

Gone' Phishing

A Guide to Protecting Yourself from Email Scams

Mississippi State University Cooperative Extension Service

Inside this issue:

Casting a Lure	2
Sniffing Out Those Phishy Emails	3
Frequently Phished Companies	4
Don't Take the Bait: 9 Steps to Avoid Being Phished	5
What to do if You Swallowed the Bait	6
Resources You Can Use	6

Hook, Line, and Sinker

Con artists are betting that you will buy their e-mail solicitations hook, line, and sinker. A new and growing e-mail scam called phishing is fast becoming the number one threat to consumers. Phishing works like this:

1. The Hook: An email is sent to you from what appears to be a legitimate source. For example: you receive an email that appears to be from your credit card company.

2. The Line: The email from the credit card company tells you that there have been major reports of identity theft and you may have been a victim. To verify that your account is ok they will need you to visit the company website and pro-

vide your name, social security number, account number, and mother's maiden name. The email provides a link to the company website at the bottom of the email. All you have to do is click on that link to take you directly to the webpage where you will give them your information.

3. The Sinker: You click on the company link at the bottom of the email which takes you to the company website. Once on the website you enter your name, social security number, account number, and mother's maiden name. You then submit your information to the company. You have just been the victim of a phishing scam.



Casting a Lure

The email you received from the credit card company was an imposter. Someone (the phisher) created an email that appeared to be from the credit card company. These emails are very sophisticated. They use company logos, company colors, and company slogans to make

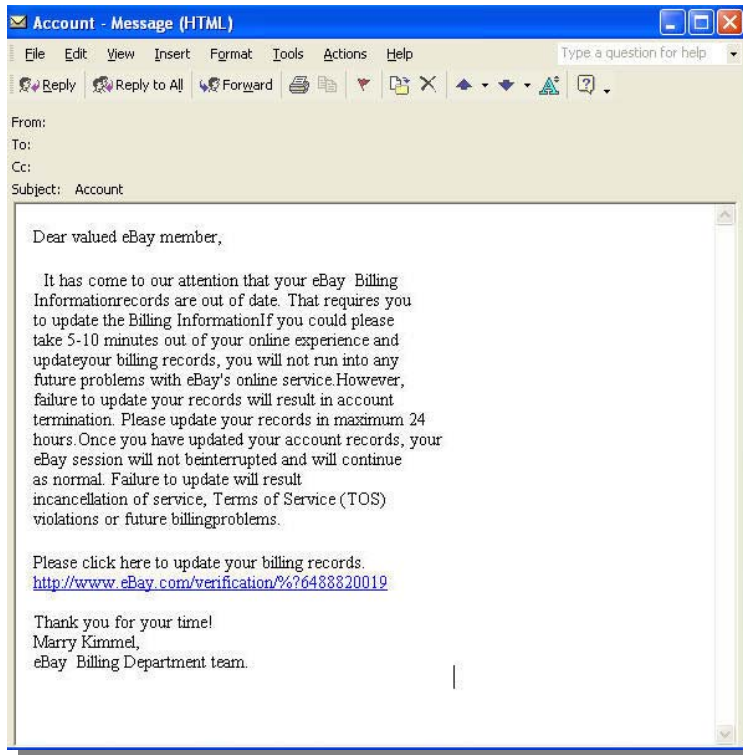
the email appear authentic. They even use the names of real people who work at the company so you will be fooled into believing the email is really from the CEO or an employee of the company.

(Continued on page 2)

Casting a Lure (Continued)

(Continued from page 1)

Take a look at the email below and decide if it is a real email or a phishing email.



Think you can spot a phishy email? Test your knowledge online at: <http://survey.mailfrontier.com/survey/quiztest.html>

While this email may look like the real thing, you can bet it is not. This is an actual email that was sent to thousands of unsuspecting recipients, many of whom fell victim to this scam.

"Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc."

-Anti-Phishing Working Group

Most phishing emails try to create a sense of urgency in the email by telling you that if you do not respond immediately your services will be terminated or suspended. When you click on the link in the email it then directs you to a phony website created by the phisher. The tricky thing about these phony websites are that they also look like the real thing! The phishers recreate the company's website imitating as much detail as they can to fool you into believing it is the official company website.

Once you enter in your personal information, the phisher now has enough information to empty your checking accounts, and make online purchases with your credit cards. The phisher can also create new bank, credit card, insurance and other online accounts in your name, using your identity and you will never know that it has happened until the bills start coming in.

Sniffing Out Those Phishy Emails

Phishers don't just use your credit cards to lure you in, they will also use your insurance company, email service provider, internet auction accounts (like eBay), and government (Secret Service, FDIC, Homeland Security) organizations to reel you in. For a list of some of the most frequently phished companies please see page 4 .

In order to protect yourself from these phishing scams it is important to know what to look for in a suspicious email. If the email includes...

- Statements that are meant to excite or upset you based on false information
- They ask you to respond to the email immediately
- The offer of a prize or special deal but requires your personal information to give you the gift
- A general greeting (such as Dear Customer) instead of a specific greeting (like Dear Jane Doe).
- A link to the company's "secure" website that begins <http://company-security.com>. All secure websites will begin with: <https://company-security.com> (remember, 's' is for security). For example: <https://company-security.com>
- An attempt to get you to enter your financial account information. Stop and think, why would my financial institution that already has my account number need me to enter that particular piece of information?
- A request for multiple pieces of personal information

Then you are likely dealing with a phishy email. If you suspect an email might be phishy, trust your instinct. Phishers can send hundreds of thousands of e-mail out every day so it is important to be on your guard.

According to the E-Commerce Safety Guide, *"The U.S.-based Anti-Phishing Working Group estimates that, in just a two-week period in December 2003, more than*

Did You Know?
Beginning June 1, 2005 an amendment to the federal Fair Credit Reporting Act requires each of the three credit reporting agencies to provide you with a free copy of your credit report.

- Federal Trade Commission
<http://www.ftc.gov/bcp/online/pubs/credit/freereports.htm>

90 phishing attacks hurled more than 60 million fraudulent e-mail messages into the Internet sea; and five percent of the recipients, or 3 million people, took the bait." (https://www.paypal.com/en_US/pdf/PayPal_Safety.pdf)

So why do so many people take the bait? Many people take the bait because the email appears to be from a legitimate source, whether it is a company or person that they know and trust. This is called spoofing.

Spoofing works by stealing legitimate email usernames. The phishers then turn around and use the stolen usernames to send out emails that appear to be from a legitimate person or company. So, even if the email appears to be from your mother, if it asks you for any personal information (financial information, passwords, etc. - not why you don't come to see her more often...) you should automatically assume it is an imposter.

Frequently Phished Companies

While there are millions of phony emails sent out every day there are a handful of companies that are targeted more frequently than others. If you believe you have received a suspicious email from a company you do business with, you should email or call the company to verify the authenticity of the email. Most companies prefer that you **forward the entire email message** to their fraud department so that they can investigate the email and issue the necessary warnings. For a more detailed list of frequently phished companies please visit the Anit-Phishing Working Group website at: http://www.antiphishing.org/phishing_archive.html.

Company	Email Address	PhoneNumber
AOL	TOSEmail1@aol.com	
Amazon	stop-spoofing@amazon.com	
AT & T	missed-spam@worldnet.att.net	
Bank of America	abuse@bankofamerica.com	1-800-432-1000
Bank One	FraudReport@BankOne.com	1-877-226-5663
Citibank	emailspooof@citigroup.com	1-800-374-9700
E-Bay	spooof@ebay.com	
Earthlink	fraud@corp.earthlink.net	
FDIC	www.consumer.gov/idtheft	1-877-IDTHEFT
People's Bank	custserv@peoples.com	1-800-772-1090
PayPal	spooof@paypal.com	1-402-935-2050
SunTrust	abuse@suntrust.com	1-800-227-3782
US Bank	fraud_help@usbank.com	1-800-595-6256
Visa	phishing@visa.com	

Don't Take the Bait: 9 Steps to Avoid Being Phished



Follow these simple steps to swim free of the phishing lures bobbing in your inbox:

Step 1: Always keep your Internet up to date with latest security patches. If you are using Microsoft's Internet Explorer you can go to <http://v4.windowsupdate.microsoft.com/en/default.asp> to download the latest security updates for your computer.

Step 2: Always keep your Antivirus software (Symantec, MacAfee, etc.) current with the latest virus definitions.

Step 3: NEVER click on a link to a website that is located in an email

Step 4: When trying to verify an email, NEVER copy and paste the link contained in an email into your Internet browser's address bar. If you copy and paste an address into the address bar it is just like clicking on the link in an email.

Step 5: Don't be intimidated into acting hastily just because an email warns of dire consequences if you do not respond immediately.

Step 6: Do not under any circumstances give personal information out to an email, web page or pop-up window. A legitimate company will never ask you for personal information.

Step 7: Always make sure that you are using a secure website (a secure website should begin with the URL <https://>, remember, 's' is for security) when entering personal information.

Step 8: Check your bank statements, bills and other financial materials monthly for irregularities.

Step 9: Check your credit report at least once a year. Beginning June 1, 2005 as a citizen of the United States you are entitled to a free credit report from each of the three nation wide consumer-reporting companies, Equifax, Experian, and Trans Union. For more information on how to receive your free credit report please visit the Federal Trade Commissions website: <http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm>.



What to do if You Swallowed the Bait

If you have disclosed personal information and think that you have been the victim of phishing there are several things you need to do immediately:

- ☞ Contact the company directly and ask them to monitor your accounts for suspicious activity. (For a list of frequently phished companies please see page 4.)
- ☞ Notify your financial institutions so that they can place fraud alerts on your credit files.
- ☞ Monitor all financial statements carefully looking for irregularities.
- ☞ Contact each of the three nation wide consumer reporting companies and discuss your situation with a representative. Together, you and the representative can decide if a fraud alert needs to be placed on your file. Placing an alert on your file will prevent phishers from opening new accounts in your name. The following is the contact information for each credit bureau's fraud division:

Equifax
800-525-6285
PO Box 740250
Atlanta, GA 30374

Experian
888-397-3742
PO Box 1017
Allen, TX 75013

TransUnion
800-680-7289
PO Box 6790
Fullerton, CA 92634

Resources You Can Use

- ✦ Anti-Phishing Working Group: <http://www.antiphishing.org/>
- ✦ Beware of Phishing:
http://www.bbbonline.org/idtheft/phishing_cond.asp
- ✦ Department of Justice Special Report on Phishing:
http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf
- ✦ E-commerce Safety Guide:
https://www.paypal.com/en_US/pdf/PayPal_Safety.pdf
- ✦ How Not to Get Hooked by a Phishing Scam:
<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>
- ✦ Is Someone Phishing For Your Information?
<http://www.ftc.gov/bcp/online/pubs/alerts/phishregsalrt.htm>
- ✦ You Can Fight Identity Theft:
<http://www.fdic.gov/news/news/press/2004/pr9304b.pdf>

