

Security Alert

The Paranoid's Guide to Facebook

BY LOGAN KUGLER

OVER HALF A billion people use Facebook. It's the largest phenomenon of human connection in history, not to mention the biggest thing on the Web. But even though we love using Facebook and other social networks, we hate the privacy and security drawbacks.

Here are some steps that you can take to keep your information private on Facebook.

Five Steps to Privacy

1 Disable Facebook Places:

Using Facebook Places has benefits. But when you broadcast your location, you expose vulnerabilities, inviting an ill-intentioned person to swoop in.

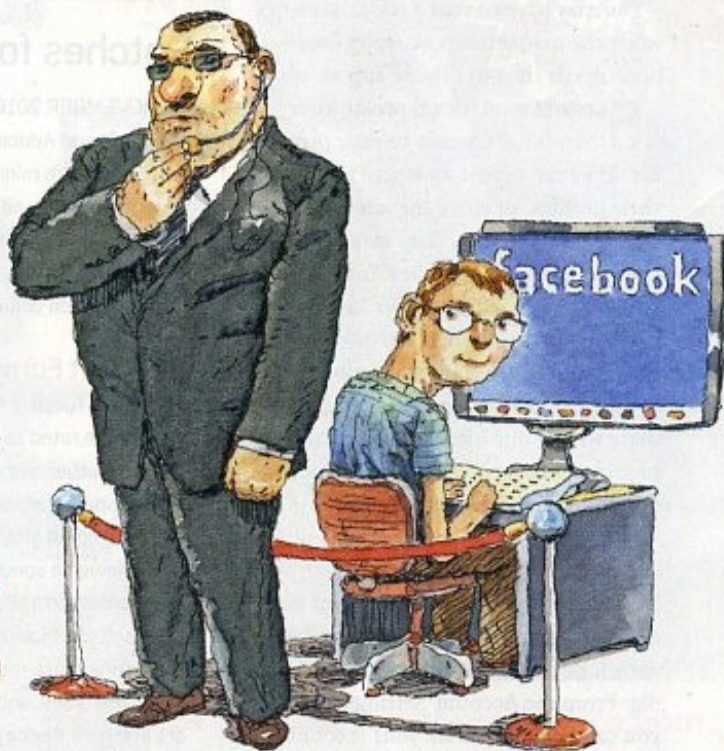
If you use Facebook Places, note that the defaults let "Everyone" see your profile—which means everyone on the Internet. Go to the *Account* tab and select *Privacy Settings*. From there, indicate who should and shouldn't see your profile, and how much others may see when you upload comments and images.

To disable Facebook Places entirely, first log in to Facebook and pick *Privacy Settings* from the *Account* drop-down menu. Click *Customize settings*. The last line under "Things I share" deals with Facebook Places; click *Edit* and select *Disable*. To stop friends from broadcasting your location, scroll to "Things others share"; for the bottom item, click *Edit* and select *Disable*.

2 Control items posted to your profile: Even if you delete your Facebook account (see the final tip), the photos and details you shared with friends can still lurk on Facebook or the Internet at large. When in doubt, don't post it—but if you do, control who sees your items by using the lock feature.

Before clicking *Share*, click the drop-down menu above and select who can see the post: *Everyone*, *Friends of Friends*, *Friends Only*, or *Customize*. The last setting will let you block individual friends irrespective of your general choice.

Facebook knows who your friends are, what you like, where you live, and what you buy. Our advice will help you secure your personal information.



3 Hide your app activity: Some games on Facebook reward players for recruiting friends. And some games and apps post messages to your wall so friends see what you've been up to (when you first run the app, you agree to the terms and conditions that allow it to do this). The posts can be a nuisance to your friends. Besides, do you really want them to know that you've been playing FarmVille all day?

Head to the *Privacy Settings* page. At the bottom left, under "Applications and websites", select *Edit Your Settings*. Below "Game and application activity", select *Custom* from the drop-down menu. Choose *Only Me* in the dialog box.

4 Disable Facebook apps: All Facebook apps can access your profile information. Facebook's policy is that app developers cannot use personal data off-site and may access only sufficient data to enable the app to run, or to "enrich" your experience. But once an app has access to personal information, it's up to the developer to keep the info safe.

If you don't like that policy, block apps. Select *Privacy Settings* under *Account*, and click *Edit your settings* under "Applications and websites". Below "Applications you use", select *Turn off all platform applications*. In the alert box, choose »

ILLUSTRATION: JOHN CUNEO

PCWORLD.COM

Reactions to Facebook Messages are mixed, with privacy concerns yet again coming to the fore. But the new e-mail service may help in the fight against online fraud. Read more at find.pcworld.com/71055.

Select all and click *Turn Off Platform*.

You may have to wait a few minutes while the new settings activate; Facebook needs time to disable app access.

5 Control what friends reveal: Your friends have access to your profile. They can repost your wall items to their profiles, or share the info, without your knowledge. They may also be using apps that access their friend lists.

Click *Privacy Settings* under Account. Go to 'Applications and websites', and click *Edit your settings* and *Info accessible through your friends*. Deselect items to share when your friends allow apps to access your profile; for full privacy, deselect everything (recommended).

The Last Resort: Deletion

Eliminating your Facebook account may be worthwhile if you no longer find it useful. But to deep-six it, you have to dig: From the Account Settings page, you can only deactivate your account, which makes it merely dormant—your profile still exists, in hibernation.

If you want to obliterate the account, the process takes 14 days, and once it's initiated you cannot use your account. The link to permanently delete your account is buried in Facebook's Help pages, at find.pcworld.com/71057. Click *Submit*, fill out the form, and click *OK*. Then leave the site, never to return.

Delete my account

Permanently delete account

You are about to permanently delete your account. Are you sure you want to do this?

If so, fill in the following:

Password

Security Check
Enter both words below, separated by a space.
Can't read the words below?
Try different words or an audio CAPTCHA.

the Klondos concerns

Text in the box:

ERADICATING YOUR FACEBOOK account is fairly simple—once you find the way to do so.

BUGS & FIXES

JAMES MULROY

Patches for Rich-Text E-Mail, Acrobat Holes

IN NOVEMBER 2010, both Microsoft and Adobe had it fairly easy, with minimal security threats and updates. The Patch Tuesday update that Microsoft released on November 9 was one of the company's smallest patch collections for the year.

Rich Text Format Flaw

The Patch Tuesday release brought only one update rated as critical; Microsoft rated the other two as important. The critical update, MS10-087, addresses a flaw that could affect you if you opened or previewed a specially crafted Rich Text Format e-mail. RTF is a Microsoft-developed format that lets you use multiple fonts, text sizes, and colors in e-mail messages. If you open an RTF e-mail that has malicious code, the attacker could gain the same rights on your PC as a local user.

The two important updates correct vulnerabilities in Microsoft Office and in the Forefront Unified Access Gateway, which permits secure remote access to corporate networks for personnel. The most dangerous of these vulnerabilities could allow remote execution and/or elevated privileges for the attacker.

The Patch Tuesday fixes apply to all supported editions of Office XP and newer for Windows; PowerPoint 2002 and 2003; Office 2004 for Mac; PowerPoint Viewer 2007 Service Pack 2; and Forefront Unified Access Gateway 2010.

As usual, you should install these patches as soon as possible through Windows Update. To learn more about each fix, as well as to download them manually, visit find.pcworld.com/71109.

Adobe Reader, Flash Updates

Recently Adobe released three critical security updates for its Adobe Flash Player, Flash Media Server, and Adobe

Plus: Apple's updates for Mac OS X and iOS fix a wide range of security issues.

Reader and Acrobat software products.

Vulnerabilities in Adobe Flash Player, Reader, and Acrobat could cause the apps to crash, and could allow an attacker to take control of your computer. Meanwhile, a bug hidden in Flash Media Server could permit an attacker to run malicious code on an affected system.

The updates affect Adobe Flash Player 10.1.85.3 and earlier for Windows, Mac, Linux, and Solaris, plus Flash Player 10.1.95.1 for Android. Also affected are

Flash Media Server 4.0 and earlier for Windows and Linux;

Reader 9.4 and earlier for Windows, Mac, and Unix; and Acrobat 9.4 and earlier 9.x versions for Windows and Mac.

Be sure to grab the latest editions of Adobe Flash Player, Media Server,

Reader, and Acrobat, using automatic update checks. Visit find.pcworld.com/71107 for the latest version of Flash Player, and go to find.pcworld.com/71108 for Flash Media Server updates. For Reader and Acrobat, select *Check for Updates* from the Help menu to get the most recent versions.

Apple's Bumper Crop of Fixes

Apple has released updates that apply to Mac OS X, as well as to iOS for iPhone, iPad, and iPod Touch. The Mac OS X 10.6.5 update addresses over 130 vulnerabilities, 55 of which involve the bundled version of Adobe Flash Player. See find.pcworld.com/71110 for more information about the patch.

The iOS 4.2.1 update also comes packed with plenty of security fixes—and it offers several new features for iPad owners. Browse to find.pcworld.com/71111 to learn more about iOS 4.2.1, and be sure to snag both Apple updates.

