

In This Issue

1. Security Myths – 2. Phishing 3. Hoaxes -- 4. Virus Alerts – 5. Microsoft and Mac Security Updates 6. Security Newsbytes

1. Security Myths

Myth: "I don't have to worry about viruses and worms because I have a Mac."

Truth: Macs with OSX are microcomputers, just like PC's with Windows XP, and the two are getting more alike every day. Macs are just as vulnerable to malware as PC's, but since Macs remain less numerous than PC's, they have been a "smaller target". This is changing. Not only is there a growing number of OSX viruses and worms in circulation, Mac users also face threats from "cross-platform" malware and software bugs that affect both OSX and Windows. Case in point: the recent rash of Firefox security holes, the latest of which has been dubbed "impossible to patch."

What to do: Always use high-quality, anti-virus software on your Mac and keep it up-to-date. Apply patches and updates regularly and promptly (See Section 5 below).

More information: <http://www.securityfocus.com/infocus/1695> & <http://software.silicon.com/security/0,39024655,39162882,00.htm>

Myth: "If I don't open any attachments, my computer won't get infected."

Truth: Modern email messages consist of more than just a text message and the occasional attachment. Email messages are often composed in HTML. That makes the message a webpage, complete with graphics, pictures, links, and scripts. Those eye-pleasing graphics and pictures can camouflage all manner of nasties, and clicking on the embedded links can take you on a phishing trip or tempt you to download malware, and invisible scripts can unleash their mischief as soon as you open the email. And the attachment? That's just the sucker punch!

What to do: Always use high-quality, anti-virus software and keep it up-to-date. Apply patches and updates regularly and promptly (See Section 5 below). If you use Outlook, activate the Junk E-mail Filter, which also provides protection against phishing emails.

More information: <http://office.microsoft.com/en-us/outlook/HP052429671033.aspx>

2. Phishing

Banking Scams

The Consumer Reports National Research Center estimates that people lost \$630 million in 2005-06 to phishing scams. Phishing emails are sent to thousands of people every day. Many are made to look like they're from banks and credit unions. The bogus emails tell recipients that their account information needs to be updated and ask them to go online to provide bank account, credit card, or Social Security numbers and passwords or PIN codes. Don't take the bait. Below is a list of banking institutions whose account holders have been recent targets of email scams.

Abbey Bank
Central Credit Union of Florida
CFCU Community Credit Union
Chase Bank
Energy Capital Credit Union

Halifax Bank
Military Bank of America
National City Bank
Nationwide Building Society
Wells Fargo Bank

More information: <http://www.trendmicro.com/en/security/phishing/overview.htm> &
<http://www.millersmiles.co.uk>

More Phishing

Subject: "CONGRATULATIONS !!! You have been chosen by the eBay Motors Inc. to take part in our quick and easy 5 question survey."

Bait: A phony email, allegedly sent from security@ebay.com, offering you a \$20 credit if you will click on the embedded link and answer some questions presented on a spoofed eBay webpage. The email claims that "the information you provide us is all non-sensitive and anonymous."

More information: <http://www.millersmiles.co.uk/report/4427>

Subject: "Dayne Jackson has just sent you 68.00 USD with PayPal"

Bait: A phony email, with British accent, allegedly sent from service@paypal.co.uk, enticing you to collect US \$68 by clicking on the embedded link and providing personal information on a spoofed website.

More information: <http://www.millersmiles.co.uk/report/4423>

3. Hoaxes

Subject: National Cellphone Directory

Now in its third year and going strong, this hoax is the offspring of the National Do-Not-Call Registry. Various emails warn cell phone owners they must register cell phone numbers to prevent release to telemarketers, who will bombard them with costly calls, even if they don't answer. This would be awful, if only it were true. FCC rules prohibit telemarketers from using automated dialers to call cell phone numbers.

More information: <http://www.snopes.com/politics/business/cell411.asp>
& <http://www.ftc.gov/opa/2005/04/dnc.htm>

4. Virus Alerts

Ransomware - Holding Your Files for Ransom

While still in its infancy and easily defeated at the moment, this ugly child of crime surfaced on the Internet in 2006 and is likely to appear in a neighborhood near you in 2007. Some examples: Archiveus, a Trojan, which locked the "My Documents" folder on the infected computer behind a 30-digit password. Victims were instructed to buy drugs from an online pharmaceutical website to retrieve the password. CryZip imprisoned files in a password protected zip file and demanded payment of \$300 for their release. Ransom A, warned victims that a file on the infected computer would be deleted every 30 minutes unless \$10.99 was wired to the scammers in exchange for an unlock code.

More information: <http://www.scambusters.org/ransomware.html>

Australian Prime Minister Heart Attack Trojan Email

This email message claims that the Australian Prime Minister, Mr. John Howard, has been stricken with a heart attack and is in serious condition in a Sydney hospital. Mr. Howard has not had a heart attack. However, the false message is also a ruse to trick recipients into clicking a link that can download a Trojan onto their computer. The link supposedly opens a page on "The Australian" newspaper website that contains the "latest information on the health of the Prime Minister". However, clicking on the link will automatically download a Trojan before displaying a genuine "404 - Page not found" page. Thus the user may believe that there was a harmless error in the link supplied, and not realize that a Trojan has been installed, which allows a hacker to control the infected computer and to harvest sensitive information.

More information: <http://www.smh.com.au/news/security/howard-heartattack-email-carries-virus/2007/02/20/1171733729115.html>

5. Microsoft and Mac Security Updates

Microsoft and Apple provide free security updates for the Windows and Mac OS X operating systems.

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 March 13th.

More information: <http://www.microsoft.com/technet/security/current.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://www.apple.com/support/downloads/>

Security Tips: Be sure your operating system is set to retrieve and install updates automatically. Check manually too, once every two weeks, to make sure all of the updates have been installed.

Windows:

<http://www.microsoft.com/athome/security/update/bulletins/automaticupdates.msp>

OS X: <http://docs.info.apple.com/article.html?artnum=106704> &

<http://docs.info.apple.com/article.html?artnum=301191>

6. Security NewsBytes

Software Makers Swat Daylight Savings Time Bugs Early

Microsoft, Apple, Oracle and Palm appear to be on top of providing free fixes for any clock or calendar bugs that might crop up with the switch to an earlier start for Daylight Savings Time later this month.

More information:

Windows: <http://support.microsoft.com/kb/931836/>

Windows Mobile:

<http://www.microsoft.com/windowsmobile/daylightsaving/default.msp>

OSX: <http://docs.info.apple.com/article.html?artnum=305056>

Oracle: <http://blogs.oracle.com/schan/2007/02/01>

PalmOS: <http://www.palm.com/us/support/downloads/dst.html>

Another Dissatisfied Microsoft Customer

A man awaiting trial for alleged gun crimes is suing Microsoft for privacy violations after FBI agents seized his home computer during a raid and found files containing sexually

explicit videos of him and his girlfriend and evidence that he frequented pornographic Web sites. Michael Alan Crooker, currently in jail in Connecticut, says security features advertised by Microsoft and its business partners should have kept federal agents from accessing the files on his PC. In court papers filed this week in Massachusetts Superior Court, Crooker says he "suffered great embarrassment" as a result of Microsoft's failure to keep the FBI's prying eyes off his computer. He is suing the software maker for \$200,000 in compensatory and punitive damages.

More information:

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197700861>

Hack Attack Forces Texas A&M to Change 96,000 Passwords

Texas A&M University is forcing 96,000 students, faculty, and staff to change their passwords after a hacker attempted a network break-in. Although the hacker attack did not affect financial, payroll, or student administrative systems, the school said, University officials have issued a mandate that all of the users of the school's computer systems change their passwords.

More information:

http://www.darkreading.com/document.asp?doc_id=118529&WT.svl=cmpnews1_1

The Safer Browser?

Two flaws found in the Firefox web browser, which became popular as a more secure alternative to Internet Explorer, could result in users exposing sensitive information to malicious attackers, according to SecuriTeam, an arm of Beyond Security Inc. One of the vulnerabilities, which affects the latest version of the popular web browser (2.0.0.1), could let an attacker fool the software into identifying a website as secure when it should warn that it is a phishing site. This security hole can be exploited by simply adding an extra forward-slash character to a website's address. The second flaw in Firefox 1.5.0.9 could give an attacker the same access rights to files as a user who manually allows pop-ups from a site, thereby granting a malicious individual access to sensitive information stored on the target computer.

More information: <http://www.cbc.ca/technology/story/2007/02/08/tech-firefoxflaws-20070208.html> & http://www.theregister.co.uk/2007/02/26/firefox_update/ & <http://www.mozilla.org/projects/security/known-vulnerabilities.html#Firefox>

An Oldie (But Goodie) Virus Attack Strategy

Researchers at the SANS Internet Storm Center say at least a few hackers have gone old school. ISC handler Kevin Liston writes that some well-known viruses, such as the Trojan-Dropper-Spy Agent and the VBS Solow worm, roaming around the Internet have begun targeting USB removable media, like thumb drives and other storage devices. Johannes Ullrich, chief research officer at the SANS Institute and chief technology officer for the Internet Storm Center, says the viruses are known malware, but their gimmick is that they are focused on unsuspecting targets. If a user's computer is infected with one of them, the malware will look automatically for a device plugged into the USB port. If there's a thumb drive there, for example, it will download itself onto it and wait for the user to click on it and start the active infection.

More information:

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197700818>

Apple Releases Security Update 2007-002

While Apple continues its policy of releasing patches and updates on an "as-needed"-rather than a regular-basis, since summer 2005 the releases have been shaping up to be bi-weekly or monthly. The February 13th release, dubbed "2007-02," plugged holes of varying severity: one in OSX Finder, two in iChat, and one in the UserNotificationCenter.

More information: <http://docs.info.apple.com/article.html?artnum=61798>

Security Tip: Hackers aren't the only threat to your computer.

Food and drink are common causes of computer damage. Try to keep them away from your computer and removable devices. Liquids can be especially damaging to laptops. If a spill occurs, clean up the mess as quickly as possible.

http://www.ehow.com/how_113592_clean-keyboard-spills.html

http://www.ehow.com/how_113626_clean-laptop-spills.html

Copyright 2007, SANS Institute (www.sans.org).

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