Volume 3, Number 5 **May 2006**

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

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

What to Watch Out for This Month

There were 162 reported Phishing alerts during the month of April, of which 22 involved banks and credit unions. Don't take the bait! Before you respond to any email requests for personal information, call the 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.

Alaska USA Federal Credit Union
Barclays Bank
BB&T
Capital One Bank
Chase Bank
Chase Manhattan Bank
CitiBank
DM Federal Credit Union
EGG Online Bank
JP Morgan Bank
JPMorgan Chase & Co
Halifax Bank
HSBC Bank
National City Bank
Nationwide Online Banking
NatWest Bank
Nordea UK Bank
U of C Federal Credit Union
UW Credit Union
WAMU Bank
Wachovia Bank
Wells Fargo

1. Phishing Scams

Subject: **PayPal – Account Notification**

Bait: You receive an email asking you to confirm a new email address was added to your account. The email then provides a link for you to click on if you did not authorize the change. The link directs you to a site that is secure but will then redirect you to a second site, which is unsecured. Both websites are fake. **Security Tip**: When you log in to your PayPal account, be sure to open up a new Web browser window and type in the PayPal URL (https://www.paypal.com) yourself. This will help ensure that you are taken to a secure, genuine PayPal Web site.

Sample: http://www.millersmiles.co.uk/report/2550

Subject: Amazon - **Congratulations! Amazon.com Gold Box Reward**

Bait: An email asks you to confirm/update/verify your account data at Amazon by visiting the embedded link. You'll notice that the site does not have a security lock displayed in your browser. This indicates the site is not secure, and its absence is a telltale sign that the site may be bogus.

Security Tip: Beware of using links embedded in email messages. Amazon never sends their users email requesting personal details in this manner. The REAL URL of the spoof Web site looks nothing like the actual Amazon URL.
Sample: http://www.millersmiles.co.uk/report/2547

Subject: **American Express -- Beware Phony Log In Screen**
American Express has reported that some customers who go directly to AmEx's secure web site are getting an authorized and malicious pop up box asking for information such as SS number, Mother's maiden name and date of birth. This may be the first time that a phishing attempt has actually targeted the actual web site of a company rather than utilizing a fake site.
For more information: http://www.eweek.com/article2/0,1895,1955288,00.asp

Subject: **eBay – Confirm Your Online eBay Records**
Bait: An email asks you to confirm/update/verify your account data at eBay by visiting the embedded link. When you visit the site, it gathers your personal account information such as registration number and password by means of a spoofed Web page.
Security Tip: The REAL URL of the spoofed Web site looks nothing like the actual eBay URL.
Sample: http://www.millersmiles.co.uk/report/2514

Subject: **PayPal – Account Review**
Bait: An email asks you to confirm/update/verify your account data at PayPal by visiting the embedded link. You will be taken to a spoofed Web site where your personal information will be captured for use by phishers.
Security Tip: PayPal never sends their users email requesting personal details in this manner.
Sample: http://www.millersmiles.co.uk/report/2534

2. Hoaxes and Scams
Jury Duty Anyone? Two emails now in general circulation warn users that scammers are committing identity theft by intimidation. And the emails are telling you the truth. The scammers phone potential victims and threaten them with prosecution for failing to report for jury duty unless they reveal sensitive personal information.
More Information: http://www.hoax-slayer.com/jury-duty-scam.html

3. Virus Alerts
WORM_LETUM.A: A worm that propagates via email -- and something of an old story by now -- the email warns you about a worm, but ***the email contains the worm it is warning you about***. This email message appears to be a warning sent by an engineer working for Symantec, a reputable maker of antivirus software. It isn't. The attachment is the "payload" and contains a worm, which, if opened, may infect your computer and use it to pass itself on to others whose email addresses are stored on your computer. Below is a sample of an email message (clumsily worded) that the worm creates and sends out to others:

> From: Symantec Security Response [pete{BLOCKED}rrie@symantec.com]
> Subject: (any of the following)

- Customer Support
- Re:
- Re:Warning
- Security Response
- Virus Alert
- Virus Report
- Warning!

Message Body:
Dear User,

Due to the high increase of the Letum worm, we have upgraded it to Category B. Please use our attached removal tool to scan and disinfect your computer from the malware.

If you have any comments or questions about this, then please contact us.

Regards
Pete{BLOCKED}rrie
Senior Anti-Virus Researcher / Senior Principal Software Engineer

©1995 - 2006 Symantec Corporation All rights reserved.

Attachment: test.exe

More information:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FLETUM%2EA

Microsoft April Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing the update. There were three "critical" updates released in April: MS06-013, MS06-014 and MS06-015. All of these security patches address vulnerabilities that could allow a hacker to execute code on your computer by remote control and without your knowledge. There was one "important" update released as well: MS06-016. This patch provides a cumulative security update for Outlook Express. There was also one “moderately” critical update released: MS06-017 for Microsoft Front Page Extensions, a tool used to create Web pages.
More information: http://www.microsoft.com/technet/security/bulletin/ms06-apr.mspx

The next set of Microsoft Security updates is scheduled to be released on May 9th.
Security Tip: Be sure your operating system, Windows and Mac alike, is set to receive updates automatically.

Security Newsbytes

Apple has discovered more flaws that may put Macintosh computers at risk for network-based attacks. Five of the flaws identified relate to how the Macintosh OS handles various common image file formats including BMP, TIFF and GIF.

Security Tips: Until Apple issues a fix, be extra careful about opening graphics files you receive as email attachments. Your best protection is to make sure the antivirus software on your Mac is working and up-to-date.
More information: http://news.zdnet.com/2100-1009_22-6063931.html

Arrests & Convictions

- - Zhijian Chen has been fined US$84,000 for using deceptive advertising techniques that urged computer users to purchase a phony anti-spyware program.
More information: http://www.techweb.com/wire/186100344

An Australian Federal Court has rejected defense claims made by Clarity1's Wayne Mansfield that his company emails, in which 56 million email messages were sent to companies, were for commercial purposes and not spam. Mansfield claimed that the recipients had agreed to receive them and that his company was allowed to use lists of harvested email addresses acquired before Australia's Spam Act took effect in April 2004. The judge didn't buy these technicalities. Mansfield and Clarity1 were found guilty and will face yet-to-be-determined penalties.
More information:
http://www.zdnet.com.au/news/communications/print.htm?TYPE=story&AT=39251708-2000061791t-10000003c

==========

Copyright 2006, SANS Institute (www.sans.org).

Editorial Board: Dave Moore, 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.