



July 2010

## Get security advice you can use at:

<http://www.sans.org/newsletters/ouch/updates/>

### In This Issue:

- Safer Social Networking
- Patches and Updates Roundup

[Editor's Note (Wyman): The number of Facebook users has surpassed 400,000,000, dwarfing its sibling MySpace, and making it No. 1 of the Top Ten social networking sites worldwide with a 55% market share. (1) While the world has fallen in love with Facebook, its popularity is not without problematic consequences. For example, psychotherapists and Facebook users alike talk openly about being

addicted to Facebook (2), and a recent study suggests that 21% of women ages 18-34 get up to check Facebook in the middle of the night (3).

Articles about Facebook tips and tricks are proliferating (4), as are lawsuits alleging, among other things, that Facebook's operators misappropriate its users' personal information for commercial purposes and change users' security and privacy settings arbitrarily. German authorities are looking into Facebook's practice of saving information about people who do not even use the site. (5) Facebook is illegal in China (6), has been outlawed for blasphemy in Pakistan (7), taken Africa by storm along with Colombia, Argentina, Venezuela, Mexico, and Chile (8), and recently opened an office in Moscow (9).

Any online organization with nearly half a billion members worldwide is bound to be the subject of curiosity, controversy and mythology, as well as a too-good-to-pass-up target for hackers, crackers, spammers and scammers. This month we offer some security tips for safer social networking with special attention to Facebook.]



## Safer Social Networking

---

**Think about how you want to use social networking.** Facebook is an all-purpose, come-as-you-are social medium. The community is gigantic, and anybody with an email address can join. It's best to limit your use of Facebook to sharing news, photos, music, videos, etc. casually with friends and family. For business, consider using a service like LinkedIn that caters specifically to professionals.

**Follow the Golden Rule.** Assume that the personal information and photos you display are available to everyone and anyone, not just to your friends.

**Do not display your full birth date.** Listing a full birth date – month, day and year – makes you an easy target for identity thieves who can use it to obtain more of your personal information and potentially gain access to bank and credit card accounts. Choose to show only the month and day, or even better, no birthday at all.

**To protect children from online predators, do not post a child's name in a photo tag or caption.** If someone else does, delete it if you can, or ask the member who owns the photo to remove the name.

**Do not mention being away from home.** Doing so is like putting a "Nobody's Home" sign on your front door. Be vague about the dates of your travel plans and vacations.

**Restrict searches for your information.** Find out what your options are for restricting public searches. At a minimum, you should be able to prevent your information from being searched for by anyone other than your designated online friends.

**Do not permit youngsters to use social networks unsupervised.** Most sites limit membership to ages 13 and older, but children younger than that find ways to use them anyway. If there's a young child or teenager in your household using Facebook, an adult in your household should become one of their online friends and use their email as the contact for the account in order to monitor their activities.

**Think about whom you are allowing to become your online friend.** Once you have accepted someone as your online friend, they will be able to access a lot of information about you, including photographs and other material you have marked as viewable by your friends. Find out if and how you can remove a friend in case you change your mind about someone or discover they aren't who they claim to be.

**Make sure you have an up-to-date web browser and comprehensive security software on your computer.** This includes anti-virus, anti-spyware, anti-phishing, and a software firewall.

**Adjust your privacy settings to help protect your identity.** Facebook and some other social networking sites provide options to protect you online, but it's up to you to understand what they do and how to use them, and to be aware that they change over time.

**Set and review your privacy settings regularly.** Familiarize yourself with the site's current privacy policies. For example, with the latest changes in May 2010, Facebook forces some of your information (e.g., your name, profile picture, gender and the networks to which you belong) to be publicly accessible.

**Make only a cut-down version of your profile visible to everyone.** Reveal the rest of the information in your profile only to people you choose to have as online friends.

**Disable options, and then add them in one by one.** If you are using a social network just to keep in touch with people, consider turning off the bells and whistles you don't need or use. Disable unfamiliar options until you understand what they do and have decided that you do need and want them.

**Join groups and networks cautiously.** Assume that all members of a group will be able to see all of your information unless and until you restrict access to it deliberately.

**Understand what happens when you quit the site.** It's usually easy to deactivate your account, but some sites, like Facebook, will retain all your information including pictures, friends, etc. even if you do. Find out how you can delete all of your information. You may have to request that the operators of the site delete it for you. When quitting Facebook, you *must* submit a deletion request, and that, too, comes with some gotcha's.

- There will be a delay of unspecified length between submitting your delete request and the actual deletion.

- If you login to Facebook after submitting your request, your deletion request will be cancelled automatically.
- There's no easy way to confirm that your deletion request has been completed.
- Even after deletion, copies of your photos may remain on Facebook servers for technical reasons.

#### More Information:

<http://www.takesontech.com/?p=16952>

[http://www.facebook.com/security?v=app\\_7146470109](http://www.facebook.com/security?v=app_7146470109)

<http://www.sophos.com/security/best-practice/facebook/>

<http://www.makeuseof.com/tag/the-complete-guide-to-facebook-privacy/>

<http://learn.linkedin.com/what-is-linkedin/>

#### Notes:

- (1) <http://www.marketingcharts.com/categories/social-networks-and-forums/>
- (2) <http://www.cnn.com/2009/HEALTH/04/23/ep.facebook.addict/index.html>  
<http://newsfeed.time.com/2010/07/08/its-time-to-confront-your-facebook-addiction/>  
<http://blog.guruofnew.com/featured-home/seven-signs-you-may-be-ready-for-a-social-media-detox>
- (3) <http://mashable.com/2010/07/07/oxygen-facebook-study/>
- (4) <http://www.hongkiat.com/blog/20-facebook-tipstricks-you-might-not-know/>
- (5) [http://www.mediapost.com/publications/?fa=Articles.showArticle&art\\_aid=116330](http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=116330)  
<http://www.betanews.com/article/Class-action-suit-in-Canada-only-the-latest-of-Facebooks-woes/1278621631>
- (6) <http://www.utilitycomputing.com.cn/china/facebook-blocked-in-china>
- (7) <http://www.asianews.it/news-en/Facebook-blocked-by-blasphemy-regulations-18452.html>
- (8) <http://www.rnw.nl/africa/article/facebook-taking-africa-storm>  
<http://www.examiner.com/x-30835-South-America-Headlines-Examiner~y2010m3d22-Facebook-increase-productivity-and-popularity-in-Latin-America>
- (9) <http://en.rian.ru/world/20100409/158494575.html>

## Patches and Updates Roundup

### **Operating Systems/Applications**

Windows & PC Office: <http://update.microsoft.com> &  
<http://www.microsoft.com/securityupdates/bulletins/201004.aspx>

Mac Office:

<http://www.microsoft.com/mac/help.mspx?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033>

OS X: <http://support.apple.com/kb/HT1338>

iPad: [http://www.ehow.com/how\\_6256127\\_update-restore-apple-ipad.html](http://www.ehow.com/how_6256127_update-restore-apple-ipad.html)

iPhone/iPod: <http://support.apple.com/kb/HT1414>

iPod: <http://support.apple.com/kb/HT1483>

Windows Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

OS X Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh>

Flash Player: <http://get.adobe.com/flashplayer/>

Firefox: <http://www.mozilla.com/en-US/firefox/update/>

Safari: [http://www.ehow.com/how\\_2033324\\_update-safari.html](http://www.ehow.com/how_2033324_update-safari.html)

Opera: <http://www.opera.com/>

Chrome: <http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95414>

Java: <http://www.java.com/en/download/manual.jsp>

Windows iTunes: [http://www.ehow.com/how\\_2016273\\_update-itunes-pc.html](http://www.ehow.com/how_2016273_update-itunes-pc.html)

OSX iTunes: [http://www.ehow.com/how\\_2016270\\_update-itunesmac.html](http://www.ehow.com/how_2016270_update-itunesmac.html)

### **Security Suites**

Symantec: <http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713>

Norton:

[http://www.symantec.com/business/security\\_response/definitions/download/detail.jsp?gid=n95](http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95)

McAfee: [http://www.mcafee.com/apps/downloads/security\\_updates/dat.asp](http://www.mcafee.com/apps/downloads/security_updates/dat.asp)

Kaspersky: <http://www.kaspersky.com/avupdates>

AVG: <http://free.avg.com/us-en/download-update>

Panda: <http://www.pandasecurity.com/homeusers/downloads/clients/>

PC Tools: <http://www.downloadatoz.com/pc-tools-internet-security/smart-update.html>

BitDefender: <http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>

Avast: <http://www.avast.com/download-update>

Webroot: <http://support.webroot.com>

Trend Micro: <http://esupport.trendmicro.com/Pages/How-to-update-Trend-Micro-Internet-Security-Pro-2010.aspx>

Microsoft Security Essentials: <http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx>

Copyright 2010, SANS Institute (<http://www.sans.org>)  
Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller  
Email: [OUCH@sans.org](mailto:OUCH@sans.org)  
OUCH! Security Information Service: <http://www.sans.org/newsletters/ouch/updates/>  
Download the formatted version of the OUCH!: <https://www.sans.org/newsletters/ouch>  
Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. We request that redistributions include attribution for the source of the material.