

**In This Issue**

*What to Watch Out for This Month --- Security Newsbytes -- Arrests and Convictions -- Training on How to Deal with Spam Email --- Four Things You Can Do*

**What to Watch Out for This Month**

There were fewer reported Phishing alerts this month, and while that is encouraging, the threat is still widespread. Information was gathered from various sites including <http://www.millersmiles.co.uk/archives/current> & <http://www.antiphishing.org>. The financial institutions listed below have been the object of Phishing attacks frequently in the last month.

Sun Trust	Natwest	HSBC
Barclays	Nationwide	Armed Forces Bank
Washington Mutual (WAMU)	Citibank	Visa
EBay	South Trust	
Bank of America	Regions	

**1. Phishing Scams**

Subject: **Bank of America - Online Banking Alert (Your Online Banking is Blocked)**

Bait: Fake email asking you to confirm/update/verify your account data at Bank of America by visiting the embedded link.

Goal: To have you visit the Phishing site and reveal your logon information to Bank of America so it can be used for fraudulent purposes.

Sample: <http://www.millersmiles.co.uk/report/1251>

Subject: **VISA & MasterCard Telephone Credit Card Scam**

Bait: Receiving a phone call from the Security and Fraud Department at VISA, indicating that your card has been flagged for an unusual purchase pattern.

Goal: To get you to reveal the three-digit security codes found on the back of some credit cards.

Explanation: <http://www.snopes.com/crime/warnings/creditcard.asp>

Subject: **eBay – FPA NOTICE: eBay Account Violation Notice**

Bait: Fake email asking you to confirm/update/verify your account data at eBay by visiting the embedded link.

Goal: Capture as much information about your eBay account as possible.

Sample: <http://www.millersmiles.co.uk/report/1253>

Subject: **Armed Forces Bank Online Expiration Notice**

Bait: Fake email asking you to confirm/update/verify your account data at Armed Forces Bank by visiting the embedded link.

Goal: Capture as much personal information as possible.

Sample: <http://www.millersmiles.co.uk/report/1284>

Subject: **HSBC – Your Account Is About to Expire**

Bait: Fake email asking you to confirm/update/verify your account data at HSBC by clicking on the embedded link.

Goal: Capture as much personal information as possible.

Sample: <http://www.millersmiles.co.uk/report/1289>

Subject: **eBay – Message from eBay Member**

Bait: Fake email asking you to confirm/update/verify your account data at eBay by visiting the embedded link.

Goal: Capture as much personal information as possible.

Sample: <http://www.millersmiles.co.uk/report/1300>

## 2. Hoaxes and Scams

**Hurricane Rita Stirs up Scammers:** As Hurricane Rita's winds whipped up off the Gulf Coast and officials evacuated over a million area residents, Internet watchdogs warned that another wave of chaos may not be far behind the storm, in the form of scammers.

<http://www.interentnews.com/xSP/article.php/3551211>

## 3. Virus Alerts

**New Bagle Trojans spammed out:** Once was not enough for the Trojan Bagle DI-U. Sophos, an anti-virus research company, has warned that a hacker is spamming several new versions of the Trojan horse to millions of email addresses all over the world.

<http://www.sophos.com/virusinfo/articles/bagledlu2.html>

**Trojan Tries to Jump from Phones to PCs:** The Cardtrap.A Trojan horse program, which attacks the operating system of Symbian mobile phones, tries to “jump” to PCs when users insert infected phone memory cards into their computers. Cardtrap.A pretends to be pirated software for mobile phones. The good news? Cardtrap.A requires user interaction for the PC to become infected, and failed to launch when tested on some Windows XP SP2 and Windows 2000 systems.

[http://www.f-secure.com/v-descs/cardtrap\\_a.shtml](http://www.f-secure.com/v-descs/cardtrap_a.shtml)

## Security Newsbytes

**Exploit Released for Firefox, Netscape Flaw:** A security update for FireFox and Netscape browsers has been released which fixes a flaw that could let attackers secretly run malicious software on PC's.

[http://news.com.com/2102-1002\\_3-5863451.html?tag=st.util.print](http://news.com.com/2102-1002_3-5863451.html?tag=st.util.print)

**Hacked Home PCs Fueling Rapid Growth in Online Fraud:** A recent report shows that online criminal activity of nearly every variety surged in the first half of 2005. This was fueled in large part by software security flaws and a huge increase in the number of home computers being "zombified" and used to distribute spam, spyware, and viruses without the knowledge or consent of their owners.

[http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091900026\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091900026_pf.html)

**Spyware Is Increasingly Stealing Identities:** A significant portion of spyware is designed specifically to steal identities, underscoring a trend toward more malicious use of such software by criminals.

<http://www.ds-osac.org/News/story.cfm?contentID=35750>

**Phishing Targets Yahoo! Users:** There is a new twist on Phishing schemes that targets Yahoo! users by using alternate Yahoo! pages. For example, users receive an instant message or email (supposedly from a friend) wanting to show you photos located on the Yahoo! Photos web site. The embedded link takes the user to a phony Phishing site. When the user logs in, the phony site records the user's ID and password, and then forwards the user on to the real Yahoo photo site.

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=296>

**Berkeley Recovers Stolen Laptop:** Campus police at the University of California, Berkeley have recovered a stolen laptop that contained personal information on more than 98,000 of the school's graduate students.

<http://www.pcworld.com/resource/printable/article/0,aid,122576,00.asp>

**VISA and MasterCard Do Not Have To Inform Card Holders of Security Breach – For Now:** San Francisco Superior Court Judge Richard Kramer denied a request for a preliminary injunction that would have required credit card companies like MasterCard and VISA to inform individual California credit card holders when their accounts are at risk for fraud.

[http://news.com.com/2102-7350\\_3-5879179.html?tag=st.util.print](http://news.com.com/2102-7350_3-5879179.html?tag=st.util.print)

## Arrests & Convictions

**Teen Sentenced for T-Mobile Break-In:** A Massachusetts teenager has been sentenced to 11 months in a juvenile detention facility for his role in several cyber attacks and threats, including the T-Mobile break-in that resulted in Paris Hilton's cell phone address book being exposed in the Internet.

<http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/4249780.stm>

**Former Student Sentenced for University Computer Intrusion and Data Theft:** Christopher Andrew Phillips, formerly a student at the University of Texas at Austin, has been sentenced to five years' probation for breaking into the school's computer system and stealing personal data, including Social Security numbers.

<http://www.technologynewsdaily.com/node/1381>

<http://austin.bizjournals.com/austin/stories/2005/09/05/daily12.html>

**Ireland's First Spam Conviction:** Ireland has seen its first conviction under its new anti-spam law. A company called 4's A Fortune Limited was found guilty of sending unsolicited commercial messages to five mobile telephones.

[http://www.theregister.co.uk/2005/09/07/irish\\_spam\\_conviction/print.html](http://www.theregister.co.uk/2005/09/07/irish_spam_conviction/print.html)

**Hackers Admit to Wave of Attacks:** In a deal with prosecutors, Richard "Krashed" Roby, 20, pleaded guilty in federal court in Toledo last month to intentionally damaging a protected computer, after launching a 2003 attack on an online satellite TV retailer that caused at least \$120,000 in losses.

<http://www.wired.com/news/print/0,1294,68800,00.html>

## Training on How to Deal with Spam Email

Watch this video to find out more about how to deal with spyware, what types of spam email messages can be dangerous, and what you can do to help reduce the amount of spam you receive.

<http://download.microsoft.com/download/3/a/4/3a426133-65eb-4de6-af26-2786e3967d79/Spam.exe>

## Four Things You Can Do to Make Your Computer & Information More Secure

### 1. Keep your operating system & software applications up to date & patched.

Microsoft now offers "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: <http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us>

Mac OSX: <http://www.apple.com/support/downloads/> &

<http://www.apple.com/macosx/features/security/>

More info: <http://www.its.monash.edu.au/security/home/patching.html> &

<http://www.softwarepatch.com/>

## **2. Check your Microsoft patches & updates**

Automated updating doesn't always work perfectly. It's a good idea to check on the patches and updates once a month to make sure they are up to date and complete. You can use Microsoft's Baseline Security Analyzer, a free tool, to check your system. MBSA provides you with information about the overall security of your computer as well as information regarding needed configuration changes, updates, patches and fixes.

More info: <http://www.microsoft.com/technet/security/tools/mbsa2/default.msp>.

## **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, an account number, or other personal information, 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](mailto:reportphishing@antiphishing.com) or [spam@uce.gov](mailto:spam@uce.gov), or by visiting these Web sites <http://www.ifcfbi.gov> or <http://www.consumer.gov/idtheft>.

More info: <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm> &

<http://www.atg.wa.gov/consumer/idprivacy/phishing.shtml>

## **4. Protect your desktop computer or laptop**

There's some commercial advertising in this article, but it does explain how to set up some antivirus products, firewall products, and how to detect, remove and protect against spyware using the Microsoft Update Service.

[http://www.washingtonpost.com/wp-srv/technology/interactives/upgradesp05/security\\_2005.html](http://www.washingtonpost.com/wp-srv/technology/interactives/upgradesp05/security_2005.html)

---

Copyright 2005, SANS Institute ([www.sans.org](http://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.