

In This Issue

1. *Consumer Awareness: The Dark Side of Social Networking* – 2. *Scams and Hoaxes* – 3. *Microsoft and Apple Security Updates* – 4. *Security Newsbytes*

1. The Dark Side of Social Networking

If you are not already engaging in social networking, statistics indicate you will be soon. Visits to social networking sites now account for 10% of the total time people spend on the Internet, according Nielsen Online. Two-thirds of Internet users in the U.S., Europe, Brazil and Australia visit social networking or blogging sites. Internet users total almost 156 million in the U.S. alone. Add in over 29 million in the United Kingdom and over 25 million in Brazil, and the numbers are just too large for the Bad Guys to ignore.

Ordinary Internet users have fallen in love with social networking. While the amount of time users spent on MySpace decreased from April 2008 to April 2009, the use of Facebook increased by 700% and of Twitter by 3,700% during the same period. Cybercriminals love social networking sites, too, because they have to remain easily accessible in order to grow their memberships. That means social networkers are in effect attending an open party where just about everybody is welcome, and who knows if anybody is watching the door.

The openness of these sites is an invitation to the Dark Side. No email verification is required, for example, when new users set up a Twitter account. It's hard to imagine an easier system in which to create counterfeit accounts. Social networking sites rely on a username and a password for security, which means that anyone who finds out your username and password can gain access to your account, assume your online identity, use it mischievously or maliciously, and leave you with little, if any, control over the situation. Until social networking site security evolves with time and improves by necessity, here are 12 Tips for Safer Social Networking.

- **Think about how a social networking site works before deciding to join it.** Some will allow only a defined community of users to access posted content; others allow anyone and everyone to view postings. Don't join any social network that asks you to share your address book or contacts.
- **Always think before you click.** Be wary of visiting the blog or webpage of other members because that other "member" may be a scammer, whose blog or webpage has been rigged to deliver a drive-by download of malware to your computer. If you think you have clicked on the wrong thing, contact your local computer support staff, your Internet Service Provider, or a computer consultant knowledgeable about security.
- **Don't click on shortened (or "condensed") URL's,** like those created by TinyURL and Bit.ly. There's no telling where these links lead to, and that makes it

easy to funnel you to malicious websites. Watch out for "misspelled" links, like www.yuotube.com. Could be a typo or a trick.

- **Keep control over the information you post.** Consider restricting access to your page or postings to a select group of people, like friends, members of your team, your community groups, or your family.
- **Keep your information to yourself.** Don't post your full name, or any personal information about yourself or about anyone else. Be cautious about posting information that could be used to identify you or locate you offline, such as where you work or work-out.
- **Make sure your screen name doesn't say too much about you.** Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues and figure out who you are and where you can be found.
- **Post only information that you are comfortable with others seeing — and knowing — about you.** Many people will see your page or postings, including the people who will be interviewing you for a job five years from now.
- **Remember that once you post information online, you can't take it back.** Even if you delete the information from a site, older versions are stored on other people's computers and may be archived for years by Web search services.
- **Think hard before posting your photo.** It can be altered and broadcast in ways you may not be happy about. If you do post one, ask yourself whether it's one you'd include in your professional resume. Posting pictures of children invites exploitation and could expose them to real-world danger.
- **Flirting with strangers online could have serious consequences.** Some people lie about who they are; you never really know whom you're dealing with.
- **Be wary if a new online friend wants to meet you in person.** Do some research about them. If you decide to meet them, be smart about it: meet in a public place, during the day, accompanied by friends you trust.
- **Trust your gut if you have suspicions.** If you feel threatened by someone or uncomfortable because of something online, report it to the police and to the operators of the social networking site. You could end up preventing someone else from becoming a victim.

More information: <http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm>
<http://www.pcmag.com/article2/0,2817,2348052,00.asp>
http://en-us.nielsen.com/main/news/news_releases/2009/june/time_on_facebook
<http://www.technewsworld.com/story/67366.html>

2. Scams and Hoaxes

New Phishing Attacks against Facebook Users

Cybercriminals have again launched attacks against Facebook to attract account holders to fake websites by sending phishing emails so they can capture usernames and passwords. The new attacks include sending a message to the victim's Facebook inbox and an email notification entitled "Hello" or "Hi" to the Facebook user's "real world" email address. The phishing emails, designed to appear to come from friends of the targeted Facebook account holders, contain text and a URL prompting them to visit a fake Facebook page where the phishers steal their login credentials.

More information: <http://www.spamfighter.com/News-12588-Symantec-%E2%80%93-New-Phishing-Attacks-Against-Facebook-Users.htm>

Friend Stranded in Foreign Country Scam Emails

You receive an email from a friend or colleague claiming that he or she is stranded in a foreign country and desperately needs your help to get home. The email originates from the friend's real email account and may even include the same email signature that your friend usually uses when emailing you. The emails can be a clever scheme by Internet criminals designed to trick people into sending them money. Be wary of any email that you receive that asks you to wire money, even if the message appears to come from a friend.

More information: <http://www.hoax-slayer.com/stranded-scam.shtml>

Enter your PIN In Reverse to Call Police?

This spam email claims that if criminals force you to withdraw money from an ATM, entering your PIN in reverse will automatically alert police. The technology that makes this possible exists, but banks have not implemented it. If you are ever forced to withdraw money from an ATM against your will, co-operate fully and let law-enforcement pursue the matter. There is little chance the reverse-PIN technology will be installed.

More information: <http://www.hoax-slayer.com/reverse-pin-ATM.shtml>

Web Sites Offer Bogus Swine Flu Products

The U.S. Food and Drug Administration (FDA) released another warning about bogus flu products that are targeting consumers via websites. The FDA has issued more than 50 warning letters to offending websites, and 66% of those have removed the offending claims or products. Examples include: a shampoo that claimed to protect against the swine flu virus, a dietary supplement that claimed to prevent infants and young children from contracting swine flu, a "new" supplement that claimed to cure swine flu infection in 4-8 hours, a spray that claimed to leave a layer of ionic silver on your hands that killed the virus, and several tests to detect the virus not approved by the FDA.

More information: <http://www.newsinferno.com/archives/6935>

[Editor's Note (Wyman): Everyone can help stem the tide of email scams by reporting them to the Federal Trade Commission at <http://www.ftc.gov/spam/>.]

3. Microsoft and Apple Security Updates

Microsoft and Apple provide free security updates for their software products.

Windows: Microsoft issues patches for all Microsoft products on the second Tuesday of each month as well as out-of-cycle patches on any day of the month. The next scheduled release date is July 14th. This is a good occasion to check manually, a practice that you should follow once every two weeks, to make sure all of the updates have been installed.

More information: <http://www.microsoft.com/athome/security/default.aspx>

OS X: Updates are issued frequently, and their contents may differ depending on which processor is in your Mac (PPC or Intel).

More information: <http://support.apple.com/kb/HT1338>

iPhones & iPods: Must be updated manually:

<http://docs.info.apple.com/article.html?artnum=305744>

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

4. Security Newsbytes

Apple Releases Fix for Six-month-old Java Vulnerability in Leopard and Tiger

At long last, Apple has released a patch for a six-month-old critical vulnerability in Mac OS X that could allow attackers to install data-stealing malware on users' computers when they visit an infected website. The released patch fixes the Java flaw in Leopard as well as the updated version of Tiger.

More information:

http://blogs.computerworld.com/os_x_patch_now_available_for_critical_java_bug

http://support.apple.com/downloads/Java_for_Mac_OS_X_10_5_Update_4

Twitter Message Could be a Cybercriminal at Work

Spain-based anti-virus maker Panda Software has been monitoring an onslaught of links with malicious software on Twitter that tag hot topics such as the Air France crash, the NBA finals, "American Idol" runner-up Adam Lambert, and the new iPhone 3GS. Cybercriminals have been targeting Twitter users by creating thousands of messages (tweets) with words involving trendy topics and embedded malicious URL's.

More information: <http://edition.cnn.com/2009/TECH/06/21/cyber.crime.internet/>

Microsoft's MSRT Takes Aim at Phony Anti-Virus Program

Microsoft's Malicious Software Removal Tool (MSRT) has been updated to detect a generic type of fake antivirus program known as "Win32/InternetAntivirus." The Microsoft Malware Protection Center gives Win32/InternetAntivirus an alert level of severe. The software is a rogue program that displays false and misleading alerts regarding malware, in order to convince users to purchase rogue security software. In addition, the rogue program runs a password stealer called "TrojanSpy:Win32/Chadem."

More information: http://news.cnet.com/8301-1009_3-10261851-83.html

Phony Anti-Virus Program Takes Aim at Microsoft's MSRT

Security researchers at Computer Associates are warning about a newly unleashed fake anti-virus program that pretends to be Microsoft's MSRT (Malicious Software Removal Tool). A fake anti-virus planted on a user's computer displays a message that says that Microsoft's MSRT has been installed and the user needs to click on the message so that

the scanning process can start. Pressing the “Finish” button causes another window named “OEM Purchase Center” to appear that offers lifelong licenses at discounted prices for products like McAfee Total Protection 2009, Norton SystemWorks 2009, Norton Internet Security 2009, and Norton 360. The “licenses” are not genuine. When users try to cancel out of the window, another bogus warning will display insisting that they purchase a license in order to protect their computers.

More information: <http://www.spamfighter.com/News-12609-Phony-Antivirus-Poses-as-Microsoft-MSRT.htm>

Malware Targets Macs and PC's Alike

Security company Sophos has Internet users on the alert for booby-trapped websites. Sophos has identified two new malware attacks that target Mac OSX with the malware OSX/Jahlav-C and OSX/Tored-Fam. Mac users visiting a rigged site receive a pop-up message that indicates a “Video ActiveX Object” needs to be installed. Users who follow the instructions end up with an infected Mac. Windows users are equally vulnerable. The booby trap identifies visitors’ operating systems (whether the web browser is running on Mac OS X or Windows) and implants malware specifically designed for PC’s.

More information: <http://www.spamfighter.com/News-12607-Sophos-Identified-Porn-Site-Malware-Targeting-Mac-Users.htm>

Copyright 2009, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Alan Reichert, Walt Scrivens, Barbara Rietveld, Alan Paller. 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. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.