live are redefining what *social* means — and in the process, straining the bounds of personal privacy.

Facebook, the big daddy of these three, has made quiet changes to its privacy settings, ones that members need to understand if they are going to manage the distribution of their personal information.

I find Facebook useful, mostly as a way to stay in touch with a select set of my friends and former co-workers. It's not my public soapbox nor a window into my personal life, left open to the world — for that, I have blogs and Twitter.

As much as I like Facebook, it has a flaw that I'll never see in my blogs and hopefully never see with Twitter. It seems the proprietors of Facebook find it necessary, desirable, or profitable to change member privacy settings, usually with little notice to members. In every case I can think of, privacy settings have become more relaxed — more open, if you will.

What's beneficial for Facebook, however, is not necessarily good for members — their personal information might end up in places they never intended. The world is filled with marketers who would love to know increasingly more about you. And if that doesn't concern you, the world also contains stalkers and hackers who might use that personal information toward evil ends.

You should take your Facebook (or any other social network) privacy as seriously as you do protection from malware on your PC.

Keep in mind that all the big social networks continually tweak privacy settings. This is not just a Facebook problem.

Review and lock down your Facebook settings

In a typical good news–bad news scenario, Facebook's privacy settings have become more granular over time — and consequently far more tedious and complicated to manage. Even more irritating is that, as Facebook adds new categories of settings, it often uses **Everyone** as the default. (And **Everyone** means just that — not only all Facebook members, but anyone viewing associated sites).

New Facebook members are especially likely to give out private information unintentionally. Working through a slew of privacy settings is not foremost in their thoughts as they first build their new Facebook wall. Unfortunately, that means they get the default, wide-open Everyone privacy setting.

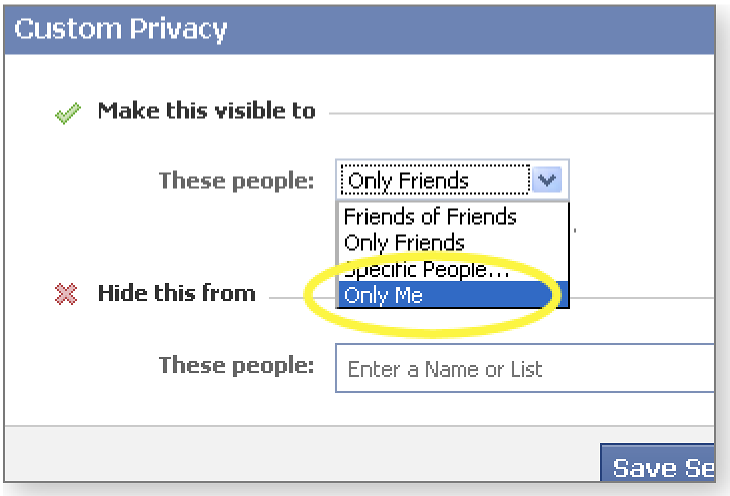
When deciding what personal information to share, you have two choices. Either don't put it on Facebook to begin with (no, you don't have to fill out every personal information field), or put it up but restrict who can see it.

Start with the simple setting for personal info

If you're going to post information you don't want the whole world to see, or if you just want to generally tighten up your privacy settings, start with the following:

- **Personal Information and Posts:** Most settings in this section default to Everyone or Friends of Friends. For a balanced level of privacy, I recommend selecting either Only Friends or Only Me, depending on your comfort level.

  Here, Facebook makes things difficult for new members. Initially, the settings dropdown list does not contain Only Me. You must select Customize and then Only Me from another dropdown list — ***for each privacy setting.*** (See Figure 1.)

  Custom Privacy

  ✓ Make this visible to

  These people: Only Friends

  ✗ Hide this from

  These people: Enter a Name or List

  Figure 1. If you want to use Facebook's most-restrictive setting, Only Me, you must go into custom settings.

  Furthermore, some of these settings affect the level of your friends' privacy when they interact through your wall. For example, when a friend posts a comment on your wall, **Posts by Friends** controls who else can see that post — everyone, friends of friends, and so on.

- **Contact information:** Facebook tightens its default settings for direct-contact information to Only Friends, but if you don't care to share your IM screen name, mobile or other phone number, or current address, change it to Only Me.

  The last three settings on the Contact Information page — **Website, Add me as a friend,** and **Send me a message** — are all preset to Everyone by default.

  If you include your Web site URL on your wall but don't want it showing up on a search engine list, consider adding a robots.txt file at your Web site. (Instructions for creating this file are contained on the robotstxt.orgs site.)

- **Friends, Tags, and Connections:** This section controls what information people see on your profile, and the options are relatively simple. Items such as Friends, Family, Relationships, and Photos are set to Only Friends by default, and that's probably how you'll want to leave them.

  Some information (such as your Pages and list of friends) is still public and can be accessed by Facebook applications you and your friends use.

  Facebook Pages offer a convenient way to stay on top of your favorite interests from within your profile page. The key is to carefully consider which Pages you choose to ***Like*** and which applications you agree to run.

  Liking a Facebook Page is different from, liking a post, photo, or link. When you ***like*** a Page, Facebook automatically subscribes you to a feed from that page — which often represents a commercial product or company.

Manage the murky realm of Facebook applications

How your privacy is kept or lost when using Facebook applications is probably the least-understood and most-worrisome aspect of this social network. The privacy controls for apps are found in the **Applications and Websites** section.

To put it simply, don't run Facebook applications if you don't want to distribute personal information beyond your friends. The following example shows what happens when you run an application. I'll use Farmville, a popular game application, as an example.

When you first run Farmville from within Facebook, all your profile information and photos, your friends' info, and ***other content it requires to work*** is pulled into the Farmville system. You have only two choices: Allow this to happen, or leave the application. If you let it happen, a vast amount of your personal information is now governed by Facebook's privacy policies ***and*** by Zynga's — the company that owns Farmville. Those policies may differ.

According to Zynga's privacy policy, it ***generally*** doesn't collect personally identifying information; in any case, it can collect only what you provide.

Bottom line: Each new application you link to in Facebook could add another layer of privacy management. This could be another argument for not posting sensitive information where it's not fully under your control.

Facebook applications have no middle ground — if you run an app, you're automatically sharing at least some information. You can't run an application just for yourself, as you would a spreadsheet or database. For this reason, I subscribe to few of them.

The most-important app settings fall under **What your friends can share about you through applications and websites.** By default, nothing can be shared except your name, sex, and profile photo — plus any information that fell under the Everyone option in the other privacy categories. I leave all boxes unchecked.

Should you choose to run Facebook applications, consider changing the **Activity on Applications and Games Dashboards** control's default setting from Only Friends to Specific People, or even to Only Me.

If you don't want to show up in the search results of unknown Facebook members, tighten the Search setting from Everyone to Friends of Friends or Only Friends. Unchecking Public Search Results also helps keep unknown Web surfers at bay.

Aside from the obvious anti-stalker benefit Block List enables, it also has a Preview My Profile button that displays how most Facebook members see your profile. It gives a good view of how tightly you're locked down.

New privacy leaks from Instant Personalization

Recently, Facebook opened up Instant Personalization, another way for strangers and outsiders to view your personal information. Currently, there is a setting at the bottom of the **Applications and Websites** page called Instant Personalization Pilot Program. If you opt into this ***service,*** selected Facebook partner Web sites can instantly personalize their applications, based on your personal information.

This list of partners is constantly expanding. Even if you opt out of Instant Personalization, your Facebook friends might still share Facebook information about you if they opt in. As far as I can tell, your only recourse is to block each of the application sites.

This could mean going to each apps page and clicking on Block Application, if it even exists. So far, the apps include the recommendation service Yelp.com, Microsoft Docs.com (a Web-based document creation and sharing system), and the music-streaming service Pandora.

No wonder so many Facebook users are annoyed. If Facebook adds dozens of these apps within the next month, a significant investment in time will be necessary just to tighten up these newly loosened controls.

For the tightest privacy, you should log out of Facebook before visiting these or any other Web sites partnering with Facebook through Instant Personalization. It's certainly inconvenient to monitor whether you're logged into Facebook, but people who wish to share as little personal information as possible with these third-party sites are force to take these steps.

Other resources:

http://zesty.ca/facebook/ "What does Facebook publish about you and your friends?," shows you what — if anything — public Internet users can see of your Facebook activities. It's a useful tool for managing the personal information other members are allowed to view. **Click on your profile picture to get your ID Number**