

Alert

Spring 2008


The Official Newsletter of noPhishing.org



I'm Being Audited by the IRS???

A creative new phishing email is bound to get just about anyone's attention. It pretends to be from the IRS and states that your tax return is going to be audited. While most phishing emails are not usually personalized, this scam frequently has your name in it, which makes it appear more authentic. It instructs you to click on links to complete

forms with personal and account information. If you comply, they can use the information to steal your identity.

Relax and remember – the IRS does not send unsolicited, tax-account related emails to taxpayers.



The Bad Guys Offer a Discount

You receive an email from a financial institution offering to sign you up for the MasterCard SecureCode program. And better yet, they offer a 16% discount on future purchases! More Internet security when making purchases plus a deep discount is a win-win situation, right? Wrong!

Con men are counting on you falling for that irresistible combination, but now you know better; while the genuine MasterCard SecureCode program offers the promise of greater security to credit card transactions, be leery of emails soliciting your participation. If you click on the link provided, you will be redirected to a phishing site that looks almost identical to the MasterCard website. Once at the phony site, you will be asked to supply your credit card number, date of birth, the credit card expiration date, and the 3-digit security code from the back of the card. This information provides all that a cybercriminal needs to either access the account or sell it on the black market at top dollar.

According to Carole Theriault, Senior Security Consultant at the Internet security firm Sophos, "Computer users must be wary of simply clicking on links in unsolicited emails and should take time to verify the site address first – it may take a little longer, but will protect your money and identity from preying cybercriminals in the long run. Also, everyone needs to use a little common sense – if it seems too good to be true, it probably is."

Beware of New Vishing Scams



There are 3 new vishing (phone call) scams where the caller claims to be an IRS employee.

The first one focuses on your Economic Stimulus Payment. The caller will ask for your bank account and Social Security numbers in order to process the payment. Don't be fooled. The IRS uses the information on your tax return to process economic stimulus payments.

Another scam claims you are eligible for a "rebate for early filing." The caller then asks for bank account information to make a direct deposit of the "rebate." If you refuse, he tells

you that you can only receive the rebate by direct deposit. The IRS has no such rebate and never demands direct deposit to an account.

Uh-oh, your phone is ringing again! This time the caller tells you that the IRS has mailed a check to you. He says that since the check hasn't been cashed yet, the IRS wants to verify your bank account number. It's just a ploy to obtain personal information about you. Do not respond.

Report any questionable emails or phone calls to phishing@irs.gov.



The Case of the Fraudulent Grand Jury Summons

The Internet Crime Complaint Center (IC3) has released a report of phishing emails containing fake subpoenas. The email looks authentic – complete with a court case number and issuing officers' names. Recipients are directed to click on a link to obtain additional information regarding the summons. Once the link is activated, malware is downloaded to the recipient's computer and can be used to steal personal information.

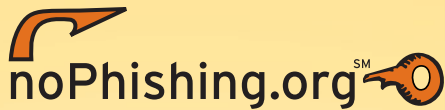
If you receive an email such as this, do not click on the link. Instead, contact the issuing court to check whether it is valid. If it is fraudulent, please file a complaint at www.ic3.gov.



Can You Hear Me Now?

In a new phishing scam targeting Verizon customers, an email tells them there's a problem with their Verizon.com or Verizon Online account, and asks them to click on a link to verify account information. The link takes customers to a fake website that requests credit card and other personal information. Verizon states they do not verify information this way and asks that you not respond. For updates and additional information, visit <http://www22.verizon.com/pages/securityalerts>.

Protect yourself!



This comprehensive website has a wealth of useful information targeted at protecting you and your personal information from phishing attacks and identity theft. It includes commonsense suggestions on how to best protect your confidential information, up-to-date reports of scams, what to do if you think your information has been compromised, and links to several other helpful websites. There's even a fun game called "Phishing Scams – Avoid the Bait" which tests your ability to recognize a phishing attempt.

Sponsored by the Maine Anti-Phishing Coalition (MEAPC), the website strives to provide timely and useful topics for your financial and cyber security. Member banks work together to maintain the site and to create posters, newsletters, and seminars dedicated to increasing your awareness of techniques used in phishing and other scams.

Please invest a few moments of your time exploring www.noPhishing.org. It will be time well spent.



WHAT TO DO IF YOU SUSPECT YOU'VE BEEN PHISHED

- **Immediately notify your bank.**
Be prepared to provide the bank with as much information as possible. They may request that you forward them the phishing email.
- **Place a fraud alert on your credit report** by contacting any of the three consumer credit bureaus below.
 - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
 - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
 - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Contacting one of these companies automatically alerts the other two, who will also place an alert in their records.

When you call, an initial 90-day fraud alert will be placed on your credit report and a free copy of your report will be sent to you. The fraud alert prevents any new accounts from being opened in your name without permission. After the initial fraud alert has expired, if you've filed a police report you can request an extended 7-year fraud alert. To obtain an extended fraud alert, you must provide the credit bureaus with a copy of your initial police report and any other fraud reports they may require.

As of February, 2006, Maine became one of several states to allow consumers to "freeze" their credit reports. With certain

specific exceptions, a security freeze prohibits a credit bureau from releasing your credit report or any information from it without your express authorization. The freeze goes into effect five business days after the credit bureau has received your letter. After ten business days from receiving your letter to place a freeze on your account, the credit bureau will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place. If your credit files are frozen, even someone who has your name and Social Security Number probably would not be able to obtain credit in your name. A security freeze is free to identity theft victims who have a police report, investigative report, or a complaint to a law enforcement agency concerning identity theft.

To place a freeze, you must write to each of the three credit bureaus. Credit bureaus charge a \$10 fee, unless you are a victim who sends a copy of your police report, investigative report, or a complaint to a law enforcement agency concerning identity theft.

Here's what else you should do:

- **File a report** with local law enforcement.
- **Review credit card or bank statements** to make certain all activity was legitimate.
- For more information on identity theft, visit the FTC Identity Theft website. <http://www.ftc.gov/bcp/edu/microsites/idtheft>

Participating Banks in the Maine Anti-Phishing Coalition

