

FCPN# FY04-05 US Bank Email Scam

Note: Level 4 APCs - IT IS YOUR RESPONSIBILITY TO GIVE THIS NOTICE WIDEST DISSEMINATION TO PROGRAM PARTICIPANTS TO INCLUDE APCs, AOs, Certifying Officials and Card Users (if applicable) IN YOUR HIERARCHY.

Identity theft and e-mail spoofs are no longer a rare occurrence because of the increased use of electronic communication methods. What is identity theft? It is the fraudulent use of another person's personal information to commit theft. This goes beyond our traditional concept of fraud, where a person has his or her credit card number stolen that results in an unauthorized charge made by someone other than the true accountholder. It is far broader in nature, because identity theft means another person's identity has been stolen to commit a crime. What is an e-mail spoof? It is misrepresenting an e-mail to make it look like it came from a legitimate organization or person. The usual goal of these e-mails is to mislead the recipient into providing personal and sensitive information, e.g., social security number. This kind of e-mail is also known as "phishing".

Credit card scams have always been around but the Internet and email have allowed these scams to reach a far greater audience and potentially cause even more damage than in the past. Some of these credit card scams have two goals: to obtain valid credit card numbers and to harvest email addresses for future spam and scam purposes. These emails look very authentic and can easily trick unsuspecting users into divulging their credit card numbers, bank account information, and enough personal details to facilitate everything from credit card fraud to identity theft. **Your best bet? Give no response and simply delete the email.** The bank has this information already and would not send out a request asking you for what they already have.

Click on the following link for additional information on the US Bank email scam:

http://urbanlegends.about.com/library/bl_us_bank_scam.htm

The following email scheme (also known as scheme phishing) has been circulating in the field.

This is not a legitimate request from our office or that of US Bank:



Dear U.S. Bank valued customer:

In an effort to protect your U.S. Bank account from fraudulent activities, we have upgraded our security software.

Your account will be automatically upgraded once you enter your security information in order to verify your identity. Access to your bank account will not be interrupted and will continue as normal. However, failure to do this may result in your account suspension for a certain period of time.

Please fill in your account information below.

[U.S. Bank Internet Banking](#)

Copyright 2004 U.S. Bancorp

Do not respond

The following are tips to help prevent identity theft and having your e-mail account spoofed.

- Safeguard your credit
 - Keep a list of your credit card numbers in a safe place along with contact numbers/addresses
 - Review your credit reports regularly
- Protect your cards
 - Sign new and reissued cards immediately
 - Always notify your bank and credit card companies of address and phone number changes
 - Store your cards in a safe place
 - Report lost/stolen cards immediately
 - Never leave your card as a security deposit
 - Close inactive accounts
- Keep your personal information personal
 - Never give your social security number or credit card account number to an unsolicited caller
 - Do not leave receipts at ATMs, gas pumps, etc.
 - Never let your debit or credit card account number be written on a check or other documents
 - Tear or shred your credit card receipts
 - Do not throw personal information in public trash containers
 - Keep your passwords in a secure location
 - Don't carry your social security card with you
- Secure your computer
 - Do not download files from strangers
 - Use a secured browser
 - Delete personal information if you dispose of your computer
 - Review the privacy policies of the website you visit and confirm if data is shared with third parties before you submit any of your personal information

If you think your identity has been stolen, you should...

- Contact US Bank to close the account(s) that you know or believe has been tampered with or opened fraudulently
- Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge
- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime
- File your complaint with the Federal Trade Commission (FTC). The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations

All Fleet Card Periodic Notices (FCPNs) are located on our website www.don-ebusiness.navsup.navy.mil under the Policy tab. Please send any questions/comments to fleet_card@navsup.navy.mil.

Helpdesk
Navy Fleet Card Component Program Manager (CPM)
DON eBusiness Operations Office
Card Management Office
5450 Carlisle Pike; P.O. Box 2050
Mechanicsburg, PA 17055
Fax: (717) 605-9362
fleet_card@navsup.navy.mil