Volume 3, Number 8 August 2006

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

What to Watch Out for This Month -- Microsoft July Security Updates – Security Newsbytes -- Arrests and Convictions

What to Watch Out for This Month

There were 156 reported Phishing alerts during the month of July, 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

Alaska USA Federal Credit Union
Bank of America
Barclays Bank
Capital One Bank
Chase Bank
CitiBank (see also Phishing Scams below)
Clydesdale Bank
Columbus Bank and Trust Co-operative Bank
Downey Savings
Elevations Credit Union
Fifth Third Bank
Flagstar Bank
JPMorgan Chase & Co
Halifax Bank
Household Bank
HSBC Bank
Indy Mac Bank & Co
LaSalle Bank
Lloyds TSB Bank
Michigan Schools & Government Credit Union
Mid America Bank
Nationwide Online Banking
NatWest Bank
NCUA
North Fork Bank
PNC Bank
Prosperity Bank
Providian Bank
Republic Bank & Trust Company
Royal Bank of Canada
Royal Bank of Scotland
Santa Barbara Bank & Trust
TD Canada Trust Bank
University of Colorado Federal Credit Union
Wachovia Bank
WAMU Bank
Wells Fargo Bank

1. Phishing Scams
Subject: MasterCard – Activate today your MasterCard SecureCode!
Bait: An email asking you to confirm/update/verify your account data at MasterCard by visiting the embedded link
Security Tip: MasterCard never sends their users emails requesting personal details in this way.
Sample: http://www.millersmiles.co.uk/report/2978

Subject: Bellsouth – Bellsouth Billing Updates
Bait: An email asking you to verify your billing information at Bellsouth by clicking on the embedded link.
Security Tip: Bellsouth never sends their users emails requesting personal details in this way.
Sample: http://www.millersmiles.co.uk/report/3021

Subject: Comcast – Billing Information Update
Bait: An email asking you to update or verify your latest billing information.
Security Tip: Comcast never sends their users emails requesting personal details in this way.
Sample: http://www.millersmiles.co.uk/report/3033

Subject: PayPal – Your PIN is incorrect
Bait: An email letting you know your PayPal PIN has been compromised.
Security Tips: PayPal never sends their users emails requesting personal details in this way.
PayPal users are regularly targeted for phishing scams and other kinds of fraud.
Sample: http://www.millersmiles.co.uk/report/3084

Subject: CitiBank Citibusiness – Someone has tried to log in to your account.
Bait: A typical phishing email, but with a couple of twists designed to fool the wary. The first is a nice touch-- the email includes the IP address of the imaginary suspect. It goes on to ask you to click on an embedded link and log in to your account so you can confirm your account information. This takes you to the phishing Web site, convincing graphics and all. Next twist: If you enter incorrect information to test whether the fake site is for real--a tactic used by some security-savvy people--it submits the data you've provided to the actual Citibusiness login site. When the actual site generates an error message, so does the phishing site, thus making it look more real.
Security Tip: Phishers are getting more clever. Security-savvy people who think they can tell a bogus site from a real one can be tricked. Your personal information is too valuable to risk.
Samples and more information:
http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

2. Hoaxes and Scams
Mr. Clean is not so clean: An email hoax warns users that Mr. Clean Magic Erasers contain formaldehyde and can pose significant health risks to users. This is a hoax.
More Information: http://www.hoax-slayer.com/magic-erasers-hoax.html

Rumors of my death have been greatly exaggerated: In June 2006 yet another fake news story falsely announcing the untimely death of a celebrity began hitting inboxes. This time, the "victim" is US-based actor and writer Jaleel White, perhaps best known for his role as the irritating but lovable Steve Urkel in the comedy series "Family Matters". However, Jaleel White is alive and well. The actor has now publicly declared this fact on his official website.
More information: http://www.hoax-slayer.com/current-issue.html#three

3. Virus Alerts
An advisory on the Microsoft Web site warns users against a new virus that exploits a vulnerability in its PowerPoint presentation software, allowing hackers to infiltrate computer systems.

Security Tip: You already know not to open unexpected attachments, even from friends, but maybe you would let a PowerPoint file slide. No more! If the file extension is PPT, do not open the file without first confirming that your friend did in fact send it.
More Information: http://www.microsoft.com/technet/security/advisory/922970.mspx

Microsoft July Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing this update. July was another busy month for Microsoft; there were five (5) "critical" updates released: MS06-035, MS06-036, MS06-037, MS06-038 and MS06-039, and two (2) "important" updates: MS06-033 and MS06-034.
More information: http://www.microsoft.com/technet/security/bulletin/ms06-jul.mspx
The next set of Microsoft Security updates is scheduled for release on August 8th.
Security Tips: Be sure your operating system, Windows and Mac alike, is set to receive updates automatically.
It appears that new vulnerabilities are being detected and exploited shortly after updates are released. And Microsoft updates for these new vulnerabilities are a month away. So just because you've updated your computers, it does not mean you are protected. You should continue to practice other safe computing.

Security Newsbytes

Five men have been charged with aggravated theft for their alleged roles in stealing data from a LexisNexis database. The men allegedly used stolen or forged accounts to access personal information, including Social Security numbers belonging to a number of celebrities. LexisNexis says information belonging to more than 300,000 individuals was stolen.
More Information: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/30/AR2006063001784_pf.html

Gmail Phishing Scam - A recently detected phishing scam targeting Gmail users pretends to offer a US$500 cash prize. Recipients are directed to a web site where they are asked to register to receive the prize. They are also asked to pay a membership fee of less than US$10. The phony registration site actually hosts malware.
More Information: http://www.theregister.co.uk/2006/07/12/gmail_phish/print.html

Arrests & Convictions

FBI agents arrested Steven Rambam (also known as Steve Rombom), the owner of a company that bills itself as the largest privately held online investigative service in the United States. Rambam was arrested by FBI agents just moments before he was to lead a panel discussion on privacy at the HOPE hacker conference in New York City.
More Information: http://blog.washingtonpost.com/securityfix/

German police have arrested five men in Bonn on suspicion of stealing €30,000 through phishing fraud and Trojan horse attacks.
More Information:
http://news.zdnet.co.uk/internet/security/0,39020375,39181670,00.htm

****