

Credit Card Fraud Training

Lesson Plan

(For the Instructor's Use)

Course Purpose & Objectives:

The purpose of this workshop is to inform participants about credit card fraud, to promote prevention and provide useful information to victims of identity theft.

By the end of the workshop, participants will understand:

- the effects of credit card fraud
- how credit card fraud is perpetrated
- how to recognize different types of deception
- how to avoid becoming a victim of credit card fraud
- steps victims of credit card fraud can take
- available helpful resources

Check List of Materials

Participant's folder, which includes:

- Recognizing Credit Card Fraud* brochure
- Activities (attached at the end of this lesson plan)
 - 1. Test Your Credit Card Fraud IQ
 - 2. Something's Phishy - Can you catch a phish?
 - 3. You Are the Judge - Credit Card Fraud Scenarios
 - 4. Credit Card Log

For the Trainer:

Training Manual: *Questions and Answers About Credit Card Fraud*

Credit Card Fraud Lesson Plan

Easel, Pad and Markers

Power Point Outline

(Optional) Power Point Presentation, LCD projector, computer

Workshop Duration: 2 hours

Credit Card Fraud Training Lesson Plan

Suggested Time Allotment	Segment
10 minutes	Welcome and training overview
15 minutes	Group introductions
10 minutes	Why learn about credit card fraud?
10 minutes	Types of deception
10 minutes	How to recognize and avoid credit card fraud
15 minutes	What to do if you become a victim
10 minutes	Helpful resources
10 minutes	Questions & Answers
20 minutes	Activities
10 minutes	Wrap-up, evaluations / take-aways

Before conducting the training, familiarize yourself with the materials:

- Credit Card Fraud brochure,
- Training manual – Questions & Answers About Credit Card Fraud
- Lesson plan & 4 activities
- Power Point presentation outline

Welcome and Training Overview

10 minutes

Welcome participants: Hand out folders (or place them on the tables before the participants arrive).

Give a quick overview about the Credit Card Fraud Training and tell them that you'd like to hear what they hope to gain from the workshop.

Go over the Credit Card Fraud workshop agenda.

Start participant introductions/ice breakers.

Group Introductions and Ice Breakers

15 minutes

Ask participants to introduce themselves. Or if time permits, ask them to pair off with someone seated close to them. Have each of them introduce their partner to the group.

To keep introductions brief, list 3-4 main questions to ask:

- their name
- how they heard about the workshop (*if appropriate*)
- what agency are they from (*if appropriate*)
- what they hope to gain from the workshop

(They can continue their conversation within the time allotted.)

Write down participants' expectations on an easel pad or whiteboard after each participant introduces themselves or one another. At the end of the introductions, go over the expectations list briefly, assuring participants that much of what they'd like to accomplish during the workshop will be covered.

Note: *Save or post the "expectations list" to use during the workshop wrap up.*

Getting started on the presentation

Start the presentation by asking participants to raise their hand if they, or someone they know, have ever been a victim of identity theft or credit card fraud. This will give people an idea of the magnitude of the problem and stress the importance of educating consumers about credit card fraud. It also helps to develop a common ground and lets people who have been victimized know they are not alone.

Start Power Point Presentation

The Power Point presentation (excluding activities) is approximately 50 minutes long.

Overview of topics (Slide 2)

In addition to defining credit card fraud, plus when, where and how it can occur, the presentation covers 4 key topics:

- 1) Recognizing types of credit card fraud
- 2) Protecting yourself from fraud
- 3) Steps to take if you become a victim
- 4) Resources and referrals

What is Credit Card Fraud? When can it occur? (Slides 3 & 4)

Stress to participants that credit card fraud can happen to any of us no matter how careful we are. There is no reason to become paranoid, but be vigilant with your credit card information and know the steps to take should you become a victim of credit card fraud.

Why learn about credit card fraud? The bottom line (Slides 5 & 6)

Credit card fraud affects us all. If we become victims of credit card theft, it takes time and effort to close down accounts and have new credit cards issued and sent to you in addition to correcting billing statement and credit reports.

What is ID theft and how can it harm you? (Slides 7 & 8)

Identity thieves use other people's personal information, such as their Social Security numbers or credit card numbers, to commit financial fraud.

They can harm victims by using personal information to open up new credit card accounts, or use the information to access existing accounts to make unauthorized charges.

Note: ID theft can harm people in other ways, in addition to making unauthorized credit card charges. For example, criminals have used other people's identities to collect Social Security and public assistance.

There are circumstances that involve family members or friends using credit cards without the permission of the cardholder. Unless a police report is filed about the unauthorized use of cards, it is not treated as identity theft and the cardholder must pay the credit card charges.

Recognizing types of credit card fraud (Slides 9-11)

Dumpster Diving

Criminals steal personal information from the garbage. Make sure you shred any paperwork containing personal information before disposing of it.

Skimming

Skimming devices can capture account information from magnetic strips on credit and ATM cards. The stolen credit information is used to make purchases by phone and on the Internet, or to make counterfeit cards

Note: Your credit card information can be captured in other ways. For instance, your card information can be swiped on a credit card imprinter to a blank credit purchase form, or by using a pencil your credit card info can be rubbed on to a purchase form.

When making a purchase, keep your eyes on your card.

Phishing

Phishing is a term that refers to fishing, but instead of catching fish, criminals catch victims.

Criminals whose scam is phishing use the Internet to catch their victims. They send out massive numbers of e-mails that look like legitimate messages from financial institutions or charitable organizations. They know that there are people who will take the bait and respond to their fraudulent e-mails by revealing personal information such as credit card numbers.

Protecting yourself from fraud (Slides 12-26)

Financial institutions and credit card companies are attempting to curb credit card fraud in a number of ways.

Security Codes

Companies now give customers additional numbers called security codes to help prevent unauthorized charges made by phone or online.

New Cards

For added protection, credit card issuers ask you to call from home to activate new credit cards. As soon as you receive your credit card in the mail, sign the back of it with a permanent ink pen.

Should you write, “Ask for ID”?

In addition to signing your credit card, it's not a bad idea to write, “Ask for ID” next to your signature.

In case your card is lost or stolen

A credit card log is included in the *Recognizing Credit Card Fraud* workshop packet. Urge participants to record all of their account numbers and company contact information using the credit card log, and to keep it in a secure place.

Protect your PIN

PIN is the acronym for personal identification number. Memorize the number and never give it to anyone.

Protect your account numbers

Never write your credit card number on post cards or on the outside of envelopes, or give your account number to anyone who calls you on the phone or sends you an e-mail.

Remember that if you let others use your credit card, you are responsible for charges.

Billing Statements

You have 60 days to report any mistakes on your credit card statement so review it closely on the day the statement arrives. Report any questionable charges to your card issuer immediately.

Contact your card issuer right away if your bill doesn't arrive around the usual date, as a missing statement may indicate stolen mail.

Online account access

Signing up for online credit card account access allow you to track your account activity between statements.

Liability

Report lost or stolen cards as soon as possible. Fraud victims are not generally required to pay for unauthorized charges; however, victims may be liable for up to \$50 of the loss, depending on the circumstances.

Protect your wallet or purse

Never carry all your credit cards. Bring only the 1 or 2 cards you might need and carry your credit cards separate from your wallet. Call your credit card issuers immediately if your wallet or purse is lost or stolen.

Watch your credit card

Often it is difficult to keep your eye on your credit card when using it at a restaurant. If you feel uncomfortable about using your card where you know that it will be briefly out of your sight, bring enough money with you to pay by cash.

Take precautions

Credit card issuers sometimes block your credit card if it is being used outside of your normal geographic area, or if the card is being used for unusually large purchases. To avoid this from happening to you, notify your credit card company if you are going to be traveling or if you are planning to make any unusually large purchases.

Sometimes credit card issuers contact their customers if they notice unusual activity on their cards.

Safeguard your mail

Be sure to shred old credit card and banking statements before discarding. Also shred unwanted credit card solicitations you receive in the mail.

If you are moving, notify your credit card issuer, banks, and the post office immediately. To make it easy for mail to reach your new address, the post office provides free information for you to follow.

Internet safeguards

Don't use "automatic sign on" for bank or credit card sites

Don't fall for "free access" web site offers that ask for your credit card number.

Install a firewall in your computer to prevent unauthorized access from hackers

Steps to take if you become a victim (Slides 27-29)

Reporting credit card fraud

If you lose your credit cards or realize that they have been lost or stolen, call the issuers immediately. Credit card companies have 24-hour customer service lines to deal with emergencies. Follow up your phone call with a letter to the issuer giving your card number, the date you discovered your card was missing and the date you called to report it. Report the loss of your card as soon as you can. Once you have reported the loss or theft, you have no responsibility for unauthorized charges. If someone has used your card without your permission, your maximum liability under federal law is \$50 per card.

The Fair Credit Billing Act

The Fair Credit Billing Act, a section of the Truth in Lending Act, protects you against inaccurate credit card bills and unauthorized purchases and allows you to withhold payments on defective goods until you are notified of the outcome of your dispute. To be fully protected, report the problem to the credit card issuer in writing and make sure your complaint is received within 60 days of the billing statement. Include your name and account number and an explanation of why you believe the charge is incorrect. Include a copy of your billing statement with the questionable charge highlighted. Send your letter to the address designated by the creditor for handling errors. Do not send it in the same envelope with your payment. You must pay the portion of your bill that is not in dispute.

Resources and referrals (Slides 30-34)

The federal Fair Credit Reporting Act (FCRA) gives you the right to get a free credit report if you are the victim of identify theft and to place a fraud alert in your file if you discover that it contains inaccurate information as a result of fraud. States can enforce FCRA and many states have their own consumer reporting laws that may give you stronger rights. Contact your state or local consumer protection agency or your state attorney general for more information. You can find these agencies in the government pages of the phone book.

Helpful resources

Urge participants to spread the word about credit card fraud. It can happen to anyone, so let people know where to go to for help.

Free Credit Reports

Get a copy of your credit report annually.

Consumers now have the right to request a free copy of their credit report from each of the three major national credit reporting agencies. The law has been phased in from the West Coast to the East Coast. Residents of the Northeastern states are the last group to be eligible for free reports as of Sept. 1, 2005.

You can get free credit reports on the Internet at www.annualcreditreport.com.

To request your free reports by phone, call 1-877-322-8228. Your reports will be mailed to you.

Federal Trade Commission (FTC)

www.ftc.gov/consumer

The Federal Trade Commission (FTC) (www.ftc.gov/consumer) offers free publications on credit cards, billing rights and how to avoid credit card fraud.

The National Fraud Information Center

www.fraud.org

The National Fraud Information Center, a project of the National Consumers League, offers advice and prevention tips

1 -800-867-7060

Your State Attorney General's Office

The National Association of Attorneys General web site is www.naag.org

Check the phone directory to find your state office.

Consumer Action

Visit our web site:

www.consumer-action.org

or contact us at info@consumer-action.org Call: 1-415-777-9635

Created by Consumer Action with funding from WaMu.
© Consumer Action 2007

Something's Phishy

Can you catch a phish?

Credit Card Fraud Training

CONSUMER ACTION
www.consumer-action.org


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>

Source: <http://www.mailfrontier.com/quiztest2/S2html/Q4.html>

Contribute to the Tsunami Disaster Relief Effort

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

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


PayPal [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 

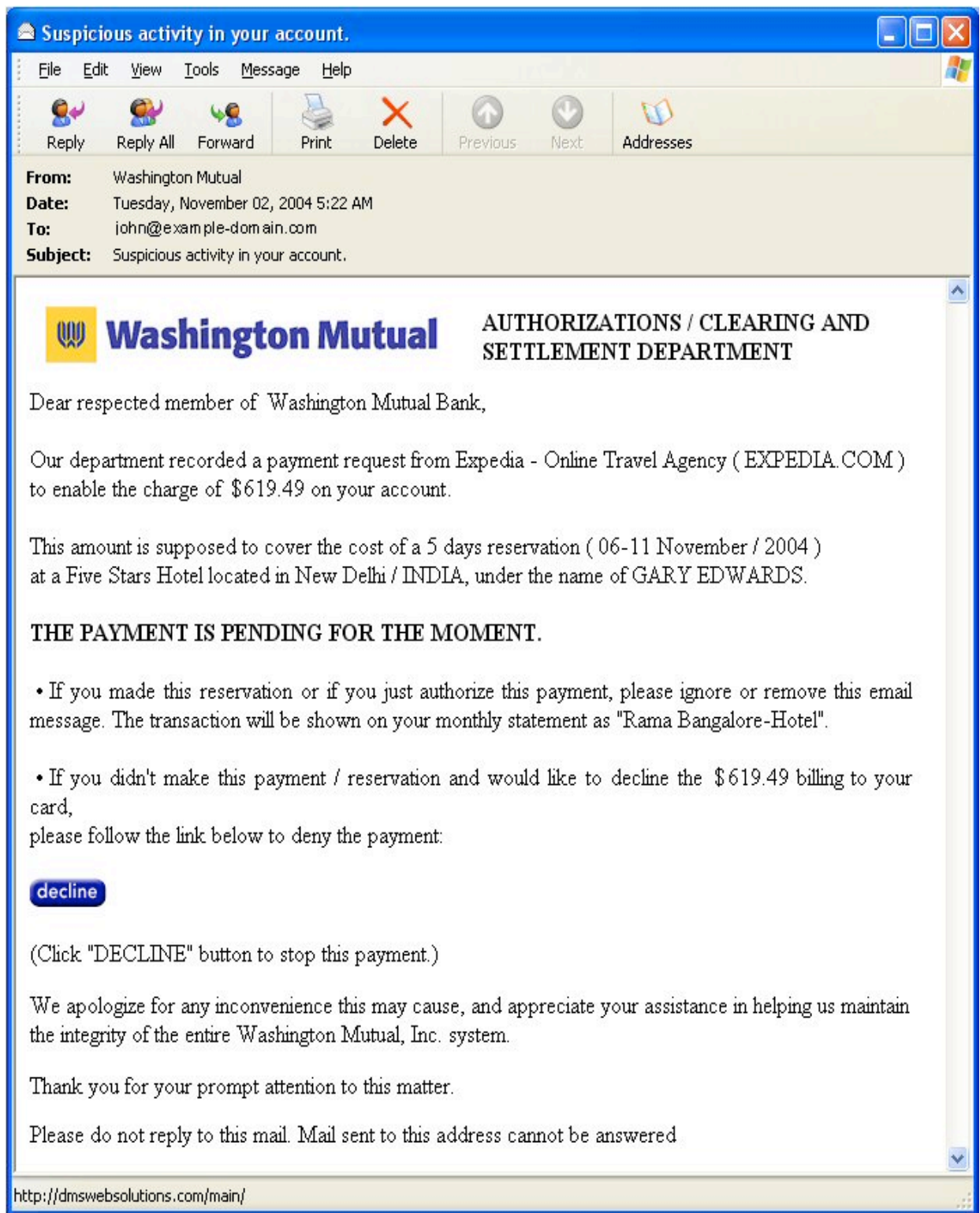
UNICEF is rushing relief assistance to the countries hardest hit by massive ocean flooding following the earthquake on 12/26. UNICEF is working to meet the needs of hundreds of thousands of people who survived the tsunamis but now need shelter, water, medical supplies and other urgent assistance.

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

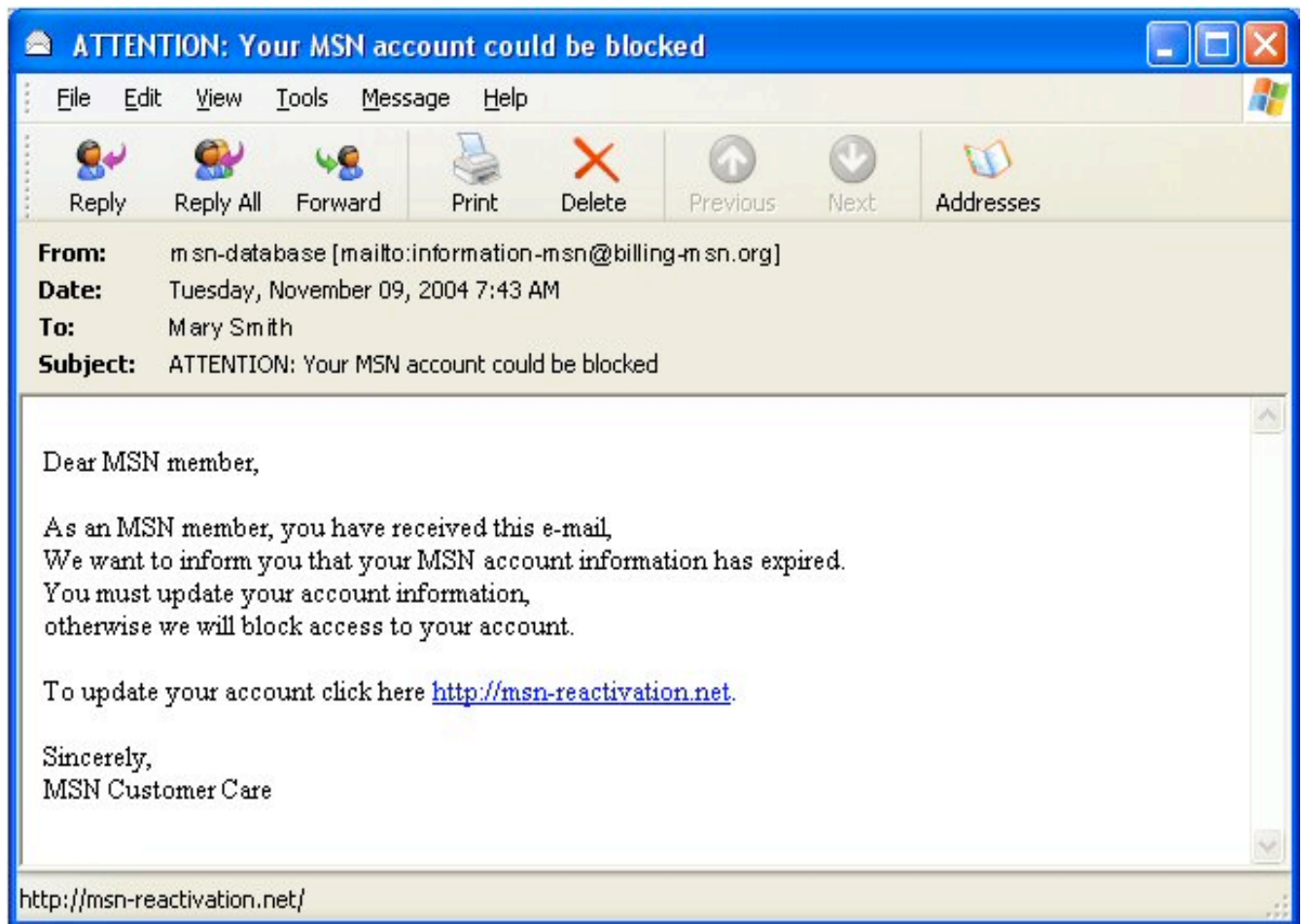
Privacy Notice: If you donate \$250 or more, PayPal will provide your name, billing address, email and donation amount to UNICEF so that UNICEF can provide you with a receipt for your donation. Other than this, PayPal will not share your information with UNICEF. PayPal will waive all fees in relation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

http://www.signupaccount.com/cgi/PayPal/PayPal-Log_In.htm

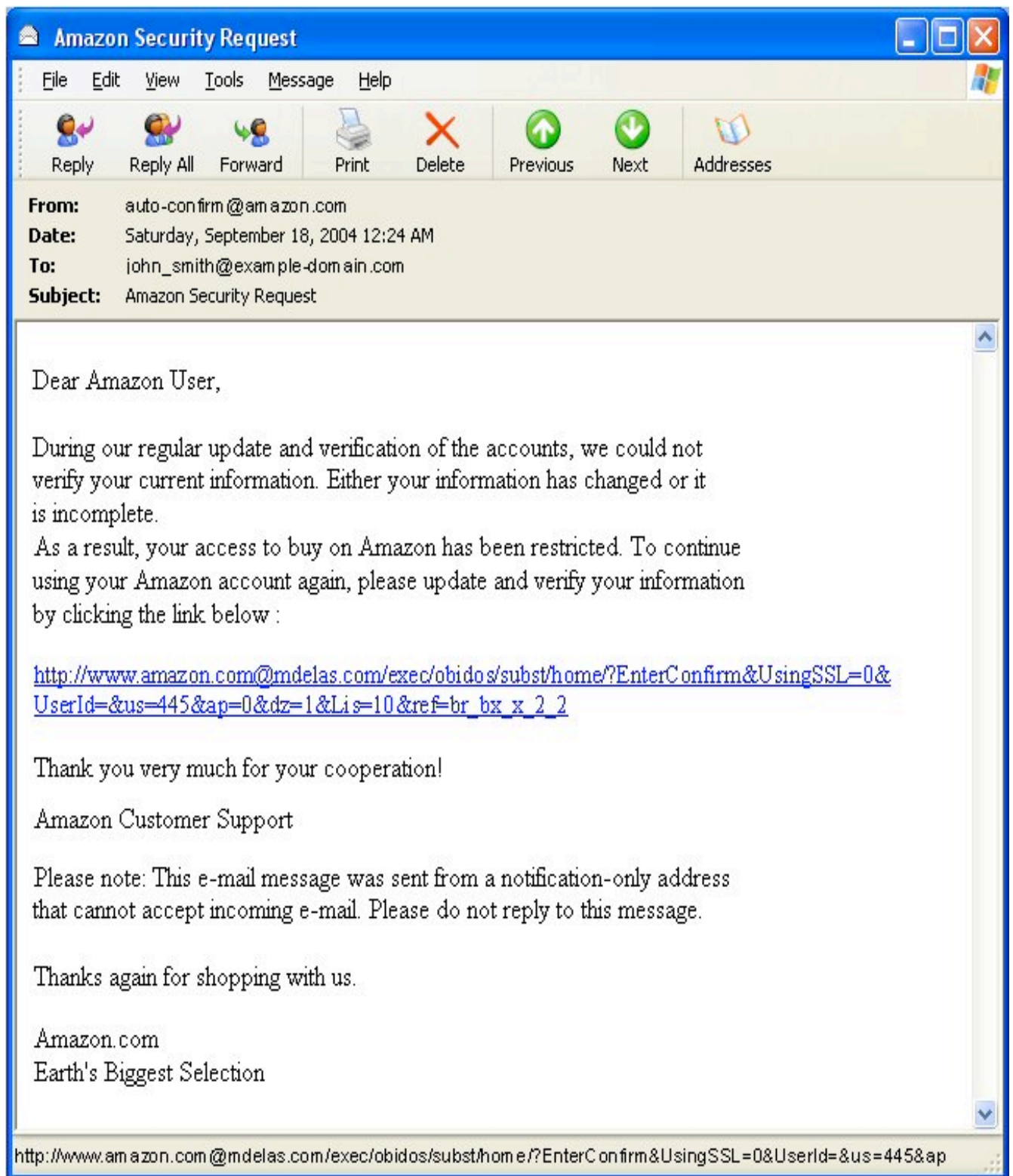
Source: <http://www.mailfrontier.com/quiztest2/S2html/Q4.html>



Source: <http://www.mailfrontier.com/quiztest2/S2html/Q4.html>



Source: <http://www.mailfrontier.com/quiztest2/S2html/Q4.html>



Source: <http://www.mailfrontier.com/quiztest2/S2html/Q4.html>

How to spot a Phish

1. Chase Example

This e-mail is legitimate

How can you tell? Companies such as Chase DO use e-mail to market offers to existing customers—but they will not ask for personal information. Legitimate e-mails link to the exact company—in this case, chase.com.

Practice safe browsing. Don't click on e-mail links. If an e-mail offer interests you, go directly to the company's homepage to learn what they offer. To find the company's legitimate web site and web address, type its name in a search engine such as Google.

2. PayPal Example

This e-mail is phish

How can you tell? No web site, phone number, address, or contact person are listed. Donations are limited to PayPal—legitimate organizations would accept other forms of payment.

*This is one of those cases where it is better to be safe than sorry. To ensure that contributions to non-profit organizations are used for intended purposes, go directly to recognized charities and aid organizations websites. **Do not click on a link to another site.***

3. Washington Mutual Example

This e-mail is phish

How can you tell? Consider the ways legitimate companies might communicate with customers by e-mail. If your credit card company found a suspicious purchase, would it send you an e-mail? NO! The company's fraud department would call you on the phone. This is a good example of "Click here or something bad will happen to you" — a sure sign of fraud that uses a sense of urgency and fear to lure you in.

When an e-mail doesn't make sense, contact the company directly.

4. MSN (Microsoft Network) Example

This e-mail is phish

How can you tell? The URL link in the e-mail does not link to www.msn.com—the Microsoft Network's official domain. Phishing e-mails often use false domain names (www.msn-reactivation.net) that contain a bit of the real company's name. Yes, this URL contains "msn" but anyone can establish a link containing 3 letters or even a name.

Things might not be what they seem. You can spot the tricks if you look closely.

5. Amazon Example

This e-mail is phish

How can you tell? Look at the link: In some browser applications, when a URL uses an @ sign, everything to the left of the "@" is disregarded and the browser only reads to the right of the @ sign. This is a common phishing trick.

When you see or suspect an @ trick, hit the delete button.

The Bottom Line

Be suspicious of all unsolicited or unexpected emails you receive, even if they appear to originate from a trusted source.

Be suspicious of any email with urgent requests for personal financial information.

If you receive "phishing" or "spoofed" e-mails:

- forward the email to reportphishing@antiphishing.com
- forward the email to the Federal Trade Commission at spam@uce.gov
- forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@msn.com")
- when forwarding spoofed messages, always include the entire original email with its original header information intact
- notify the Internet Fraud Complaint Center of the FBI by filing a complaint on at www.ifccfbi.gov

Test Your Credit Card Fraud IQ

Test to see if you are at risk for Credit Card Fraud. Check "True" or "False" to answer the following questions.

- 1) You should keep your Social Security number in your wallet at all times. True False
- 2) Never allow anyone to use your credit cards. True False
- 3) You should always shred unwanted credit card solicitations you receive in the mail before you throw them away. True False
- 4) You should write down your personal identification numbers on your credit cards so you won't forget them. True False
- 5) Keep an eye on your credit card when it is being used for a payment transaction. True False
- 6) You should check your credit report at least once a year. True False
- 7) It is safe to give out your personal information or account and credit card numbers when responding to e-mails you receive. True False
- 8) You should carry all of your credit cards whenever you go shopping. True False
- 9) If your credit card statement doesn't arrive in the mail, you don't need to pay your credit card bill. True False
- 10) You should review your credit card statements as soon as you receive them. True False

Answers:

- 1) **False.** No one should carry their Social Security card with them unless they need it for business reasons such as filing for an unemployment claim or enrolling in school.
- 2) **True.** You shouldn't allow anyone to use your credit card, as you will be responsible for the debt.
- 3) **True.** Always shred credit applications as well as credit statements before you throw them away.
- 4) **False.** Never write down your personal identification number (PIN) on your card. It's best to memorize your PIN.
- 5) **True.** Keep your eye on your card to avoid someone stealing your credit card information. (Skimming)
- 6) **True.** Check your credit report at least once a year to make sure all the information is accurate.
- 7) **False.** It is not safe to give out your personal information in response to e-mails you receive. (Phishing)
- 8) **False.** You should only carry the credit cards you plan to use that day.
- 9) **False.** You are responsible for paying your credit card bill each month whether you receive the statement or not. If you don't receive your credit card statement in the mail around the expected due date, contact your credit card company.
- 10) **True.** Review your credit card statements as soon as you receive them to make sure there aren't any mistakes or unauthorized charges.

Write down all of your credit cards, account numbers, company contact information, payment due dates, and approximate statement arrival dates for your records. Keep this information in a safe place. It will come in handy in case you ever need access to your card information or if you have to report lost or stolen cards

Credit Card Log

Name of Creditor	Account Number	Billing Address	Phone	E-mail	Payment Due Date	Statement Arrival Date