

In This Issue

1. *Security Mini-Quiz* – 2. *Top Ten Reasons* – 3. *Scams and Hoaxes* – 4. *Microsoft and Apple Security Updates* – 5. *Security Screw-Up of the Month* – 6. *Security Newsbytes*

1. Security Mini-Quiz

(1) **You can trust an email if the sender is**

- a. Your CEO
- b. Your company security officer
- c. Your bank or credit union
- d. Someone you've known a long time

(2) **Which of the following security features do you need to keep your computer safe?**

- a. A hardware firewall
- b. An anti-virus program
- c. An anti-spyware program
- d. A hardware firewall and a software firewall

Answers appear at the end of this OUCH.

2. Top Ten Reasons Why People Don't Have Better Computer Security

- 10. I don't have anything important on my computer.
- 9. My computer is brand new. It came with all the security stuff on it.
- 8. My IT department takes care of everything, so I don't have to worry about it.
- 7. I'm positive my anti-virus program is working, and it will take care of the worst stuff.
- 6. I have a hardware firewall; nobody can get into my computer.
- 5. Anti-virus and anti-spyware programs slow my computer down too much.
- 4. I only open attachments from people I know.
- 3. I don't use the same password for all of my files.
- 2. Who is going to break into MY computer?
- 1. I'm planning to install all the security stuff as soon as I get caught up on my work.

3. Scams and Hoaxes

Bank, Credit Union, Pay-Pal, and eBay Phishing Scams

Bait: These email phishing scams are fewer in number, but are still going strong. Remember that financial institutions, such as banks, credit unions, Pay-Pal, and eBay, never send out emails asking account holders and members to provide or verify personal information. If you receive such an email, contact the financial institution and report it.

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

Examples: <http://www.hoax-slayer.com/citizens-bank-phish.shtml> and http://blogs.pcmag.com/securitywatch/2007/09/bank_phish_bonanza.php

Dating Fraud Spam Emails

Bait: A brief email in which a “nice girl,” purporting to be the sender, promises to send pictures if her recipient will reply to a specified email address. But “she” is really after

your money. Scammers have been quick to capitalize on the growing popularity of Internet dating, often making contact with potential victims via online dating services. In other cases, they use a less targeted approach by randomly distributing vast numbers of bait emails in the hope of hooking just a few gullible recipients.

More information: <http://www.hoax-slayer.com/dating-fraud-spam.shtml>

Cheap Software Scams

Bait: An email with links to a website where you can purportedly buy a license for software products—particularly those made by Microsoft and Adobe—at prices so low that they cannot be believed. And they can't. Software piracy schemes never go out of style; they just keep coming back in different guises. If the price is too good to be true, you can bet it isn't.

More information: <http://graphicssoft.about.com/cs/faq/a/softwarecams.htm>

4. Microsoft and Apple Security Updates

Microsoft provides free security updates for Windows, as does Apple for Mac OSX and the iPhone.

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 9th. 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/>

iPhones: Must be updated manually:

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

Security Tips: 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=301191>

5. Security Screw-Up of the Month

Ameritrade Breach Exposes Personal Information on Millions of Customers

An attorney has launched a class-action lawsuit against TD Ameritrade Holding, alleging that the online brokerage knew a hacker had access to a customer database as far back as a year ago. Ameritrade recently emailed account holders and put a public advisory on its website alerting users that a hacker broke into one of its databases and stole personally identifiable information for an undisclosed number of its 6.3 million customers. The company said names, email addresses, phone numbers, and home addresses were taken in the data breach. Client assets, along with user IDs, personal identification numbers, and passwords, were not stored in the compromised database.

That news might have come as a relief to worried customers, but Ameritrade's website advisory noted that it was unclear whether or not account numbers, dates of birth, and Social Security numbers had been stolen. Ameritrade did not say when the hackers got into the database or how long they remained there. Kim Hillyer, a spokeswoman for

Ameritrade, said that all of the company's 6.3 million accounts opened before July 18th of this year had been breached. She would not say when the company first learned of the breach, only that "they had been investigating client reports of spam for some time." Go figure.

Meanwhile, emails obtained by *Network World* show that Ameritrade received explicit and repeated warnings from an IT security expert starting January 9, 2006 that its customer data had apparently been compromised, placing the start of the breach much earlier than reported and likely pushing it back to 2005. Nevertheless, the company insisted for the next 20 months that a flood of stock-related spam received by numerous clients did not indicate a more serious problem. Following the January 2006 email, subsequent warnings from multiple sources also failed to prompt the company to alert its clients. Not until September 21st did Ameritrade publicly acknowledge that "unauthorized code" on its systems had "allowed certain information stored in one of our databases, including email addresses, to be retrieved by an external source." Apparently, Ms. Hillyer hadn't seen those emails.

More information:

http://www.informationweek.com/story/showArticle.jhtml?articleID=201807006&cid=RSSfeed_IWK_News

<http://www.networkworld.com/community/node/19720>

6. Security Newsbytes

Sophos Charges That China Hosts Nearly Half of All Malware Sites . . .

According to a report released by antivirus company Sophos, China - including Hong Kong - hosted 44.8 percent of the world's infected sites in August. The U.S. ranked a distant second, hosting 20.8 percent of sites that contain malicious code. The number of infected Web pages has also grown. Sophos said it detected an average of 5,000 new infected pages each day in the month of August.

More information: http://www.news.com/China-hosts-nearly-half-of-all-malware-sites/2100-7349_3-6205896.html?tag=cd.hed

. . . But China Says It's a Cyber-Attack Victim, Not the Villain

China has been the target of a big increase in cyber-attacks in recent years and faces more of a threat from hackers than any country in the West. Beijing has hotly denied recent reports in Western media that Chinese hackers penetrated systems in the Pentagon and in the Chancellery and key ministries of Germany. Computers in Britain's Foreign Office have also been hit, according to the Guardian newspaper. "Countries that are victims of computer hackers should work together instead of arbitrarily blaming China," Wang Xinjun, a researcher at the Academy of Military Sciences, told the official Xinhua news agency.

More information: http://www.news.com/China-says-its-a-cyber-attack-victim%2C-not-villain/2100-7349_3-6209570.html?tag=cd.top

You've Heard about Bluetooth. But How about Bluejacking, Bluesnarfing, and Bluebugging?

A study by research firm InsightExpress has revealed that 73% of mobile device users are not acquainted with security issues that could put at risk mobile devices such as cell-phones and Bluetooth-equipped notebooks. To these users, terms such as bluejacking,

bluesnarfing or even bluebugging would probably be unfamiliar. Bluejacking, also known as bluespamming, is a technique used to send anonymous text messages to mobile users via Bluetooth. Bluesnarfing, a more dangerous technique, can allow a hacker to access information stored on a mobile device without its user's knowledge. Possibly the most serious of the three risks is bluebugging. This technique allows attackers to access mobile-phone commands using Bluetooth technology, without notifying or alerting the device owner, and initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.

More information: http://www.news.com/Symantec-warns-users-over-Bluetooth-security/2100-1029_3-6209361.html?tag=cd.lede

Yahoo Messenger Hit with Ninth Zero-Day Exploit

Attack code that targets Yahoo Messenger has been published on the Internet, a security researcher warned Wednesday, marking the ninth exploit aimed at the popular instant messaging software so far this year. In a posting to the milw0rm.com Web site, someone identified as "shinnai" disclosed malicious Visual Basic code that allegedly lets attackers feed any file to users of the latest version of Messenger. The exploit code successfully executes on a fully-patched PC running Windows XP SP2, "shinnai" said, although the effect depends on the security settings of Internet Explorer.

More information: <http://www.networkworld.com/news/2007/092007-yahoo-messenger-zero-day.html>

Skype Worm Blows Bubbles at Victims

Miscreants have created a worm that uses the chat function built into Skype to spread. The malware--known as Ramex, Skipi or Pykspa--sends a short message containing a link to a seemingly benign JPEG* file to contacts of users with infected Windows PC's. Users who click on the link are prompted to download and run a copy of an image (actually a malware payload), after which their machines become infected. Ramex contains functions designed to disable anti-malware packages on infected PC's and disable the downloading of security updates. Ramex displays soap bubbles (one of the default built-in wallpapers** in Windows) on infected PC's. While anti-virus vendors are in the process of updating detection to seek out the malware, Skype users are urged to be wary of clicking on even seemingly benign message links.

More information: http://www.theregister.co.uk/2007/09/11/skype_worm/

* <http://en.wikipedia.org/wiki/Jpeg>

** http://en.wikipedia.org/wiki/Computer_wallpaper

OUCH October Security Mini-Quiz Answers

- (1) None of them. The name and email address of any sender may be spoofed.
- (2) b, c and d. Each of these four security measures provides specific kinds of needed protection.

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>.