Volume 3, Number 10 October 2006

SANS OUCH!

SANS Institute Security Newsletter
for Computer Users

In This Issue

1. What to Watch Out for This Month

There were 164 reported Phishing alerts during the month of September, of which 105 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. Reputable financial institutions will not request personal information from you by email. Remember: "Your credit card information only expires when you do." 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

American Eagle Federal Credit Union
ANZ Bank
BB&T
Bank of America
Bank of Ireland
Barclays Bank
Bright Start Credit Union
Chase Bank
CitiBank
Clydesdale Bank
Commonwealth Bank of Australia
CUNA
Egg Bank (formerly Prudential Banking plc)
First National Bank
Flagstar Bank
JPMorgan Chase & Co
Halifax Bank
Hawaiian Tel Federal Credit Union
HSBC Bank
IOWA Credit Union
Lloyds TSB Bank
Michigan Schools & Government Federal Credit Union
Mid America Bank
Nationwide Online Banking
NAFCU
NatWest Bank
Royal Bank of Scotland
Santa Barbara Bank and Trust
Sierra Central Credit Union
Smile Bank
Sun Trust Bank
U.S. Bank
Wachovia Bank
WAMU Bank
Warren Federal Credit Union
Wells Fargo Bank

2. More Phishing

Subject: Amazon Billing Review
Bait: A phony email, written in poor English and allegedly sent by Amazon.com, inviting you to click on the embedded link and visit an unsecured, fake website in order to update your account information.
Security Tip: The spoofed website looks nothing like an actual Amazon Web page.
Sample: http://www.millersmiles.co.uk/report/3359

Subject: PayPal – Your payment has been sent to DonutsStore!
Bait: A phony email, allegedly sent by PayPal, stating that you sent $328 USD to the DonutsStore (a photo sharing website) and suggesting that you click on the embedded link if you did not authorize payment.

Security Tips: 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/3372

3. Virus Alerts

Backdoor.IRS.Flood – Blended threat
A fake email greeting, allegedly from All-Yours.net, lures you in to installing a Trojan downloader worm from a bogus website.
More Information: http://www.hoax-slayer.com/all-yours.net-fake.shtml

W32/Opanki & W32/Spybot.gen.p - Worms
Spread via AOL Instant Messenger, the MIRC chat client, improperly configured/protected network shares, and by exploiting known, but unpatched vulnerabilities in Windows.
More information: http://vil.nai.com/vil/content/v_140546.htm

4. Spyware and Antispyware

Spyware is malicious software designed to monitor your computer activity surreptitiously and transmit that information over the Internet. Spyware can infect PC's or Macs, alter browser and security settings, download further malicious software, such as keystroke loggers and Trojans, and cause your system to slow down and behave unpredictably. Like a virus or worm, spyware can infect your computer via email, your Web browser, or through your network connection. Installing an antispyware program is the best way to protect your PC or Mac.
More information:
Windows:
http://www.microsoft.com/athome/security/protect/windowsxpsp2/antispy.mspx
OS X: http://www.apple.com/macosx/features/security

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. An out-of-cycle update was issued on September 25th. (See "Dat Patch Don't Patch" in 7. below.) The next scheduled release date is October 10th.
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 Tips: 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 &
http://docs.info.apple.com/article.html?artnum=301191

Check manually, too, once every two weeks to make sure all of the updates have been installed.

6. Security Screw-Up of the Month

Astronomical Fumbles and the Freedom to Lose
In less than two years' time the Privacy Rights Clearinghouse in San Diego has tallied 93,754,333 screw-ups involving private records—roughly the distance in miles for a voyage from the Earth to the Sun. Kicking off the return trip is this month's biggie blunder from those freedom-loving folks at Chase Card Services. Owing to "human error," computer tapes containing information about 2.6 million current and former Circuit City credit card holders were inadvertently thrown out with the trash. The news prompted Chase CEO Richard Srednicki to promise, after the fact, that: "The privacy of our customers' personal information is of utmost importance to us, and we take the responsibility to safeguard this information very seriously." Thanks, Dick. Others may side with NYT author Mr. Zeller who in breaking the Chase story noted that when it comes to keeping personal information secure, "The enemy is us."
More information:
http://www.nytimes.com/2006/09/25/technology/25link.html?_r=1&oref=slogin (free registration required)
http://www.networkworld.com/news/2006/090806-chase-card-services-dumps-customer.html

7. Security Newsbytes

Dat Patch Don't Patch.
According to officials at Microsoft, hackers have released sample code showing how to exploit an Internet Explorer flaw on a fully patched version of Windows XP, a move that security experts believe will step up attacks (See "Windows" in 5. above). The patch in question was released out-of-cycle on September 25th to address a Vector Markup Language (VML) flaw, which digital miscreants are exploiting actively via malicious Web sites, including several pornographic sites based in Russia.
More Information:
http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/06/09/25/HNmspressured2patchie_1.html

The American Way
According to officials at the Commerce Department, 1,137 laptop computers have gone missing since 2001, about half of which were assigned to the Census Bureau. The Census Bureau, the main collector of information about Americans, has admitted to losing 672 laptops, of which 246 were reported to contain some personal data. The Census Bureau said in a statement that "No personal information from any of the missing computers has been known to have been improperly used."
More Information: http://www.usatoday.com/news/washington/2006-09-21-commerce-laptop_x.htm
Editor's Note: (Wyman). A mind-boggling damage control failure. Is that statement a good news/bad news joke? Bad news from the cops: "Thousands of cars have been stolen." Good news: "As far we know, no one is driving them." And, if only 246 of the laptops lost by the Census Bureau contained "personal data," what were our census-takers using the other ones for—playing World of Warcraft in the field? And, what

exactly would constitute a proper use of personal information about United States citizens lost by a Federal agency?

Crime Begins in the Home
According to Symantec's semi-annual “Internet Threat Report,” home computer users are becoming the preferred target of cyber criminals. The report noted an 81 percent jump in the number of phishing emails in the first half of 2006 over the previous six months. Among home users surveyed, just 46.3% say their anti-virus software is up-to-date.
More Information: http://news.com.com/2102-7349_3-6118920.html?tag=st.util.print

GE Employees Experience the Future
A laptop computer stolen from the locked hotel room of a General Electric employee held the names and Social Security numbers of approximately 50,000 current and former GE employees. A company spokesperson said GE is offering all affected individuals a year of free credit monitoring.
More Information: http://www.wten.com/Global/story.asp?S=5452721&nav=6uyN

Free Credit Report Scam Sites
This month marks the one-year anniversary of the law that entitles Americans to get free copies of their credit reports from each of the three main credit bureaus every year. There is only one website, AnnualCreditReport.com, where you can order or download your free credit reports. Unfortunately, studies have found that there are over 100 fraudulent sites that are misspellings of the real site.
More information: http://www.scambusters.org/freecreditreports.html

Bad Chemistry at Purdue
Purdue University is notifying approximately 2,500 individuals who were students at the school in 2000 that their personal data may have been compromised. The data include names and Social Security numbers. A security check of an administrative workstation in the University's Chemistry Department found that files might have been accessed by a cyber intruder.
More Information:
http://www.insideindianabusiness.com/newsitem.asp?ID=19775&print=1

Mac Invulnerability Myth Reaches Apple
Apple issued an advisory admitting that wireless flaws are present in the Mac notebook AirPort. Software drivers for this built-in wireless device are vulnerable to exploitation in a well-known manner and one very similar to the way 3rd party wireless cards for PC’s have been exploited in the past.
The advisory: http://docs.info.apple.com/article.html?artnum=304420

****