

In This Issue

1. Security Myths – 2. Phishing --3. Hoaxes – 4. Virus Alerts – 5. Microsoft and Mac Security Updates – 6. Security Screw-Up of the Month -- 7. Security Newsbytes

1. Security Myths

Myth: I don't apply patches and updates. I don't need them, and they just cause problems.

Truth: A recipe for disaster. Computers are machines, and like all machines, they require maintenance. While it's true that an update or patch occasionally contains a troublesome flaw or a bug, applying them regularly to your computer is nevertheless essential to maintaining security. They help protect your computer and other networked computers against continuous security threats. Viruses and worms are stealthy. Users often don't even know that their computer system has been hacked or infected until it stops working entirely. By the time an infection becomes obvious, it's likely your information will have been compromised or lost, and even more likely that your computer will have spread the infection to other computers -- perhaps many other computers. Think of it as a public health issue.

Myth: I've heard that wireless networks are pretty secure.

Truth: You've heard wrong. Wireless networking has grown so explosively over the last three years that it's hard to find a hotel, café, office, or home without one. All that connectivity, especially “open” or “unsecured” wireless networks in many café-style, business, and home environments -- extend an open invitation to malicious users. Other networks continue to rely on older protection schemes, such as WEP (wired equivalent privacy) and restricting access by MAC (media access control) address, which, while still widely in use, are effectively obsolete. A hacker can beat them in a matter of minutes. Newer security standards such as WPA (Wi-Fi Protected Access) and WPA2 provide reliable protection and security. Using them in your home or office may require you to purchase new equipment or trade in what you have, but as insurance goes, this kind is cheap. When on the road, always ask before you connect. If the wireless is not secured by WPA or WPA2 (or the proprietor can't tell you), be aware that the risks may outweigh the convenience.

2. Phishing

Subject: Banking Scam 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 website. Don't take the bait! Below is a list of some of the banking institutions whose account holders have been recent targets of phishing attacks.

Arizona Federal
Bank of America
First United Bank
Flagstar Bank
HSBC Bank

NatWest Bank
Wachovia Bank
Washington Mutual
Yorkshire Bank

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

Subject: Virginia Tech Tragedy

Spam emails have been sent promising images of the shootings and carrying a photograph of gunman, Cho Seung-Hui, who killed more than 30 students and teachers at the Virginia school before killing himself. They also include a bogus link to a Brazilian website where you can supposedly see footage of the campus shootings. However, clicking on the link downloads a malicious screensaver file called Terror_em_Virginia.SCR, which in turn installs spyware that acts as a banking Trojan for stealing your passwords, usernames, and account numbers.

More information:

<http://www.informationweek.com/security/showArticle.jhtml?articleID=199100863>

3. Hoaxes

Subject: Your cellphone can kill you?

A rumor is spreading rapidly via word-of-mouth, email, phone and SMS claiming that simply receiving a mobile cellphone call from certain numbers will activate a terrible virus that causes brain hemorrhaging and death. According to the message, the phone calls create high-frequency tones that damage the user's brain, causing fatal injuries. The message claims that 27 people have already died and names several news outlets where people can supposedly find out more information.

More information: <http://www.hoax-slayer.com/killer-mobile-phone-calls-hoax.shtml>

Subject: Use Your Common Sense.

An email message warning that a new and destructive computer virus is targeting webmail users and arrives in an email with the subject line, "Obituary of the late Mr. Common Sense...may he rest in peace". There is no virus like the one described in the warning, and the message is just a variant of the Life is Beautiful Virus Hoax that has been hitting inboxes everywhere since 2002.

More information: <http://www.hoax-slayer.com/mr-common-sense-virus-hoax.shtml>

4. Virus Alerts

Worm: Zhelatin.CQ is an email-based virus that uses attachments named "read me.exe", "video.exe", "movie.exe", "click me.exe" etc. The subject line of the email contains war news like "Missile Strike: The USA kills more then 20000 Iranian citizens" .. Opening the attachment unleashes a worm that creates its own peer-to-peer network so it can infect other computers, harvest more email addresses, and send out copies of itself.

More information: <http://www.hoax-slayer.com/iran-missile-strike-worm.shtml>

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 May 8th. 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.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 Tip: Be sure your operating system is set to retrieve and install updates automatically.

Windows:

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

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

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

6. Security Screw-Up of the Month

Department of Agriculture Admits to Exposing SSN's for 26 Years

The Social Security numbers of about 150,000 people were found to be at risk for identity theft after it was discovered that USDA had exposed personal identifying information on farmers and others for the last 26 years. USDA admitted that it had posted sensitive information such as names and Social Security numbers online in a publicly available database. The database has existed since 1981 and the information has been exposed ever since it was put online according to Terri Teuber, USDA director of communications. Teuber said in an interview that she's not sure when the database went online, but her agency became aware of the situation on April 13th after a farmer was researching the name of her farm on the Internet and stumbled upon the information. USDA has identified between 105,000 and 150,000 individuals whose private information had been entered into the Federal database at some time in the last 26 years.

More information:

<http://www.informationweek.com/showArticle.jhtml?articleID=199200365>

7. Security Newsbytes

Apple Releases Fourth OS X Security Update

Apple has issued an update to address 25 security flaws in OS X, down from 45 last month. The most serious of the flaws could let attackers take control of unpatched systems. However, according to Apple, none of the vulnerabilities is "known to have been exploited."

More information:

http://news.com.com/Apple+plugs+25+Mac+OS+X+flaws/2100-1002_3-6177758.html
& <http://docs.info.apple.com/article.html?artnum=305391>

Editor's Note: (Wyman) And, by the way, Apple's patch release came out just as white-hat hackers (Good guys who break into systems with authorization from owners to help make them aware of security flaws) at the CanSecWest security conference in Vancouver, B.C. received a cruising-for-a-bruising challenge from Apple to break into

two MacBooks. Promptly thereafter, a hacker delivered the blow successfully and collected his winnings: a MacBook and \$10,000. Pride goeth before a fall.

Securemac Releases Enhanced Antispyware

MacScan 2.4, designed for OS X 10.2.4 and later, detects, isolates, removes and protects Macs against spyware, keystroke loggers and Trojans using both real-time spyware definition updating and detection methods. It also helps manage Internet-related clutter on your Mac. Mac users as a group have tended to minimize or ignore the threat that malware poses to OS X and Mac software applications.

More information: <http://macscan.securemac.com/>

Fraudster on the Loose on eBay

Fraudulent listings on eBay continue to pile up, and the online auctioneer appears incapable of proactively putting an end to them. Pornographic images by the hundreds are showing up as phony auctions on eBay, apparently posted by established users with highly favorable feedback ratings--a hallmark of accounts that have been hijacked and then used to con unsuspecting buyers. eBay representatives emphasize that the company's security department continuously snuffs out phony postings, which comprise a tiny percentage of overall listings. Still, some fraudulent auctions contain links that direct would-be buyers to spoofed sites that attempt to phish their eBay credentials.

More information: http://www.theregister.co.uk/2007/03/21/ebay_fraud_anatomy/

Google Pulls Sponsored Ads Gone Bad

Google has removed paid links that advertised seemingly legitimate websites but which were wired to install nefarious programs on PCs. The links were displayed as "sponsored links" after visitors entered specific words into Google's search service. Clicking the sponsored links would eventually take visitors to a legitimate site, but by way of another site that attempted a "drive-by installation" of password-stealing software. Miscreants placed the links using Google's AdWords service for advertisers.

More information: <http://software.silicon.com/malware/0,3800003100,39166930,00.htm>

Teen Charged in Attack on AOL Systems

A complaint has been filed by the Manhattan District Attorney's office charging that 17-year-old Mike Nevins committed computer trespassing, computer tampering, and criminal possession of computer material in December 2006 and April 2007. The DA said that the teen broke into AOL and infected their systems with malicious programming designed to transfer information back to his computer. AOL is remaining silent about whether or not customer information was compromised.

More information:

http://tech.monstersandcritics.com/news/article_1298329.php/Teen_charged_with_attack_on_AOL_systems

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>.