What to Watch Out for This Month

Top Ten Phished Sites
A special feature for OUCH readers. CipherTrust is providing OUCH readers with a list of the ten sites that were most often used for phishing. This is data that comes from the thousands of organizations that use IronMail to filter their mail so it is authoritative (www.ciphertrust.com)

EBay
PayPal
Bank First
Amazon.com
Chase Bank
Wells Fargo
Bank of Oklahoma
Barclays Bank
Bank of America
People's Bank

There were 192 reported Phishing alerts this month and of that 64 were against the banking industry -- the threat is still widespread. The information below was gathered from various sites, including http://www.millersmiles.co.uk/archives/current & http://www.antiphishing.org.

1. Phishing Scams
Subject: Halifax Online Banking Update
Bait: Fake email asking you to confirm your account data by clicking on the embedded link.
Goal: To have you visit the Phishing site and reveal your logon information.
Sample: http://www.millersmiles.co.uk/report/1446

Subject: Armed Forces Bank Notice
Bait: Fake email asking you to confirm/update/verify your account data by clicking on the embedded link.
Goal: Capture your Social Security number, your customer ID, and password.
Sample: http://www.millersmiles.co.uk/report/1428

Subject: PayPal Special Department Notice (Anti-Fraud Alert 98760)
Bait: Fake email asking you to confirm/update/verify your account data by clicking on the embedded link.
Goal: To have you visit the Phishing site and reveal your logon information.
Sample: http://www.millersmiles.co.uk/report/1420

Subject: Bank of Oklahoma - Notice: Unauthorized Charge to Your Bank Account
Bait: Fake email asking you to confirm or update or verify your account data by clicking on the embedded link.
Goal: To have you visit the Phishing site and reveal your logon information.
Sample: http://www.millersmiles.co.uk/report/1450

Subject: First Credit Union - Renew Your Account Information
Bait: Fake email asking you to confirm or update or verify your account data by clicking on the embedded link.
Goal: Capture as much personal information as possible.
Sample: http://www.millersmiles.co.uk/report/1495

2. Hoaxes and Scams
Lottery Hoax: A money transfer hoax that sets out to convince people they have won a lottery. Naturally, no money is ever paid out and all kinds of transfer fees are collected from the unsuspecting people who respond. http://tinyurl.com/aycl5 or http://www.fsecure.com/hoaxes/interlotto.shtml

3. Virus Alerts
New Sober Variant now worldwide: Anti-virus firms started to get reports about a new dropper for the Sober.S worm at noon on October 6th, 2005. When the dropper is run, a message box is displayed as a decoy. http://tinyurl.com/92uhn or http://www.f-secure.com/v-descs/sober_sdr.shtml

Samy Worm Exploits Cross-Site Scripting Hole: The Samy worm is believed to be among the first to exploit a cross-site scripting vulnerability. It has been alleged that a MySpace.com community site member created the worm to increase his popularity rating. http://tinyurl.com/7w7dm or http://www.computerworld.com/printthis/2005/0,4814,105484,00.html

Three Things You Can Do to Make Your Computer & Information More Secure
1. Keep your operating system & software applications up to date & patched.
Upgrade to "Microsoft Update" which provides many patches for Microsoft Windows and other Microsoft programs, such as Microsoft Office, Visio, Project, Publisher, Microsoft Exchange Server, and Microsoft SQL Server, at one convenient location. This service from Microsoft includes all the updating and patching features of
Windows Update and Office Update, plus downloads for other Microsoft products—even those still in Beta—as well as updates for software drivers. Go to the Windows Update page, click on the "News" item "Upgrade to Microsoft Update" in the lower right hand corner, and follow the instructions. Remember: Making the patching process automatic will help minimize the risk of your computer being infected or getting hacked.

Windows:

2. Backups, Backups and Backups
How important is your data to you? You can respond to this question with words, but the steps you take to protect your data are the real answer. Backups are an essential part of data protection. Why don't people make them?

* They don't understand how important they are, because they haven't had a catastrophic loss (yet).
* They don't know how to make them.
* They forget to do them because they don't have a routine for doing backups.
* Doing the backup is time-consuming and they have more urgent things to do.

Here are some software packages available to you.
http://tinyurl.com/7zg62 or http://www.pcmag.com/category2/0,1738,4798,00.asp

3. Avoid Phishing scams & protect your identity.
Beware of fraudulent emails and Web sites that masquerade as messages from familiar institutions. By tricking you into disclosing your Social Security Number, PIN number, a password, or an account number, identity thieves can drain your bank account or run up bills on your credit card.
The best ways to avoid becoming a victim are:
* Never disclose personal information in response to an unsolicited email
* Never click on the link in the email
* Always access the Web site by manually typing in the Web address in a browser

You can report suspected Phishing scams by sending an email to reportphishing@antiphishing.com or spam@uce.gov, or by visiting these Web sites http://www.ifccfbi.gov or http://www.consumer.gov/idtheft.

Security Newsbytes

Phishing Attack Targets Yahoo Photos Users: A new phishing attack targeting Yahoo Photos users arrives as an email or instant message that appears to come from someone you know that asks you to look at vacation or birthday party photos. http://tinyurl.com/8kf4v or http://www.computerworld.com/printthis/2005/0,4814,104946,00.html

Mozilla Releases Updated Versions of Firefox and Mozilla Suite: A flaw in the way earlier versions of Firefox handle Unix and Linux shell commands could allow unauthorized software to run on vulnerable machines. http://www.computerworld.com/printthis/2005/0,4814,104825,00.html or http://tinyurl.com/cnnk3


Arrests & Convictions

Man Sentenced to Five Months for Attempted Cyber Scam: A man in Norway was sentenced to five months in prison for a cyber extortion scam. He created a web site for the Inner Norwegian Seamen's Church and placed pornographic images on it, then blamed the offensive photographs on unknown cyber attackers and charged the church 84,000 NOK ($13,059) as a deposit to clean up the site and then never did the work. http://www.aftenposten.no/english/local/article1139982.ece or http://tinyurl.com/cfyot


Spammer's Sentence is Under Seal: Anthony Greco was sentenced in a closed session for sending nine million spam email messages through instant messages to members of MySpace.com. Greco reached a plea agreement with prosecutors under which he would serve a sentence of between 18 months and two years in prison in exchange for a guilty plea. http://tinyurl.com/7ofle or http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/10/17/financial/f190259D40.DTL&type=printable
Training on What You Should Know About Phishing Scams See how fraudulent phishing e-mail messages can trick you into sending personal information to an identity thief. You'll also learn three things you can do to protect yourself from being hooked by an identity-theft scam. 
http://download.microsoft.com/download/3/a/4/3a426133-65eb-4de6-af26-2786e3967d79/Phishing.exe
or http://tinyurl.com/bbgbx

Copyright 2005, 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.