

# Protect Yourself Against Identity Theft

Watch out for Phishing Attacks!

A Message from District Attorney  
P. David Soares



Dear Friends,

In the age of the Internet, the information highway runs right into your home computer and the street corner mugging all too often takes place right inside your home. The Internet is a fabulously powerful tool of convenience, efficiency and productivity but it is increasingly being used by ever more sophisticated criminals who have devised pernicious and devious methods for robbing your identity and taking your money.

The best protections against such an attack are care, caution, and vigilance. This booklet talks about identity theft in general and a new form of identity theft called "Phishing" in particular. Every day, tens of millions of Phishing emails are being sent to computer users throughout the world. Protecting yourself is not difficult once you become aware of the problem. Please review this booklet for advice about how to recognize a Phishing attack and how to protect yourself against identity theft. Also, I've included a section on steps to take if you believe that you have become a victim of such an attack.

Don't hesitate to contact my office if you need more assistance.

Sincerely,

P. David Soares  
District Attorney  
Albany County

What is Phishing? .....	1
How Big is the Problem? .....	1
How to Spot a Phishing Attack.....	1
How to Protect Yourself From Becoming a Victim .....	2
What Other Steps Can You Take to Protect Yourself? .....	2
What On-line Resources Exist to Provide Additional Information? .....	3
What to Do if you Think You Have Received a Phishing Message .....	3
What to Do if You Become a Victim.....	3
Credit Reporting Bureaus .....	4
Take the Phishing Test.....	5

I wish to thank the Anti-Phishing Working Group and the Federal Trade Commission which developed many of the materials included in this pamphlet.

P. David Soares

## **What is Phishing?**

Phishing is a form of on-line identity theft that uses sophisticated fraudulent email messages to fool even the most sophisticated internet users into providing critical security information such as logon I.D.'s and passwords.

A typical Phishing attack includes an email from a trusted financial institution that notifies you of some sort of action that requires you to sign into their website. You are then asked to enter some key financial data such as your credit card number, your password, or your social security number. This data is then captured by the creator of the Phishing message who uses the data to steal money from your account.

The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond such as having your account frozen. The message contains a link, which, if you click on it, directs you to a Web site that looks just like the legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity, transfer money out of your account, run up bills in your name or even commit crimes in your name.

## **How Big is the Problem?**

The number of these so-called Phishing attacks increased by over 1200% last year and the amount stolen through these techniques exceeded \$300 million. According to a March 2005 report by Symantec, there are now over 33 million Phishing attacks every week. Although the Albany DA's office hasn't received any reports of victims here in Albany County, it is better to protect yourself from becoming a victim than it is to try to repair the damage of lost funds and a tarnished credit rating.

## **How to Spot a Phishing Attack**

Early Phishing attacks were relatively easy to spot since very often they contained typographical errors, poor grammar and odd syntax. Additionally, they were very often addressed to "Dear Customer" and since Phishing emails are sent out to very large lists of email addresses most were sent to people who aren't, in fact, customers of the supposed source of the message. A Phishing attack very often will include some sort of warning and a request to click on a supplied link to provide or correct some key personal information.

However Phishing attacks have become increasingly sophisticated. Recent attacks have included personalized letters and have become less threatening in tone. They appear to be a notice from your financial institution requesting some sort of routine maintenance of your account.

But the common thread of virtually all Phishing attacks is that they request that you log on to the financial institutions website and enter or update some personal information using a link provided in the email message.

## **How to Protect Yourself From Becoming a Victim**

The first and most important rule to protect yourself from a Phishing attack is to:

**NEVER CLICK ON A LINK**

in such a message. Similarly:

**NEVER CUT AND PASTE A LINK PROVIDED IN THE MESSAGE.**

If you think that the message is legitimate, sign onto the website using your standard weblink or, call a customer support number from the financial institution and ask if the message is legitimate. But just as you should never use a link provided in the email message so should you never call a number listed in the email message.

**DO NOT CALL ANY NUMBER INCLUDED IN THE EMAIL MESSAGE**

Phone numbers included in Phishing attacks will route you to a criminal phone bank. If you think the message is legitimate, call the number listed in your regular monthly statement or call your local branch and ask them to connect you to the computer operations department or computer fraud department.

## **What Other Steps Can You Take to Protect Yourself?**

**Don't ever email personal or financial information.**

**Never enter personal or financial information on any website that is not secure.** The URL for a secure website begins with "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some Phishers have recently learned how to forge security icons.

One excellent source of protection is to **check all your accounts regularly** to ensure that there are no illegitimate transactions. When you get your monthly statements, go over them promptly and carefully. Federal law provides protections if you report a fraudulent transaction within 60 days of receiving your statement but it limits the bank's liability thereafter, so promptness is important.

**Use anti-virus software and keep it up to date.** Some Phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

**Install a firewall in your computer.** A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection.

**Keep your software up to date.** Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or Phishers could exploit.

**Use caution in opening any attachment** or downloading any files from emails you receive, regardless of who sent them.

**Use complex passwords** that are difficult to guess and security questions that are difficult to guess. For example passwords should include a random combination of numbers and letters. And secret security questions such as your mother's maiden name should not be used for financial accounts.

## **What On-line Resources Exist to Provide Additional Information?**

[Anti-Phishing Working Group](http://www.anti-phishing.org) <http://www.anti-phishing.org> - Daily news from the net about Phishing attacks.

The Federal Trade Commission ID Theft Home Page  
<http://www.consumer.gov/idtheft/>

Fight Identity Theft  
[http://www.fightidentitytheft.com/paypal\\_scam.html](http://www.fightidentitytheft.com/paypal_scam.html)

## **What to Do if you Think You Have Received a Phishing Message**

If you think that the message is a Phishing message, forward it to the Federal Trade Commission (FTC) at [spam@uce.gov](mailto:spam@uce.gov). You can also send a copy to the Anti-Phishing Work Group at [Anti-Phishing Working Group: Report Phishing](#)

## **What to Do if You Become a Victim**

**Immediately report the situation to the fraud units of the three credit reporting companies** -- Experian (formerly TRW), Equifax and TransUnion. Report that your identifying information is being used by another person to obtain credit fraudulently in your name. Ask that your file be flagged with a fraud alert. Add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications.")

**Close the accounts** that you know or believe have been tampered with or opened fraudulently. Use the **ID Theft Affidavit** when disputing new unauthorized accounts.

**File your complaint** at [www.ftc.gov](http://www.ftc.gov), and then visit the FTC's Identity Theft Web site at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to learn how to minimize your risk of damage from ID theft. Visit [www.ftc.gov/spam](http://www.ftc.gov/spam) to learn other ways to avoid email scams and deal with deceptive spam.

The following report provides an excellent set of guidance for victims of Identity Theft:

*Identity Theft: What to Do if It Happens to You*

A Joint Publication of the Privacy Rights Clearinghouse and CALPIRG

<http://www.privacyrights.org/fs/fs17a.htm>

**Contact all creditors** immediately with whom your name has been used fraudulently, by phone and in writing. You will see evidence of these accounts on your credit reports. Creditors will likely ask you to fill out fraud affidavits. The Federal Trade Commission (FTC) provides a uniform affidavit form that most creditors accept (Web: [www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf)).

**Report the crime to your local police** or sheriff's department. You might also need to report it to police departments where the crime occurred. Give them as much documented evidence as possible. *Make sure the police report lists the fraud accounts.* Get a copy of the report. Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime.

If your existing credit accounts have been used fraudulently, **get replacement cards with new account numbers**. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as blaming you.) Monitor your mail and bills for evidence of new fraudulent activity. Report it immediately to creditor grantors. **Add passwords to all accounts**. This should not be your mother's maiden name or a word that is easily guessed.

**Do not pay** any bill or portion of a bill that is a result of fraud. Do not cover any checks that were written or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected. No legal action should be taken against you. If any merchant, financial company or collection agency suggests otherwise, restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

## Credit Reporting Bureaus

**Equifax:** P.O. Box 105069, Atlanta, GA 30348.

Report fraud: Call (800) 525-6285 and write to address above.

Order credit report: (800) 685-1111.

TDD: (800) 255-0056 Web: [www.equifax.com](http://www.equifax.com)

**Experian (formerly TRW):**

P.O. Box 9532 Allen, TX 75013.

Report fraud: Call (888) EXPERIAN (888-397-3742) and write to address above.

Order credit report: (888) EXPERIAN.

TDD Use relay to fraud number above.

Web: [www.experian.com](http://www.experian.com)

**TransUnion:**

P.O. Box 6790,

Fullerton, CA 92834

Report fraud: (800) 680-7289 and write to address above.

Order credit report: (800) 888-4213.

TDD: (877) 553-7803

E-mail (fraud victims only): [fvad@transunion.com](mailto:fvad@transunion.com)

Web: [www.transunion.com](http://www.transunion.com)

**Take the Phishing Test**

Look at the following email messages and see if you can figure out which are Phish and which are legitimate.


Information about your Chase credit card

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** Chase Credit Cards  
**Date:** Tuesday, November 02, 2004 3:30 AM  
**To:** Jill Smith  
**Subject:** Information about your Chase credit card

[Click here](#) to view this message in your browser



THE RIGHT RELATIONSHIP IS EVERYTHING.®

### Service Notice

We are pleased to offer you the opportunity to save up to hundreds of dollars by simply transferring your high-interest balances to your Chase credit card. Use our [Savings Calculator](#) to determine how much money you can save and be sure to act quickly - **this offer expires on January 5, 2005**. [Click here](#) to learn more.

**Transfer balances now**

Balances can be transferred from any non-Chase credit card or personal loan, including balances from other bank cards, department store cards and gasoline cards. Plus, when you transfer balances online, you'll be able to:

- Save time
- Calculate your potential savings before you start
- Check the status of transfers

[Click here to transfer balances today](#) -- it's free, it's secure, it's easy...and you could save hundreds of dollars on interest.

---

**ABOUT THIS MESSAGE**  
This service message was delivered to you as a Chase credit card customer to provide you account updates and information about your card benefits. Chase values your privacy and your preferences.

If you wish to unsubscribe from e-mail promotional messages from Chase Credit Card, please [click here](#). Please note that by making this choice, you may not receive certain cardmember benefits communications via e-mail.

If you wish to specify your e-mail preferences for certain types of credit card communications or update your e-mail address, please [click here](#).

To view the Chase Privacy Policy, please [click here](#). Please note that this e-mail was delivered by Bigfoot Interactive, Inc., an e-mail service provider of Chase.

Please do not reply to this message as the "reply" function is not equipped to handle customer service inquiries. For your convenience, please [click here](#) to contact Chase via e-mail.

Chase Manhattan Bank USA, N.A. Attention: Privacy • 600 White Clay Center • Newark, DE 19711-5455

Copyright © 2004 J.P. Morgan Chase & Co. All Rights Reserved.

<http://email.chase.com/WARH047CEF790388E9C763F6A77430>

**From:** Contribute Paypal  
**Date:** Monday, January 10, 2005 10:22 PM  
**To:**  
**Subject:** Contribute to the Tsunami Disaster Relief Effort



[Sign Up](#) | [Log In](#) | [Help](#)

## Contribute to the Tsunami Disaster Relief Effort

We at PayPal wish to express our profound sorrow over the suffering and loss of life resulting from the earthquakes and tsunami in South Asia and Africa. You can help those affected by this disaster by donating directly to UNICEF's Tsunami Disaster Relief effort using your PayPal account.

**Make a donation to the Tsunami Relief Effort through PayPal**  
[Donate now](#)

UNICEF works to bring relief to all disaster victims, particularly women and children who are the most vulnerable. The organization is working closely with the governments in all the countries affected by this disaster to combat the spread of disease and ensure that the victims have immediate access to fresh water, food, shelter, medical care and supplies. Visit [www.unicefusa.org](http://www.unicefusa.org) to learn more about UNICEF's Tsunami Disaster Relief efforts.



*UNICEF is rushing relief assistance to the countries hardest hit by massive ocean flooding following the earthquake on 12/26. UNICEF is working to meet the needs of hundreds of thousands of people who survived the tsunamis but now need shelter, water, medical supplies and other urgent assistance.*

*Privacy Notice: If you donate \$250 or more, PayPal will provide your name, billing address, email and donation amount to UNICEF so that UNICEF can provide you with a receipt for your donation. Other than this, PayPal will not share your information with UNICEF. PayPal will waive all fees in relation to the donation, so that UNICEF will receive 100% of the amount you donate.*

**Total Collected: \$731,481.18 USD  
contributed by 15568 donors**

Important information regarding your e-mail address

File Edit View Tools Message Help

 Reply
  Reply All
  Forward
  Print
  Delete
  Previous
  Next
  Addresses

**From:** Bank of America  
**Date:** Monday, September 27, 2004 9:29 AM  
**To:** Jane Doe  
**Subject:** Important information regarding your e-mail address



**Useful financial information delivered right to your inbox.**

Thank you for providing us with your e-mail address. You can rest assured that we protect your information, including your e-mail address, and will never sell or share it with marketers outside Bank of America. Read our [Privacy Policy](#) to find out more.

As part of our service to you, we may occasionally send you free, informative e-mails to:

- Keep you up to date on products, features, and services
- Let you know how Bank of America and its affiliates can help you financially — wherever you are in life
- Provide you with the tools and resources you need to make sound financial decisions

You can help us provide you with the most relevant information by taking a moment to tell us your [e-mail preferences](#).

And of course you can [unsubscribe](#) at any time.

Remember, Bank of America is committed to your security and protection. Please be aware that we will never e-mail you to request or verify security information about passcodes, PINs, or other sensitive details. To find out more, take a look at our [Information Security](#) section under Privacy and Security on the Web site.

The security and confidentiality of your personal information is important to us. BECAUSE E-MAIL IS NOT A SECURE FORM OF COMMUNICATION, THIS E-MAIL BOX IS NOT EQUIPPED TO HANDLE REPLIES. If you are a Bank of America customer and have sensitive account-related questions, please call the phone number provided on your account statement or the appropriate phone number indicated in the following "Contact Us" link so we can properly verify your identity. For all other questions or comments, please use the Web forms available via [Contact Us](#)

We respect your privacy, and you can rest assured that we protect your information, including your e-mail address, and will never sell or share it with marketers outside Bank of America. To find out more, please read our [Privacy Policy](#)

Bank of America E-mail, 6th Floor, 101 North Tryon Street, Charlotte, NC 28255-0001

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)   
 © 2004 Bank of America Corporation. All rights reserved.

This e-mail was sent to: janedoe@example-domain.com


[http://links.bankofamerica1.com:8082/Click?q=58-mr3xIdJHw\\_RH5tNYrBD7vD0CzRR&a=1](http://links.bankofamerica1.com:8082/Click?q=58-mr3xIdJHw_RH5tNYrBD7vD0CzRR&a=1)

Suspicious activity in your account.

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** Washington Mutual  
**Date:** Tuesday, November 02, 2004 5:22 AM  
**To:** john@example-domain.com  
**Subject:** Suspicious activity in your account.

 **Washington Mutual** AUTHORIZATIONS / CLEARING AND SETTLEMENT DEPARTMENT

Dear respected member of Washington Mutual Bank,

Our department recorded a payment request from Expedia - Online Travel Agency (EXPEDIA.COM) to enable the charge of \$619.49 on your account.

This amount is supposed to cover the cost of a 5 days reservation (06-11 November / 2004) at a Five Stars Hotel located in New Delhi / INDIA, under the name of GARY EDWARDS.

**THE PAYMENT IS PENDING FOR THE MOMENT.**

- If you made this reservation or if you just authorize this payment, please ignore or remove this email message. The transaction will be shown on your monthly statement as "Rama Bangalore-Hotel".
- If you didn't make this payment / reservation and would like to decline the \$619.49 billing to your card, please follow the link below to deny the payment:

[decline](#)

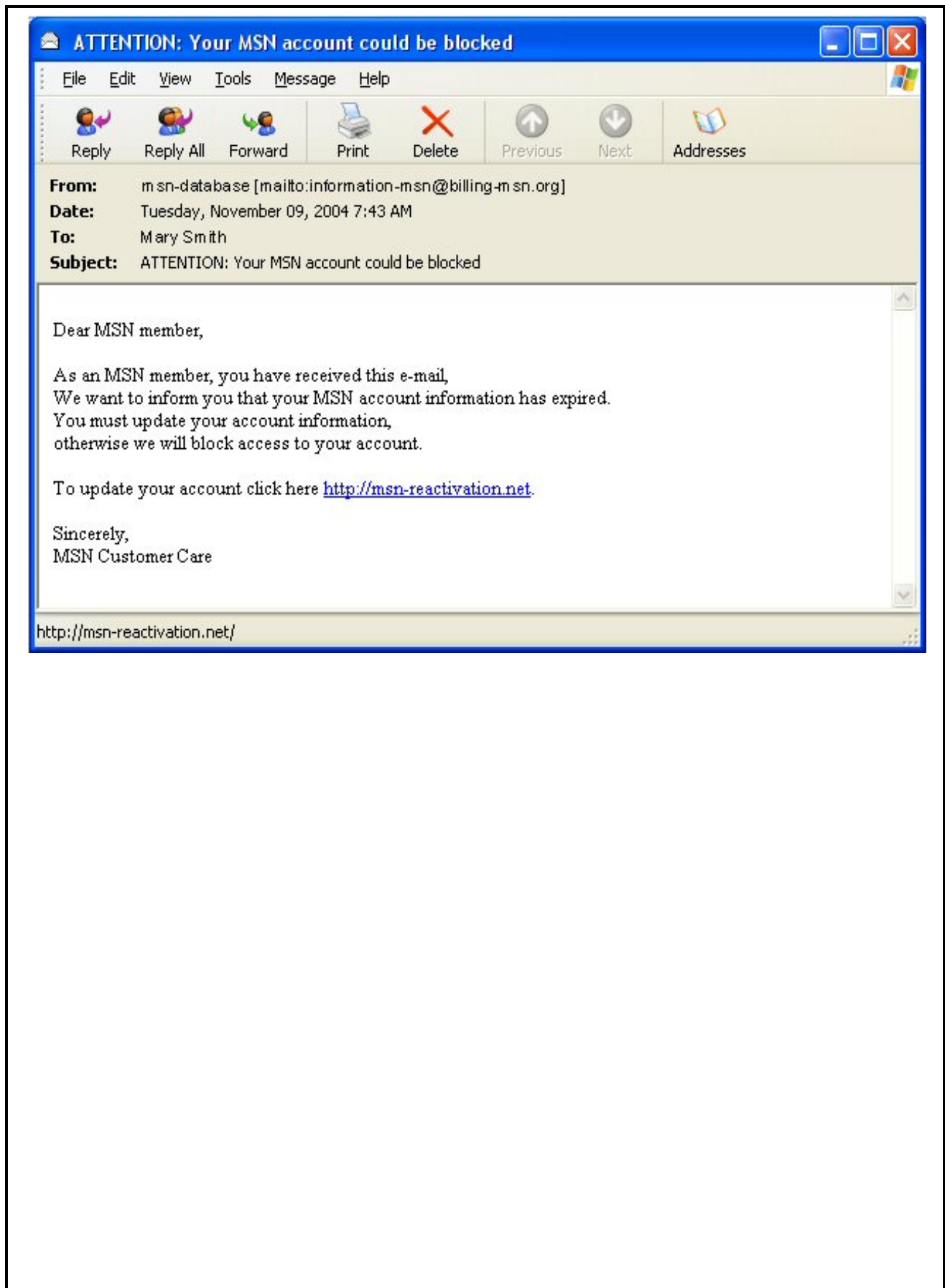
(Click "DECLINE" button to stop this payment.)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Washington Mutual, Inc. system.

Thank you for your prompt attention to this matter.

Please do not reply to this mail. Mail sent to this address cannot be answered

<http://dmswebsolutions.com/main/>




**EarthLink Benefit Information: Email**

File Edit View Tools Message Help


Reply Reply All Forward Print Delete Previous Next Addresses

**From:** EarthLink Customer Experience Team  
**Date:** Wednesday, July 14, 2004 1:29 AM  
**To:** tom--doe@earthlink.net  
**Subject:** EarthLink Benefit Information: Email



## Keep your email separate—and private!

Activate up to eight personal email addresses today!




**FREE benefit exclusively for EarthLink® members**

With up to eight email addresses from EarthLink, everyone in your household can have their own email address, password, Personal Start Page<sup>SM</sup>, and more! So your email can stay private in your own customized mailbox.

You can also set up a separate email address for your professional contacts and keep your work and personal email organized!

**Activate your FREE email addresses in 3 easy steps:**

1. Sign in to [My Account](#)\*
2. Click the **Add a new profile** link
3. Choose your new email address and password!



**▶ GO TO MY ACCOUNT NOW**

**CUSTOMIZE SPAMBLOCKER FOR EACH ADDRESS**

Learn how EarthLink spamBlocker can block virtually 100% of all junk email out of your new email inboxes.

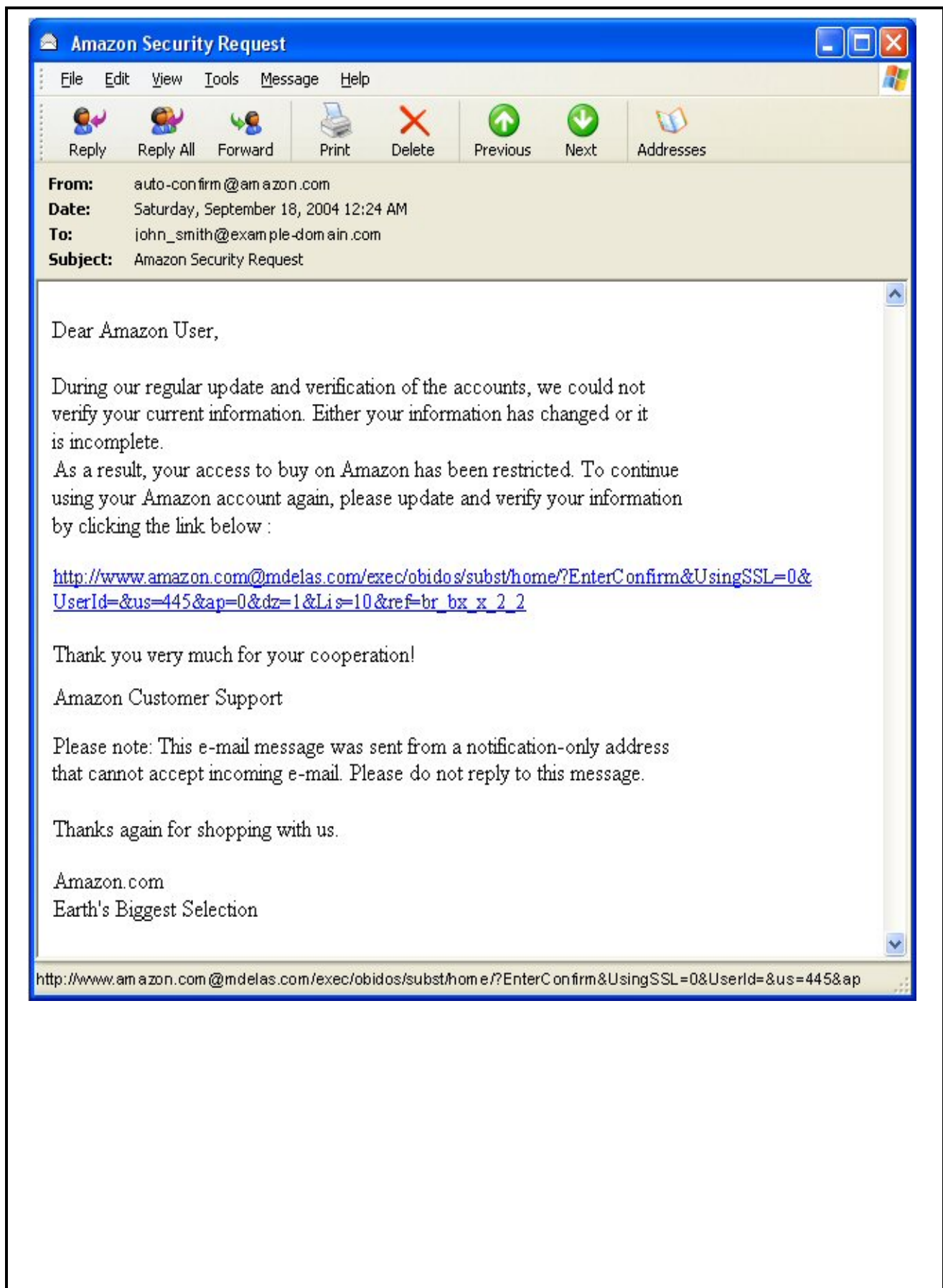
**▶ Go to SPAMBLOCKER Now**

**EarthLink** *revolves around you™*

\* Please note: If you already have more than one email address, you must sign in as the primary account holder to activate another one. If you sign in using a secondary email address, you can only make changes to that particular profile.

© 2004 EarthLink, Inc. EarthLink and the EarthLink logo are registered trademarks of EarthLink, Inc. Trademarks are property of their respective owners. All rights reserved.

<http://tr.earthlink.net/t/lnk?id=td1089201123&url=http://myaccount.earthlink.net>



Required: eBay Billing Information Update

File Edit View Tools Message Help



**From:** aw-confirm@eBay.com  
**Date:** Wednesday, October 27, 2004 6:07 AM  
**To:** John Doe  
**Subject:** Required: eBay Billing Information Update



It has come to our attention that your eBay billing updates are out of order. If you could please take 1-2 minutes out of your online experience and update your billing records you will not run into any future problems with the online service. However, failure to update your records will result in account termination. Please update your records.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

To update your eBay records now click here:

<http://cgi1.ebay.com/aw-cgi/ebayISAPI.dll?UPdate>

GO TO eBay!

eBay sent this e-mail to you because your Notification Preferences indicate that you want to receive information your eBay Credit Card Statement.

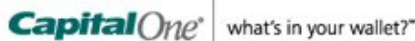
To change your communication preferences, [click here](#). Or, simply reply to this e-mail with UNSUBSCRIBE in the subject line. Please note that it may take up to 14 days to process your request. Visit our [Privacy Policy](#) and [User Agreement](#) if you have any questions.

Copyright © 2004 eBay Inc. All Rights Reserved.  
Designated trademarks and brands are the property of their respective owners.  
eBay and the eBay logo are trademarks of eBay Inc.

<http://awcg1dln.com/aw-confirm/signin.ebay/?UPdate&ssPageName=h:h:sin:US>



From: Capital One
Date: Thursday, July 15, 2004 12:08 PM
To: jon\_doe@example-domain.com
Subject: Your Capital One statement is ready



Manage Your Card Account

Log In

Log in to see your Capital One Statement



While you're in Online Account Services, click on the Customer Service Tab to...

- Update your e-mail address
• Change your payment due date
• Change your password
• Request your PIN
• View your account terms
• View your online account history

RE: Your account ending in 7163

Your current Capital One statement is now available for viewing online. Simply log in to Online Account Services and click the My Statement tab.

Is all your information reaching you?

To help ensure this time-sensitive message reaches your inbox each month, add the Capital One address that appears in the "From" line above to your electronic address book. This is especially important if you or your service provider uses e-mail filters.

Pay your bill for free

You can make payments safely and securely through Online Account Services. Just click the Pay My Bill tab and complete the payment profile. Online payments post the same day when they're made before 3:00 p.m. ET Monday through Saturday.\*

Use our Web site as a resource to access a variety of consumer lending products and special services.

Thanks for using Capital One's Online Account Services.

Click here to log in

Important Information from Capital One

Capital One and its service providers are committed to providing meaningful privacy protection for their customers. To protect your privacy, please do not send sensitive account information through e-mail. For information on our privacy policy or how to contact us, please visit our web site at www.capitalone.com.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.

\*Your online payment posts the same day when it's made before 3:00 p.m. ET Monday through Saturday. Payments made after 3:00 p.m. ET Monday through Friday will post the following day. Payments made after 3:00 p.m. ET on Saturday and anytime on Sunday will post to your account on Monday. Payments will not be posted on Thanksgiving, Christmas and New Years day.

© 2004 Capital One Services, Inc. Capital One is a federally registered service mark. All rights reserved.

**WHOIS Contact Information Confirmation**

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** Network Solutions  
**Date:** Friday, October 29, 2004 7:24 AM  
**To:** example-admin@example-domain.com  
**Subject:** WHOIS Contact Information Confirmation

---

**NetworkSolutions®**

**Important Information  
About Your Account**

Dear Network Solutions Customer:

To comply with the ICANN (Internet Corporation for Assigned Names and Numbers) WHOIS policy, we request each year that you [confirm](#) the accuracy of your WHOIS contact information. WHOIS is a publicly accessed database containing contact information associated with every domain name registration.

When you registered your domain name, you agreed to keep your contact information in Account Manager current. Please remember that providing inaccurate or dated contact information may be grounds for domain name cancellation. If your WHOIS information has changed or is inaccurate, please [update it](#) through your Network Solutions Account.

You may review the ICANN policy [here](#).

Thank you for your attention to this important ICANN required message. We look forward to helping you grow your business on the Web.

Sincerely,

Network Solutions Customer Support

---

This e-mail was sent from a notification-only address. Please do not reply to this message. For Network Solutions customer service inquiries, please [click here](#).

In accordance with our Privacy Policy, we will continue to send you notices and other important information affecting your account or services in order to fulfill our service obligations to you.

Access our [Privacy Policy](#).

Access our [Service Agreement](#).

(C) 2004 Network Solutions, LLC. All Rights Reserved.  
Network Solutions, 13200 Woodland Park Road, Department CCD, Herndon, VA 20171

<http://info1.networksolutions.com/h/7CF/F5N/T3/UGZX?a1=G918&a2=example-admin@example-domain.com>

**Correct Answers:**

1. Chase	Legitimate	why?
2. Paypal	Fraud	why?
3. Bank of America	Legitimate	why?
4. Washington Mutual	Fraud	why?
5. MSN	Fraud	why?
6. Earthlink	Legitimate	why?
7. Amazon	Fraud	why?
8. eBay	Fraud	why?
9. Capital One	Legitimate	why?
10. Network Solutions	Legitimate	why?

Answer explanations are listed on the DA's website at  
<http://www.albanycountyda.com/Phish.pdf>

Contact the DA's Office:

District Attorney P. David Soares  
Albany County Court House  
Albany NY 12207  
518 487 5460

Email: [pdavidsoares@albanycounty.com](mailto:pdavidsoares@albanycounty.com)  
Website: <http://www.albanycountyda.com>

## Information about your Chase credit card

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

**From:** Chase Credit Cards  
**Date:** Tuesday, November 02, 2004 3:30 AM  
**To:** Jill Smith  
**Subject:** Information about your Chase credit card

[Click here](#) to view this message in your browser



THE RIGHT RELATIONSHIP IS EVERYTHING.®

### Service Notice

We are pleased to offer you the opportunity to save up to hundreds of dollars by simply transferring your high-interest balances to your Chase credit card. Use our [Savings Calculator](#) to determine how much money you can save and be sure to act quickly - **this offer expires on January 5, 2005**. [Click here](#) to learn more.

**Transfer balances now**

Balances can be transferred from any non-Chase credit card or personal loan, including balances from other bank cards, department store cards and gasoline cards. Plus, when you transfer balances online, you'll be able to:

- Save time
- Calculate your potential savings before you start
- Check the status of transfers

[Click here to transfer balances today](#) -- it's free, it's secure, it's easy...and you could save hundreds of dollars on interest.

#### ABOUT THIS MESSAGE

This service message was delivered to you as a Chase credit card customer to provide you account updates and information about your card benefits. Chase values your privacy and your preferences.

If you wish to unsubscribe from e-mail promotional messages from Chase Credit Card, please [click here](#). Please note that by making this choice, you may not receive certain cardmember benefits communications via e-mail.

If you wish to specify your e-mail preferences for certain types of credit card communications or update your e-mail address, please [click here](#).

To view the Chase Privacy Policy, please [click here](#). Please note that this e-mail was delivered by Bigfoot Interactive, Inc., an e-mail service provider of Chase.

Please do not reply to this message as the "reply" function is not equipped to handle customer service inquiries. For your convenience, please [click here](#) to contact Chase via e-mail.

Chase Manhattan Bank USA, N.A. Attention: Privacy • 600 White Clay Center • Newark, DE 19711-5455

Copyright © 2004 J.P. Morgan Chase & Co. All Rights Reserved.

<http://email.chase.com/WARH047CEF790388E9C763F6A77430>

### This Email is Legitimate

**How can you tell?** Companies such as Chase use email to communicate special offers to their customers. In a good email, look for the links to go to URLs that are expected- chase.com for example. Also, the email should be free of spelling or grammatical errors. Still, fraudsters can fake URLs and their spelling is getting better – so it pays to be wary. The best defense is to **always practice safe browsing**. When email offers like this one offer products and services that interest you – go directly to the company's homepage and find out about them there.

**Contribute to the Tsunami Disaster Relief Effort**

File Edit View Tools Message Help

Reply Reply All Forward Print Delete

**From:** Contribute Paypal  
**Date:** Monday, January 10, 2005 10:22 PM  
**To:**  
**Subject:** Contribute to the Tsunami Disaster Relief Effort

**This Email is Phish**

**How can you tell?** Unless you could look at the URL listed in the status bar at the bottom of the email, it would be difficult to tell if this message were real or fraudulent. The URL shown in the status bar is "signupaccount.com" which even seems reasonable. This is one of those cases where it is better to be safe than sorry. If you receive an email such as this and wish to donate, open a new browser window, go directly to the donation web site and complete your donation there.

[Sign Up](#) | [Log In](#) | [Help](#)



## Contribute to the Tsunami Disaster Relief Effort

We at PayPal wish to express our profound sorrow over the suffering and loss of life resulting from the earthquakes and tsunami in South Asia and Africa. You can help those affected by this disaster by donating directly to UNICEF's Tsunami Disaster Relief effort using your PayPal account.

**Make a donation to the Tsunami Relief Effort through PayPal**

[Donate now](#)

UNICEF works to bring relief to all disaster victims, particularly women and children who are the most vulnerable. The organization is working closely with the governments in all the countries affected by this disaster to combat the spread of disease and ensure that the victims have immediate access to fresh water, food, shelter, medical care and supplies. Visit [www.unicefusa.org](http://www.unicefusa.org) to learn more about UNICEF's Tsunami Disaster Relief efforts.

*UNICEF is rushing relief assistance to the countries hardest hit by massive ocean flooding following the earthquake on 12/26. UNICEF is working to meet the needs of hundreds of thousands of people who survived the tsunamis but now need shelter, water, medical supplies and other urgent assistance.*

*Privacy Notice: If you donate \$250 or more, PayPal will provide your name, billing address, email and donation amount to UNICEF so that UNICEF can provide you with a receipt for your donation. Other than this, PayPal will not share your information with UNICEF. PayPal will waive all fees in relation to the donation, so that UNICEF will receive 100% of the amount you donate.*

**Total Collected: \$731,481.18 USD**  
 contributed by 15568 donors

[http://www.signupaccount.com/cgi/PayPal/PayPal-Log\\_In.htm](http://www.signupaccount.com/cgi/PayPal/PayPal-Log_In.htm)

**Important information regarding your e-mail address**

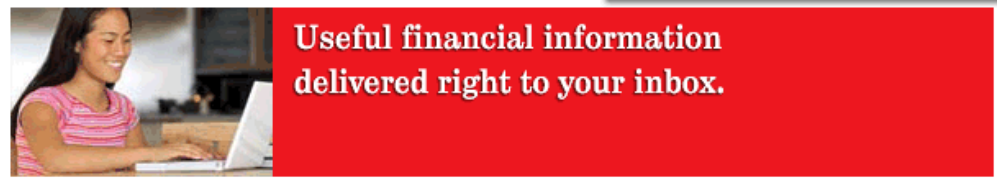
File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

**From:** Bank of America  
**Date:** Monday, September 27, 2004 9:29 AM  
**To:** Jane Doe  
**Subject:** Important information regarding your e-mail address

**This Email is Legitimate**

**How can you tell?** The content of this email introduces privacy policies—so it's good, right? But the email is not personalized and some of the links go to bankofamerica1.com, which might be bad, right? But none of the links ask you to enter personal information—they just lead you to information sources. So that makes it good...doesn't it? **Don't risk it.** Practice safe browsing by only logging in only on the known company homepage and save this email as a source of account information.



Thank you for providing us with your e-mail address. You can rest assured that we protect your information, including your e-mail address, and will never sell or share it with marketers outside Bank of America. Read our [Privacy Policy](#) to find out more.

As part of our service to you, we may occasionally send you free, informative e-mails to:

- Keep you up to date on products, features, and services
- Let you know how Bank of America and its affiliates can help you financially — wherever you are in life
- Provide you with the tools and resources you need to make sound financial decisions

You can help us provide you with the most relevant information by taking a moment to tell us your [e-mail preferences](#).

And of course you can [unsubscribe](#) at any time.

Remember, Bank of America is committed to your security and protection. Please be aware that we will never e-mail you to request or verify security information about passcodes, PINs, or other sensitive details. To find out more, take a look at our [Information Security](#) section under Privacy and Security on the Web site.

The security and confidentiality of your personal information is important to us. BECAUSE E-MAIL IS NOT A SECURE FORM OF COMMUNICATION, THIS E-MAIL BOX IS NOT EQUIPPED TO HANDLE REPLIES. If you are a Bank of America customer and have sensitive account-related questions, please call the phone number provided on your account statement or the appropriate phone number indicated in the following "Contact Us" link so we can properly verify your identity. For all other questions or comments, please use the Web forms available via [Contact Us](#)

We respect your privacy, and you can rest assured that we protect your information, including your e-mail address, and will never sell or share it with marketers outside Bank of America. To find out more, please read our [Privacy Policy](#).

Bank of America E-mail, 6th Floor, 101 North Tryon Street, Charlotte, NC 28255-0001

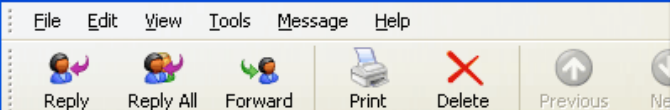
Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)

© 2004 Bank of America Corporation. All rights reserved.

This e-mail was sent to: janedoe@example-domain.com

[http://links.bankofamerica1.com:8082/Click?q=58-mr3x1dJHw\\_RH5tNYrbd7vD0CzsRR&a=1](http://links.bankofamerica1.com:8082/Click?q=58-mr3x1dJHw_RH5tNYrbd7vD0CzsRR&a=1)

**Suspicious activity in your account.**



**From:** Washington Mutual  
**Date:** Tuesday, November 02, 2004 5:22 AM  
**To:** john@example-domain.com  
**Subject:** Suspicious activity in your account.



**AUTHOR  
SETTLED**

**This Email is Phish**

**How can you tell?** Think about how legitimate companies communicate with customers. Does an email seem appropriate for this type of problem? Why is there no phone number to call for more information? Why is there no transaction or reference information? Why does the email not mention what account is going to be charged? Finally, why would a company such as a national bank direct you to a third party domain—and not allow you to reply with questions? Be aware. **When an email doesn't make sense, contact the company directly.**

Dear respected member of Washington Mutual Bank,

Our department recorded a payment request from Expedia - Online Travel Agency ( EXPEDIA.COM ) to enable the charge of \$619.49 on your account.

This amount is supposed to cover the cost of a 5 days reservation ( 06-11 November / 2004 ) at a Five Stars Hotel located in New Delhi / INDIA, under the name of GARY EDWARDS.

**THE PAYMENT IS PENDING FOR THE MOMENT.**

- If you made this reservation or if you just authorize this payment, please ignore or remove this email message. The transaction will be shown on your monthly statement as "Rama Bangalore-Hotel".
- If you didn't make this payment / reservation and would like to decline the \$619.49 billing to your card, please follow the link below to deny the payment:

[decline](#)

(Click "DECLINE" button to stop this payment.)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Washington Mutual, Inc. system.

Thank you for your prompt attention to this matter.

Please do not reply to this mail. Mail sent to this address cannot be answered

<http://dmswebsolutions.com/main/>

 **ATTENTION: Your MSN account could be blocked**

File Edit View Tools Message Help

**From:** msn-database [mailto:information-msn@billing-  
**Date:** Tuesday, November 09, 2004 7:43 AM  
**To:** Mary Smith  
**Subject:** ATTENTION: Your MSN account could be blocked

Dear MSN member,

As an MSN member, you have received this e-mail.  
We want to inform you that your MSN account information has expired.  
You must update your account information,  
otherwise we will block access to your account.

To update your account click here <http://msn-reactivation.net>.

Sincerely,  
MSN Customer Care

<http://msn-reactivation.net/>

## This Email is Phish

**How can you tell?** Even when a domain name sounds legitimate, always look carefully to make sure that the links or URLs in an email refer back to that domain or another expected domain. If the sender's domain does not match the domain a link or URL sends you to, be suspicious. Also know that phishing emails often disguise displayed domain names and URLs—**things might not be what they seem!**

**EarthLink Benefit Information: Email**


File Edit View Tools Message Help

Reply Reply All Forward Print Delete

**From:** EarthLink Customer Experience Team  
**Date:** Wednesday, July 14, 2004 1:29 AM  
**To:** tom--doe@earthlink.net  
**Subject:** EarthLink Benefit Information: Email


**This Email is Legitimate**

**How can you tell?** Know the company- Earthlink uses email to communicate with its customers. This email is consistent with other types of emails that Earthlink sends to its customers. In addition, the links in the email appear to take you to expected Earthlink destinations. But the email provides links to login to your account-which could be abused by phishers. **So always practice safe browsing.** Go to the homepage or to your personal user page to login and take advantage of special offers.



**Keep your email separate— and private!**

*Activate up to eight personal email addresses today!*




With up to eight email addresses from EarthLink, everyone in your household can have their own email address, password, Personal Start Page<sup>SM</sup>, and more! So your email can stay private in your own customized mailbox.

You can also set up a separate email address for your professional contacts and keep your work and personal email organized!

**Activate your FREE email addresses in 3 easy steps:**

1. Sign in to [My Account](#)\*
2. Click the **Add a new profile** link
3. Choose your new email address and password!



**▶ GO TO MY ACCOUNT NOW**

**CUSTOMIZE SPAMBLOCKER FOR EACH ADDRESS**

Learn how EarthLink spamBlocker can block virtually 100% of all junk email out of your new email inboxes.

**▶ Go to SPAMBLOCKER Now**

**EarthLink *revolves around you***

\* Please note: If you already have more than one email address, you must sign in as the primary account holder to activate another one. If you sign in using a secondary email address, you can only make changes to that particular profile.

© 2004 EarthLink, Inc. EarthLink and the EarthLink logo are registered trademarks of EarthLink, Inc. Trademarks are property of their respective owners. All rights reserved.

<http://tr.earthlink.net/t/lnk?id=td1089201123&url=http://myaccount.earthlink.net>

## Amazon Security Request

File Edit View Tools Message Help



Reply



Reply All



Forward



Print



Delete



Previous

**From:** auto-confirm@amazon.com  
**Date:** Saturday, September 18, 2004 12:24 AM  
**To:** john\_smith@example-domain.com  
**Subject:** Amazon Security Request

Dear Amazon User,

During our regular update and verification of the accounts, we could not verify your current information. Either your information has changed or it is incomplete.

As a result, your access to buy on Amazon has been restricted. To continue using your Amazon account again, please update and verify your information by clicking the link below :

[http://www.amazon.com@mdelas.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0&UserId=&us=445&ap=0&dz=1&Lis=10&ref=br\\_bx\\_x\\_2\\_2](http://www.amazon.com@mdelas.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0&UserId=&us=445&ap=0&dz=1&Lis=10&ref=br_bx_x_2_2)

Thank you very much for your cooperation!

Amazon Customer Support

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks again for shopping with us.

Amazon.com  
Earth's Biggest Selection

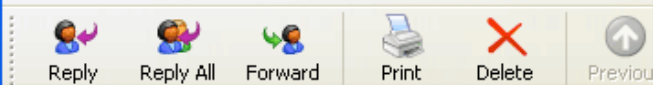
<http://www.amazon.com@mdelas.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0&UserId=&us=445&ap>

### This Email is Phish

**How can you tell?** Look carefully at the link. See the @ sign? This is a common phishing trick. In some browser applications, when a URL uses an @ sign, everything to the left of the @ sign is disregarded and the browser only reads to the right of the @ sign. **When you see or suspect an @ trick, be suspicious.** Look carefully at everything to the right of the @ sign. If you think that the sender of the email has no legitimate association with the domain you see there, suspect a phish.

Required: eBay Billing Information Update

File Edit View Tools Message Help



From: aw-confirm@eBay.com
Date: Wednesday, October 27, 2004 6:07 AM
To: John Doe
Subject: Required: eBay Billing Information Update

This Email is Phish
How can you tell? Know the company—eBay generally does not send out emails to customers containing login links. Look carefully at the status bar for all links and URLs—the URL in the status bar for the login link is not eBay.com. Differences between links or URLs in an email and the status bar should make you suspicious. If you receive an email like this one, open a new browser window and login into your account there to see if there are any real account problems.



It has come to our attention that your eBay billing updates are out of order. If you could please take 1-2 minutes out of your online experience and update your billing records you will not run into any future problems with the online service. However, failure to update your records will result in account termination. Please update your records.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

To update your eBay records now click here:

http://cgi1.ebay.com/aw-cgi/ebay!SAPI.dll?UPdate



eBay sent this e-mail to you because your Notification Preferences indicate that you want to receive information your eBay Credit Card Statement.

To change your communication preferences, click here. Or, simply reply to this e-mail with UNSUBSCRIBE in the subject line. Please note that it may take up to 14 days to process your request. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc.

http://awcg1.dln.com/aw-confirm/signin.ebay?UPdate&ssPageName=h:h:sin:US

**Your Capital One statement is ready**

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

**From:** Capital One  
**Date:** Thursday, July 15, 2004 12:08 PM  
**To:** jon\_doe@example-domain.com  
**Subject:** Your Capital One statement is ready

**Capital One** what's in your wallet?™


**This Email is Legitimate**

**How can you tell?** The purpose of the email is to introduce a customer to online banking services and it does show a partial account number (7163) to establish credibility. However, the links, including the account login links, go to an unexpected domain "bf0.com" – this is usually a red flag. If a company you deal with sends you an email like this, **practice safe browsing.** Open a new browser, go to the company home page and log into your account from there.

**Manage Your Card Account**

[Log In](#)

**Log in to see your Capital One Statement**



RE: Your account ending in 7163

Your current Capital One® statement is now available for viewing online. Simply [log in](#) to Online Account Services and click the My Statement tab.

**Is all your information reaching you?**  
 To help ensure this time-sensitive message reaches your inbox each month, add the Capital One address that appears in the "From" line above to your electronic address book. This is especially important if you or your service provider uses e-mail filters.

**Pay your bill for free**  
 You can make payments safely and securely through Online Account Services. Just click the Pay My Bill tab and complete the payment profile. Online payments post the same day when they're made before 3:00 p.m. ET Monday through Saturday.\*

[Use our Web site](#) as a resource to access a variety of consumer lending products and special services.

Thanks for using Capital One's Online Account Services.

[Click here to log in](#)

---

Important Information from Capital One

Capital One and its service providers are committed to providing meaningful privacy protection for their customers. To protect your privacy, please do not send sensitive account information through e-mail. For information on our privacy policy or how to contact us, please visit our web site at [www.capitalone.com](http://www.capitalone.com). If you are not a Capital One customer and believe you received this message in error, please notify us by responding to this e-mail.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.

\*Your online payment posts the same day when it's made before 3:00 p.m. ET Monday through Saturday. Payments made after 3:00 p.m. ET Monday through Friday will post the following day. Payments made after 3:00 p.m. ET on Saturday and anytime on Sunday will post to your account on Monday. Payments will not be posted on Thanksgiving, Christmas and New Years day.

© 2004 Capital One Services, Inc. Capital One is a federally registered service mark. All rights reserved.

<http://capitalone.bf0.com/TR5711904A7DB234A341155000>

**WHOIS Contact Information Confirmation**

File Edit View Tools Message Help

Reply Reply All Forward Print Delete

**From:** Network Solutions  
**Date:** Friday, October 29, 2004 7:24 AM  
**To:** example-admin@example-domain.com  
**Subject:** WHOIS Contact Information Confirmation

**This Email is Legitimate**

**How can you tell?** Network Solutions does use email to ensure that its records are up to date. The email gives users links to help them log in to their account. These links seem legitimate as the URL displayed in the status bar at the bottom of the email appears to go to the legitimate Network Solution domain, but always remember that this display can be faked. **If you receive an email like this, play it safe.** Open a new browser, go to the homepage, and login to your account from there.

**Important Information About Your Account**



Dear Network Solutions Customer:

To comply with the ICANN (Internet Corporation for Assigned Names and Numbers) WHOIS policy, we request each year that you [confirm](#) the accuracy of your WHOIS contact information. WHOIS is a publicly accessed database containing contact information associated with every domain name registration.

When you registered your domain name, you agreed to keep your contact information in Account Manager current. Please remember that providing inaccurate or dated contact information may be grounds for domain name cancellation. If your WHOIS information has changed or is inaccurate, please [update it](#) through your Network Solutions Account.

You may review the ICANN policy [here](#).

Thank you for your attention to this important ICANN required message. We look forward to helping you grow your business on the Web.

Sincerely,

Network Solutions Customer Support

---

This e-mail was sent from a notification-only address. Please do not reply to this message. For Network Solutions customer service inquiries, please [click here](#).

In accordance with our Privacy Policy, we will continue to send you notices and other important information affecting your account or services in order to fulfill our service obligations to you.

Access our [Privacy Policy](#).

Access our [Service Agreement](#).

(C) 2004 Network Solutions, LLC. All Rights Reserved.  
Network Solutions, 13200 Woodland Park Road, Department CCD, Herndon, VA 20171

<http://info1.networksolutions.com/h/7CF/F5N/T3/UGZX?a1=G918&a2=example-admin@example-domain.com>

Contact the DA's Office:

District Attorney P. David Soares  
Albany County Court House  
Albany NY 12207  
518 487 5460

Email: [pdavidsoares@albanycounty.com](mailto:pdavidsoares@albanycounty.com)  
Website: <http://www.albanycountyda.com>