Volume 3, Number 7 **July 2006**

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

What to Watch Out for This Month -- Microsoft June Security Updates – Security Screw-Up of the Month -- Security Newsbytes -- Arrests and Convictions

What to Watch Out for This Month

There were 162 reported Phishing alerts during the month of June, of which 96 involved the banks and credit unions listed below. 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. Information for this report was gathered from various sites including:
http://www.trendmicro.com/en/security/phishing/overview.htm
http://www.millersmiles.co.uk

Androscoggin Bank
Bank of America
Barclays Bank
Capital One Bank
Chartway Federal Credit Union
Chase Bank
CitiBank
EDS Credit Union
Flagstar Bank
Florida Credit Union
JPMorgan Chase & Co
Halifax Bank
HSBC Bank
Indiana University Credit Union
Lloyds TSB Bank
MBNA America Bank
Mid America Bank
Nationwide Online Banking
NCUA
North Fork Bank
Ohio Savings Bank
Prosperity Bank
Royal Bank of Scotland
St. George Bank
University of Utah Federal Credit Union
Vision Federal Credit Union
Wachovia Bank
WAMU Bank
Wells Fargo Bank

1. Phishing Scams

Subject: eBay - FPA NOTICE: eBay Registration Suspension - Abusing eBay
Bait: An email from the eBay abuse department asking you to confirm/update/verify your account data at eBay by visiting the given link. The link directs you to a site that is unsecured. The Web site is fake.
Security Tip: The REAL URL of the spoof website looks nothing like the actual eBay URL.
Sample: http://www.millersmiles.co.uk/report/2824

Subject: America Online – Last Notice!!!
Bait: An email asking you to confirm/update/verify your account data at America Online by visiting the embedded link.
Security Tips: America Online never sends their users emails requesting personal details in this way. The REAL URL of the spoof website looks nothing like the actual America Online URL.
Sample: http://www.millersmiles.co.uk/report/2902

Subject: PULSE EFT – Electronic Funds Transfer Alert!
Bait: An email asking you to confirm your ATM Debit card and your scheduled payment.
Security Tips: PULSE EFT never sends their users emails requesting personal details in this way. The REAL URL of the spoof Web site looks nothing like the actual PULSE EFT URL.
For more information: http://www.millersmiles.co.uk/report/2899

Subject: Educational Systems FCU – Important message regarding your Bill-Pay deactivation notice
Bait: An email asking you to confirm/update/verify your account data including your user ID and password at Educational Systems Federal Credit Union by clicking on the embedded link.
Security Tips: Educational Systems Federal Credit Union never sends their users emails requesting personal details in this way. The REAL URL of the spoof website looks nothing like the actual Educational Systems Federal Credit Union URL.
Sample: http://www.millersmiles.co.uk/report/2930

2. Hoaxes and Scams

Missed phone call scam - An email message warns that answering a missed call on your mobile phone can lead to high phone charges when you attempt to claim a $40 prize by calling another number. It is untrue that the caller will be instantly charged $100.00 for the first call.
More Information: http://www.hoax-slayer.com/missed-call-phone-scam.html

Toxic floor cleaner scam - An email claims that household pets have died as a result of licking floors cleaned with the Swiffer Wetjet cleaning system. The claims in the email rumor are only rumors. A safety warning in the Swiffer Wetjet users guide does advise you to keep the product out of reach of children and pets. However, such warnings are present on many cleaning products and do not in any way imply that animals (or children) could be harmed by licking residue left after use.
More Information: http://www.hoax-slayer.com/swiffer-pet-death.html
Swiffer FAQ: <http://homemadesimple.custhelp.com/cgi-bin/homemadesimple.cfg/php/enduser/std_alp.php?p_sid=CKVB_uRh>

3. Virus Alerts
A JavaScript key-filtering flaw in all versions of Internet Explorer and Mozilla Firefox Web browsers could be exploited to gather sensitive data surreptitiously as users enter it on their computers. The flaw also affects SeaMonkey, the successor to Mozilla
More information:
http://www.informationweek.com/story/showArticle.jhtml?articleID=188702223

Microsoft June Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing this update. June was a busy month for Microsoft. There were eight "critical" updates: MS06-021 through MS06-028.
More information: http://www.microsoft.com/technet/security/bulletin/ms06-jun.mspx

The next set of Microsoft Security updates are scheduled for release on July 11th.
Security Tip: Be sure your operating system, Windows and Mac alike, is set to receive updates automatically.

Interesting questions: "If the updates are 'automatic,' why do you have to check on them?" "If they are 'automated,' why do you have to do them manually?" "Does everybody do this routine maintenance thing?" "Why doesn't Microsoft just fix the problem with the automation?"

An easy answer: Updating your software is about as interesting a task as backing up your files, or watching paint dry. Automated updating improves the chances that updates will be applied in timely fashion, so it's a good idea to use it. It can help keep bad things from happening. However, there is always a chance that an automatic update may be missed or fail for some reason. It is a good idea to check your updates once a month and apply any missing ones manually.

Security Screw-Up of the Month

Getting around to it - Senior Energy Department officials learned on June 7th that a cyber intruder stole a file in September 2005 containing names and Social Security numbers of 1,500 workers at the Energy Department's nuclear weapons agency from a computer system at the National Nuclear Security Administration (NNSA). Why did the news about the theft not see the light of day until 9 months later? NNSA Administrator Linton Brooks told a House hearing that he learned of the security breach last September, but failed to inform DOE Samuel Bodman about it because he assumed the DOE's counterintelligence office had briefed the two senior officials. Secretary Bodman has directed that the individuals affected by the data theft be notified immediately.

Editor's Note (Wyman): Higher-ups keep showing us regularly that they don't understand zip about computer security, and since they don't know what to do when a breach occurs, they do nothing. "After all, the lights are on, the phones are working, my email's OK, my printer prints, and *I'm here,* so what's the big problem?" Cybercrime is often invisible and silent. It may be days or weeks before it is discovered, and months or years before its victims feel the effects. By then the perpetrator's trail is ice cold. The reports we see in the media prove that the bigger the breach, the bigger the non-response.
More Information: http://www.msnbc.msn.com/id/13232863/

Security Newsbytes

Just keeps getting better - A computer security breach at the Agriculture Department during the June 2nd weekend put the personal information of 26,000 current and retired employees and contractors at risk, according to a June 22nd announcement on the FirstGov Federal information Web portal.
More information: http://www.fcw.com/article94991-06-22-06-Web

FBI recovers stolen VA laptop -- The Veterans Affairs Department said that law enforcement officials had recovered the stolen laptop containing the personal data of more than 26 million veterans, and that initially it looks as though the data has not been accessed. More Information: http://www.gcn.com/online/vol1_no1/41204-1.html

Phone phishing - An attacker sends a spoofed spam email that appears to come from a bank, financial services institution or government agency, claiming that the user's account has been frozen due to fraudulent activity. The email tells users to call a phone number included in the email to reactivate their credit cards or other financial accounts. When a user calls this number, a friendly voice message claiming to be a financial institution prompts the user to enter an account number and/or PIN. The reassuring voice explains that the account has been reactivated. Unfortunately for the unwitting user, a fraudster has just harvested vital account information.
More Information:
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1193304,00.html

More PayPal woes - PayPal says it has fixed a flaw in its Web site that was being exploited by phishers to gather sensitive personal and financial data from its customers. Attackers exploiting the vulnerability were redirecting PayPal users to a phony Web site. Code on the PayPal Web site has been changed to block this type of attack; PayPal is also taking steps to help shut down the phony site.
More Information:
http://www.zdnetasia.com/news/security/printfriendly.htm?AT=39368806-39000005c

Arrests & Convictions

Timothy Mattos has been sentenced to 70 months in prison for reselling Verizon Wireless prepaid cellular service card personal identification numbers (PINs) that he stole from the company's computer system. The thefts occurred while Mattos was employed as a Verizon customer service representative and continued for a year after he left the company. Mattos has also been ordered to pay US$21.3 million in restitution.
More Information:
http://www.bizjournals.com/sacramento/stories/2006/06/12/daily15.html?jst=m_ln_hl&surround=lfn

Ryan Pitylak has agreed to pay US$1 million to settle a lawsuit brought by Microsoft and the State of Texas accusing him of sending millions of unsolicited commercial email messages on a daily basis. Authorities have also seized the assets Pitylak acquired as a result of sending spam. Pitylak has written contritely on his blog that he understands now why spam is such a problem, and a better man for his legal problems, has started a consulting company to advise others on protecting their systems from spam.
More Information:
http://www.silicon.com/research/specialreports/thespamreport/0,39025005,39159291,00.htm

****