Volume 3, Number 11 **November 2006**

SANS OUCH!

SANS Institute Security Newsletter for Computer Users

In This Issue

1. What to Watch Out for This Month

There were 180 reported Phishing alerts during the month of October, of which 106 involved the following banks and credit unions. Don't take the bait! Before you respond to any email requests for personal information, call your bank, credit union or other institution. In general, reputable financial institutions do not request personal information via email. Listed below are banks and credit unions whose account holders were the object of Phishing scams last month. Information for this report was gathered from various sites including:
http://www.trendmicro.com/en/security/phishing/overview.htm
http://www.millersmiles.co.uk

Alliance Bank
BB&T
Bank of America
Bank of America Military Bank
Barclays Bank
Bendigo Bank
Brattleboro Savings & Loan
Central Willamette Community Credit Union
Chase Bank
CitiBank
Commonwealth Bank of Australia
Consumers Cooperative Credit Union
Co-operative Bank of UK
Desjardins Bank
Egg Bank (Formerly Prudential Banking plc)
Empire Federal Credit Union
FAIRWINDS Credit Union
JPMorgan Chase & Co
Halifax Bank
HSBC Bank
Lloyds TSB Bank
National Australia Bank
Nationwide Bank
Nationwide Online Banking
Navy Federal Credit Union
North Fork Bank
Royal Bank of Canada
Scott Credit Union
Sears Bank
Sovereign Bank
Staley Credit Union
Teachers Credit Union
Wachovia Bank
WAMU Bank
Warren Federal Credit Union
Wells Fargo Bank
Westpac Bank
Zions Bank

2. More Phishing

Subject: Earthlink – "IMPORTANT: Alert about your Earthlink billing information on file."
Bait: A phony email, allegedly sent from Billing@Earthlink.net, inviting you to update your Earthlink personal information, which includes an embedded link directing you to an unsecured, fake website.
Security Tip: The spoofed website looks nothing like an actual Earthlink webpage.
Sample: http://www.millersmiles.co.uk/report/3569

Subject: PayPal – "Congratulations!!!"
Bait: A phony email, allegedly sent from service@paypal.com, stating that you have been chosen by PayPal's online department to take part in a quick and easy 5 question survey, in return for which you will receive a credit of $100 to your account, and inviting you to

click on the embedded link and take part in this unique offer. However, the link takes you to a fake, phishing website.
Security Tip: PayPal never sends emails requesting personal information in this way. The spoofed website looks nothing like an actual PayPal webpage.
Sample: http://www.millersmiles.co.uk/report/3684

Subject: eBay – "Violation Concerning Your Ebay Account"
Bait: A phony email, allegedly sent from update@validationserver.net, stating that there is a dispute about an auction and that an eBay member, kuhawkers (84), has indicated that he already paid for item #216573321157. The embedded link, which invites you to submit details regarding the payment, leads to a fake website.
Security Tip: eBay never sends their users emails requesting personal details in this way. The spoofed website looks nothing like an actual eBay webpage.
Sample: http://www.millersmiles.co.uk/report/3680

3. Hoaxes

ATM Security Advice Email: Enter PIN in Reverse to call the Police.
An email advising ATM users that if you are forced by robbers to withdraw money from an ATM, you can secretly alert police by entering your PIN in reverse. Although such technology exists, it has never been deployed, and the claim is not true.
More information: http://www.hoax-slayer.com/reverse-pin-ATM.shtml

4. Virus Alerts

QQpass spyware – Trojan variant
As many as 100,000 Flash MP3 players, given away as prizes by McDonald's in Japan, were found to be infected with a variant of the QQpass spyware Trojan horse program. The players were preloaded with ten songs and the malware. McDonald's Japan has apologized, established a helpline to facilitate the recall of the infected MP3 players, and posted directions for cleaning infected PCs.
More information:
http://www.theregister.co.uk/2006/10/16/mcd_spyware_mp3_recall/print.html

RavMonE.exe – Virus
Apple has announced that a small number of the Video iPods available for purchase after September 12, 2006, left their contract manufacturer carrying the Windows RavMonE.exe virus. According to Apple, they have seen fewer than 25 reports concerning this problem, and the iPod nano, iPod shuffle and Mac OS X are not affected. Apple says that Video iPods now shipping are virus free.
More information: http://www.apple.com/support/windowsvirus/

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 and occasionally out-of-cycle on any day of the month. The next scheduled release date is November 14th.
More information:
http://www.microsoft.com/athome/security/protect/windowsxpsp2/wsc.mspx

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.mspx
OS X: http://docs.info.apple.com/article.html?artnum=106704
Check manually, too, once every two weeks to make sure all of the updates have been installed.

6. Security Screw-Up of the Month

Prescription for Wriggling

Hackers broke into Akron Children's Hospital's computer files over Labor Day weekend, and gained access to the names, addresses, birth dates, and Social Security numbers of about 230,000 patients and their families, as well as to a database containing the bank account information of about 12,000 donors. The hospital did not begin notifying families until seven weeks after the breach was discovered by sending out 10,000 letters, followed by 120,000 more two days later. As for the remaining 100,000 notifications, "Everyone that's going to be contacted should know by next Wednesday," said Bob Howard, the hospital's director of planning. The hackers gained access to the hospital's computer network during an expansion of the system. "We don't know that anybody was actually affected," Howard said. "All we know is, it's possible. We don't even know if [the two hackers] took anything." According to a statement on the hospital's web site (www.akronchildrens.org), computer security consultants hired by the hospital "found no evidence that any specific data was downloaded, tampered with or compromised; however, the opportunity to view the data existed."
More information: http://www.ohio.com/mld/beaconjournal/15871658.htm
[Editor's note (Reichert): How can any consultant guarantee that evidence would even exist if a site was so broken to start with? More wriggling, in my opinion.]

7. Security Newsbytes

eCards May Deliver More Than Holiday Greetings

Most people never consider the dangers of ecards, and there are plenty of dangers. A legitimate-looking ecard, once clicked and/or downloaded, might turn out to be a phishing ploy, or to contain concealed malware. If the ecard is from someone you don't know, think twice before opening or downloading it, and always keep the security software on your computer up-to-date and in good working condition.
More information: http://www.scambusters.org/ecards.html

Apple Wrestles With OSX Security Flaws

Apple has released Mac OS X 10.4.8 (Security Update 2006-006), an update that addresses 15 flaws in OS X, Safari, and Adobe Flash Player, vulnerabilities that could allow an attacker to take control of a Mac. Some of the flaws can be exploited simply by manipulating the user into viewing specially crafted images or websites.
[Editor's note: (Wyman) Why is Apple so slow on the uptake? Mac software is now the target of some of the very same security exploits that were identified and corrected in the Windows world months ago. Predictable Mac vulnerabilities like this can and should be patched immediately and preemptively.]

More information: http://news.com.com/2102-1002_3-6121372.html?tag=st.util.print

Number of Records Breached in US Approaches 100 Million
The Privacy Rights Clearinghouse's running tally of the number of records involved in security breaches is approaching 100,000,000. PRC has been keeping tabs on security breaches since shortly after the ChoicePoint debacle became public in February 2005. The sheer number of records affected indicates a need to go beyond passwords and encryption to ensure security. Organizations also need to establish rules for who has access to what information, where it is stored, and when, where and why it is moved.
More information: http://www.technewsworld.com/story/53222.html

Theft by Malware
The Metropolitan Police Computer Crime Unit is investigating the theft of credit card data and passwords from thousands of personal computers in the United Kingdom and potentially tens of thousands more around the world. The stolen data, harvested using Backdoor blended-threat malware, were discovered stored on a computer in the United States.
More information: http://www.guardian.co.uk/uklatest/story/0,,-6139406,00.html

FBI's Imprimatur Added to Phishing Scams
Fraudulent phishing e-mails claiming to be from Richard Mueller III, FBI Director, and Donna M. Uzzell, FBI Compact Council Chairman, offer recipients big bucks and threaten big penalties if you don't cooperate.
More information:
http://www.emergencyemail.org/newsemergency/anmviewer.asp?a=155&z=1

Anti-Social Uses for Internet Social Networks
Web-based social networks, such as MySpace, Facebook and Flickr provide a new way for Netizens to meet friends, trade information, and share pictures. But they are also a way for miscreants to spread malware. Recent exploits for Internet Explorer were found in poison banner ads on MySpace, Webshots, and many other sites. You can help keep your computer safe by running anti-virus, a firewall and one or more anti-spyware programs.
More information:
http://www.pcworld.com/article/id,127347-c,onlinesecurity/article.html

8. Security Question of the Month

What is a "Zero-Day Exploit?
A zero-day exploit (attack) is one that takes advantage of a security vulnerability before or on the day that the existence of the vulnerability becomes widely known. Three or four years ago, hackers needed 7-14 days to figure out how to use a newly discovered vulnerability in order to launch an exploit. That "lead time" allowed hardware manufacturers and software developers to notify their customers, recommend ways to cope with it, and distribute software patches and anti-virus updates.

But there are more hackers, and they're getting better at what they do. So, how do you defend your computer when you have 0 days to prepare? You can't. But if you keep your computer security software up-to-date, you'll help decrease your overall risk and increase the chances that a patch or update will reach your computer ahead of an exploit.