

Member Awareness of Potential Risk of Online Transactions

Prevent Identity Theft

Doing business online is becoming more common every day, but we must be diligent to protect ourselves from fraud and identity theft. Please review the following paragraphs about how to protect yourself online

Phishing Phishing," is the practice of sending an e-mail that appears to be from a reputable company that you recognize and do business with, such as your financial institution. The e-mail will typically warn you of a serious problem that requires your immediate attention. The e-mail will then encourage you to click on a link to go to the institution's "website" in order to update your account information or to provide information for verification purposes: your Social Security Number, account number, PIN or password, credit card information, or verification information such as your mother's maiden name or place of birth. The goal of phishers is to persuade you to share this sensitive information that can be used to commit fraud or identity theft against you. If you feel the e-mail may be legitimate, please contact the company or financial institution directly through a listed telephone number, but never through the link provided in the e-mail you received. **NEOFCU will never ask you to verify sensitive or private information in an email.** We will never ask for your user name, password or other electronic banking credentials. Please be aware that you have already given legitimate companies (like NEOFCU) the information they need to do business with you. If you have any questions regarding the legitimacy of an email, contact the institution you received it from by phone.

Vishing A scam dubbed "vishing," mimics phishing by trying to trap you into divulging your account numbers over the telephone. With vishing, instead of being phished in an e-mail message, you may receive a telephone call from an automated random dialer, and the voice on the other end of the line may tell you your credit card has been used illegally. You are then asked to dial a fake 800 number with another voice that asks you to confirm your account details and credit card number. If you give the information, you can count on your accounts being drained. Read the following tips on how to avoid being vished:

- If you get a phone call and someone asks you to give or confirm credit card or personal information, hang up. Then call your credit union or the financial institution that issued the card by using the phone number on the back of the card or on your statement and report the attempt.
- If you get a call from someone who claims to be from a financial institution you do business with, and who knows your credit card account number but wants the three-digit code on the back of the card, immediately hang up.
- If you get an e-mail message asking you to call a toll-free number to verify account information, delete the e-mail. Never provide personal information or account information based on an e-mail request.
- Don't be fooled by the fact that the caller's phone number appears to be a regional telephone number--it could have been spoofed.
- Be suspicious of any phone or e-mail contact that doesn't use your full name.
- Never dial a call return number--or reply to an e-mail--regarding any financial matter.

The NCUA said vishing is attractive to criminals because Voice over Internet Protocol (VoIP) technology is fairly inexpensive, especially for long distance, making it cheap to make fake calls. Also, because it's Web-based, criminals can use software programs to create phony automated customer call center service lines. It also exploits the public's trust in landline telephone services

What To Do If You Suspect Identity Theft First, contact your financial institution(s) immediately and alert them to the situation. Next, contact the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here's the contact information for each bureau's fraud division:

Major Credit Bureaus
Equifax: 800-525-6285, P.O. Box 740250, Atlanta, GA 30374
Experian: 888-397-3742, P.O. Box 1017, Allen, TX 75013
TransUnion: 800-680-7289, P.O. Box 6790, Fullerton, CA 92634