

In This Issue

1. Malware and Five Ways to Protect Against It – 2. Malware – 3. Scams and Hoaxes – 4. Microsoft and Apple Security Updates – 5. Security Newsbytes

1. Malware and Five Ways to Protect Against It

Malware is a catch-all term, short for “malicious software.” It used to be that viruses spread from one computer to another. Then they got smarter and began spreading from one network of computers to another. Now we are all on one big Internet. New varieties of malicious software pop up every day: viruses, worms, spyware, Trojans, downloaders, keyloggers, backdoors, rootkits, adware, crimeware, and so on. All these threats have been lumped together as malware. The days of unwittingly inserting an infected floppy disk into your computer and shooting yourself in the foot are over. Today, many emails and websites can automatically launch attacks directly on your computer.

Certain kinds of attacks require user intervention. Phishing scams, for instance, lure you into clicking a link in an email or visiting a rigged website where malware is pushed at your computer immediately -- the drive-by download. Even worse, an increasing number of legitimate websites are being rigged by Bad Guys to deliver malware without the knowledge of the site owners or its visitors.

The bottom line: Simply avoiding suspicious, sleazy, or unfamiliar websites will no longer safeguard your computer. Anti-spam or anti-virus software alone can no longer protect your computer against sophisticated attacks that exploit ever-changing combinations of user gullibility, rigged websites, web browser vulnerabilities, and booby-trapped emails. Sophisticated threats require multiple layers of protection. The best defense against a clever Bad Guy is to become a knowledgeable computer user.

-- **Think before you click.** Email phishing scams work because people don't think before they click. Don't open email attachments sent by people you don't know or that arrive unexpectedly. Look before you click on any link. Amazon.com is not the same website as amazon-com.cn. Don't divulge personal information unless you are sure who is asking for it, why, and what they are going to with it.

-- **Protect your computer at the far end.** Install a hardware firewall or a router as an extra layer of protection between your home network and the Internet—even if it's only for one computer.

-- **Protect your computer at the near end.** Install a reliable suite of security software on your computer: anti-virus, a software firewall, and anti-spyware, and keep all of it up to date.

-- **Turn on the features in your security suite.** They may make your computer run a little slower, but will save you time, money, and grief in the long run.

-- **Set your security suite to run a complete scan automatically.** Once a week is a good rule of thumb. If you like, schedule the scan to run at 2:00 AM when you are not using your system.

More information: <http://www.pcmag.com/article2/0,2817,2327810,00.asp>

2. Malware

PersonalAntiSpy Free. Rogue anti-spyware that purports to scan and detect malware on your computer, but which attempts to badger you into purchasing the program by presenting intrusive, deceptive warnings, and misleading security scan results.

PersonalAntiSpy Free can severely compromise the security of your computer by opening network connections without your knowledge, disabling other legitimate, installed security software, modifying system files, and installing additional malware. It may also collect and transmit personally identifiable information without your consent while degrading the performance and stability of your computer.

More information: <http://sunbeltblog.blogspot.com/2008/09/new-rogue-personalantispy-free.html>

Troj/Agent-HNY. A Trojan that masquerades as an iPhone game. Cybercriminals are sending spam emails with subject lines such as “Virtual iPhone games!”, “Apple: The most popular game!”, and “Virtual iPhone toys!” in an effort to encourage iPhone owners to download a malicious file. The emails are sent with an attachment called Penguin.Panic.zip, which poses as a version of the popular, although silly, game for the iPhone platform. The file actually contains a Trojan that infects and can take control of Windows PC’s.

More information: <http://arstechnica.com/journals/apple.ars/2008/09/18/penguin-panic-trojan-targets-windows-iphone-users>

3. Scams and Hoaxes

Obama Survey Gas Card Scam

As the U.S. presidential elections near, online scammers are taking advantage of the candidates’ popularity. This scam begins with a spam email--complete with a photo of Senator Barack Obama--that asks recipients to participate in a survey for the Democratic Party nominee in exchange for \$500 worth of gas gift cards. However, that is the last you’ll see or hear about any free gasoline. Users who click on the button to answer the poll get redirected to a webpage whose content is not in any way related to any survey, but which does contain references to other legitimate websites. Clicking on the “Always Free” button on this page brings up a prompt for you to install a Trojan information-stealer disguised as an ActiveX control.

More information:

http://blogs.pcmag.com/securitywatch/2008/09/obama_survey_gas_card_scam.php

<http://blog.trendmicro.com/obama-survey-offers-500-gas-gift-cards/>

[Editor’s Note (Rietveld): “Always Free” should always be read as “Don’t even think about clicking on this.” And PS, there is no free lunch.]

Virus Complaint Email Carries Malware

According to this bogus complaint email, the sender has been receiving virus emails that originate from the recipient's computer and is intending to take legal action. The message demands that the recipient print out a copy of the email log and data files, supposedly contained in an email attachment, and pass them to his or her Internet Service Provider so that they can fix the problem. The email warns that the police will become involved and a lawsuit will be filed if the recipient does not comply with this request immediately.

However, instead of log files, the attachment actually contains malware. Opening the attachment installs a Trojan that collects sensitive information from the infected computer and communicates to the Bad Guys.

More information: <http://www.hoax-slayer.com/malware-from-your-computer.shtml>

Internet Access Suspended Malware Email

This email warning claims that the recipient's Internet access will be suspended if he or she does not stop “the illegal downloading of copyrighted material.” The message appears to be from the “Internet Service Provider Consortium [sic],” and urges the recipient to open an attachment that supposedly contains a report of the recipient's illegal activities over the last six months. However, the “Internet Service Provider Consortium” does not exist and opening the zip file attachment will install malware on the user's computer that may steal information, communicate it to the Bad Guys, and download other malware components.

More information: <http://www.hoax-slayer.com/internet-access-suspended-malware.shtml>

American Airlines Loyalty Program Phishing Scam

This fake email, purportedly from American Airlines, promises the recipient \$50 in return for logging on to a website and filling out a short customer survey. The message claims that the bonus is a new rewards program that forms part of the existing American Airlines AAdvantage program. Customers are instructed to click a link in the message to log on to the American Airlines website and follow the steps to claim their bonus. However, the message does not originate from American Airlines and the promised bonus is bait for a clever trap designed to steal personal information. Those who take the bait and click the included link will be taken to a bogus website where they are instructed to login, take the survey, and then provide a bevy of personal and financial information.

More information: <http://www.hoax-slayer.com/american-airlines-phishing-scam.shtml>

4. 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 October 14th. 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/>

iPhones: Must be updated manually:

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

5. Security Newsbytes

Massive Mac Leopard/Tiger Update Fixes 34 Vulnerabilities

Two huge updates to the Mac operating system were released recently as version 10.5.5 and Security Update 2008-006. 34 separate vulnerabilities in OS X 10.4.x (Tiger) and 10.5.x (Leopard) are addressed. All manner of vulnerabilities are present in 18 different components and bundled applications. They range from threats posed by malicious font files and graphic files, to the unintended disclosure of the usernames list on the system through the login window as well as the administrator password, and to allowing logons without any password at all.

More information: <http://support.apple.com/kb/HT3137>

Lack of User Awareness Hurts Users, Other Users, and Businesses

What you don't know when it comes to your computer system's security--and more to the point, Internet security--can hurt you, other users, and your business big time. Results of two security surveys by McAfee* show that many of the 378 computer users interviewed by phone were undereducated when it comes to recognizing threats that the Internet poses to their computers and to their personal privacy. About half of the 3,000 businesses surveyed ignored, discounted, or denied the dangers posed by cybercrime.

- 92% of users surveyed believed their anti-virus software was up to date, but only 51% had updated their anti-virus software within the past week
- 73% of users surveyed believed they had a firewall installed and enabled, yet only 64% actually did.
- About 70 % of PC users believed they had anti-spyware software, but only 55% actually had it installed.
- 25% of users surveyed believed they had anti-phishing software, but only 12% actually had the software.
- 42% of businesses surveyed dedicate just one hour a week to proactive IT security management, despite the fact that 21% acknowledged an attack could put them out of business.
- 44% of businesses surveyed think cybercrime is only an issue for larger organizations and does not affect them.
- 52% of businesses surveyed believe that because they are not well-known, cybercriminals will not target them.
- 45% of businesses surveyed do not think they are a "valuable target" for cybercriminals.
- 46% of businesses surveyed do not think they can be a source of profit for cybercriminals.

More information: <http://billmullins.wordpress.com/2008/09/25/your-lack-of-security-awareness-hurts-you-and-me-on-the-internet/>

http://www.mcafee.com/us/about/press/corporate/2008/20080723_191010_q.html

* http://download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf
http://www.mcafee.com/us/research/does_size_matter/index_noreg.html

Copyright 2008, SANS Institute (www.sans.org).

***Editorial Board:** Bill Wyman, John York, 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>.