

## In This Issue

1. *Security Myths* – 2. *Scams and Hoaxes* – 3. *Malware* – 4. *Microsoft and Mac Security Updates* – 5. *Security Screw-Up of the Month* – 6. *Security Newsbytes*

### 1. Security Myths

**Myth: No amount of security will keep a determined hacker from getting into your computer.**

**Truth:** Probably true, but read on. It is scary to think that somebody out there is working away at getting into *your* system. The fact is that most hacking nowadays is not carried out by a person who wants into *your* system, but by computer robots programmed to try to get into as many systems as possible. A feeling of helplessness can lure you into thinking that if nothing will keep your system safe, why worry about it? Think again. No amount of home security would keep a determined burglar from getting in, but that is no reason not to lock your doors and windows. Well-designed security software not only defends your computer, but also alerts you to attacks and attempted intrusions so that you know it's time to take steps to thwart the Bad Guy—robot or human being.

**Myth: I don't have anything important on my computer, so I don't have to protect it or back it up.**

**Truth:** Let's try this by the numbers. The system hard drive of a modern PC with ordinary software installed contains about 100,000 files. That's not counting any of your own saved documents, emails and attachments, photos, music files, browser favorites, cookies, shortcuts, and customized settings. If you are an average user and your system is 2-3 years old, the total number of files may be 300,000 or more. How could anyone know which of those files are important? Most computer users do not think about what is stored on their computers until some or all of their files are lost or their system has been compromised. Then panic sets in. The alternative? Protect your computer and back up your files as if everything were important.

### 2. Scams and Hoaxes

**Subject: Banking Scams**

**Bait:** Scam emails, pretending to come from banks and credit unions around the world, ask you to provide personal financial information such as account numbers and login details. These scams are often supported by fake or spoofed websites, and victims are tricked into thinking they are logging in to a real financial institution website. Don't take the bait! Remember, reputable financial institutions do not ask you to provide financial or personal information over email. Below is a list of some of the banking institutions whose account holders have been recent targets of phishing attacks.

Bank of Montreal  
Barclay's Bank PLC  
Commerce Bank

Fifth Third Bank  
NatWest Bank  
Washington Mutual

**Subject: E-mail Scammers Hiding Malware in Fake IRS Notices**

**Bait:** If you get an email telling you that you're under investigation by the U.S. Internal Revenue Service, take a breath before calling your attorney. Two fraudulent schemes using the IRS name attempt to get victims to install malicious Trojan software on their computers. In the first, the email claims to come from the IRS Criminal Investigation division, and says that the victim is under investigation for filing a false tax return. An attachment, which appears to be the IRS complaint, actually installs malicious software that gives criminals access to the victim's PC. The second email says a complaint about the victim's "business services" has been lodged and advises that this can be arbitrated by the IRS. The "complaint" attachment is a new type of Trojan called Backdoor.Robofo. (See 3. Malware below)

**More information:** <http://www.networkworld.com/news/2007/053107-e-mail-scammers-hiding-malware-in.html>

**Subject: Microsoft World Lottery Scam**

**Bait:** A phony email claiming that the "lucky" recipient has won \$1 million in an international lottery promotion organized by the Microsoft Corporation. But there is no prize or annual lottery promotion and the email was not sent by Microsoft. A recipient who falls for the ruse and submits the requested details to the "Foreign Service Manager" will soon be asked to pay advance fees supposedly required before the "winnings" can be released. Victims who send the required fees will most likely receive further requests for money until they run out of funds or realize that the promised prize is imaginary. Ultimately, victims may reveal enough personal information to allow the scammers to steal their identity, too.

**More information:** <http://www.hoax-slayer.com/microsoft-world-lottery-scam.shtml>

### 3. Malware

**Backdoor.Robofo.** A Trojan that spreads via an attachment to phishing emails appearing to be from the IRS. The malware opens a backdoor (malware that bypasses normal authentication methods, like username and password) on your computer and steals sensitive information by disabling the Windows firewall, logging your keystrokes, and taking screenshots. (See 2. Scams and Hoaxes above)

**More information:**

[http://www.symantec.com/enterprise/security\\_response/writeup.jsp?docid=2007-053013-4425-99&tabid=2](http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-053013-4425-99&tabid=2)

**Cheburgen.a.** A worm that spreads via email attachments and drive-by-download (download of malware through exploitation of a web browser, email client or operating system bug, without any user intervention), as well as by scanning local networks for Windows systems with an unpatched vulnerability dating back to April 2004. The name of the attachment is randomly chosen from a list of words like data, body, doc, and text, and a list of file extensions like bat, cmd, exe, scr, pif, and zip. The malware can send copies of itself to email addresses harvested from the Windows address book of the compromised computer, and it prevents infected computers from accessing the websites of some security companies. The malware also has backdoor capabilities. It opens certain ports, connects to Internet Relay Chat channels, and takes orders from the remote

attacker. The attacker can direct the malware to download files from the Internet and execute them.

**Editor's Note (Rietveld):** These two items are a mere sampling of the damage caused when people open infected attachments. If people practiced *not* clicking when they don't know who sent the attachment or didn't expect it, we'd have a much shorter OUCH.

**More information:**

<http://www.zdnetindia.com/zdnetnew2007/index.php?action=article&prodid=6810>

## 4. 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 June 12th. Check manually too, once every two weeks, to make sure all of the updates have been installed.

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

**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 Tip:** Be sure your operating system is set to retrieve and install updates automatically.

**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>

## 5. Security Screw-Up of the Month

### 45,000 Student Names and SSN's Exposed at the University of Colorado

A hacker broke into a server at the University of Colorado's College of Arts and Sciences' Academic Advising Center, exposing the names and Social Security numbers of nearly 45,000 students. University officials are sending letters notifying students enrolled at CU-Boulder from 2002 until the present that their information has been compromised. Computer security investigators discovered a worm had entered the server through a known vulnerability in its antivirus software, which had not been properly patched by the Center's IT staff, and the server's firewall had been turned off, according to a CU network security expert. "Through a combination of human and technical errors, these personal data were exposed, although we have no evidence that they were extracted," said Bobby Schnabel, CU-Boulder Vice Provost for Technology.

**(Editor's Note (Reichert):** We've heard similar statements before. If you are on a system that has been breached, always assume that your information has been taken. Over the past two years, this editor has been notified of three different system breaches where his personal information was involved, and knows of one ID theft attempt against him.

**More information:** [http://www.denverpost.com/sports/ci\\_5962767](http://www.denverpost.com/sports/ci_5962767)

## 6. Security Newsbytes

### -- Google Warns of "Dirty" Websites

Google has warned users of the increasing threat posed by malware that can be dropped onto a computer when a web surfer visits a "dirty" site. In-depth research on 4.5 million websites carried out by the web search giant found 1 web page in 10 could launch a "drive-by-download," depositing malware onto a visitor's computer. Such software may allow hackers to access sensitive information or install more rogue applications. Graham Cluley, senior technology consultant at Sophos, said that Google is right to highlight what he said is a worsening trend and "a considerable problem" for businesses and end users, adding that an average of around 8,000 new URLs containing malware emerged every day during April.

**More information:** <http://software.silicon.com/security/0,39024655,39167124,00.htm>

### -- Apple Patches 17 Flaws with Fifth Security Update for 2007

Apple has released its fifth major security update this year for users of Mac OS X v10.3.9, Mac OS X Server v10.3.9, Mac OS X v10.4.9, and Mac OS X Server v10.4.9. The most serious of these vulnerabilities is for CoreGraphics in which an attacker could entice a user to open a specially crafted PDF file, resulting in an application crash and an overflow allowing the execution of malicious code. Other serious patches are included for Bind, Fetchmail, and GNU Screen..

**More information:** [http://news.com.com/8301-10784\\_3-9722829-7.html](http://news.com.com/8301-10784_3-9722829-7.html)

### -- F-Secure's Antivirus Lets in Hackers

F-Secure has patched several vulnerabilities in its security products, the most critical of which could be used to run unauthorized software on a victim's computer. The most serious bug affects F-Secure's antivirus products. A flaw in the way the software unpacks files that have been compressed using LHA (a freeware compression utility and associated file format), could allow an attacker to crash the system or run unauthorized software on the computer.

**More information:**

<http://www.techworld.com/security/news/index.cfm?newsID=8995&pagetype=all>

### -- Apple Plugs Gaping Holes in QuickTime

Apple has released a patch for QuickTime 7.1.6 that addresses two issues in the way both the PC and Mac versions of its media player work on the Java platform. One problem could allow hackers to take control of an unpatched computer from a remote location. The second bug could allow an attacker to see sensitive information contained in the web browser's memory.

**More information:** <http://www.macnewsworld.com/story/6U6BnUvYMvBGRE/Apple-Plugs-Gaping-Hole-in-Media-Player.xhtml>

\*\*\*\*\*

*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>.*