Can You Catch a Phish?

re the following emails legitimate or phish (scams)?

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

CHASE

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.

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.

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.

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 to learn more about UNICEF's Tsunami Disaster Relief efforts.

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 this donation, so that UNICEF will receive 100% of the amount you donate.

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

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

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.

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/

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 email 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.

om: msn-database [mailto:information-msn@billing-msn.org]
te: Tuesday, November 09, 2004 7:43 AM
: Mary Smith
bject: ATTENTION: Your MSN account could be blocked

ear MSN member,

s an MSN member, you have received this e-mail,
'e want to inform you that your MSN account information has expired.
ou must update your account information,
herwise we will block access to your account.

o update your account click here http://msn-reactivation.net.

ncerely,
SN Customer Care

//msn-reactivation.net/

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.msnreactivation.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.

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

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 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.

Test Your Credit Card Fraud IQ

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 Insurance 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