Scam Alerts

New Money Moving Scam Uses Members' Personal CU Accounts

Summary:
Credit union members seeking jobs have fallen victim to a new money moving scam. A recent case displayed a scammer's technique, which utilized a member's personal credit union account to move money. Be on the look out for incoming ACH credits (less than $10,000) being posted to a member's account.

Details:
Credit union members seeking jobs have fallen victim to a new money moving scam. A recent case displayed a scammer's technique that utilizes a member's personal credit union account to move money. The original funds were placed into the "newly hired" member's account as an ACH credit. The funds were withdrawn by the member, who then went to a Western Union location to wire the funds to the scammer's "business partners."

New Phishing Scam Sounds like Official Telephone Call

A new twist on phishing aims to obtain the three-digit security code printed on the back of VISA and MasterCard credit and debit cards. The phishers are trying to get enough information to perform fraudulent card-not-present transactions (Internet, telephone, and mail-order purchases).

Under this scam, a telephone call is placed to a legitimate cardholder. The caller claims to be a representative from VISA or MasterCard informing the cardholder of suspicious card activity. The caller provides details of an unusual transaction and asks if the cardholder made this purchase, which, of course, the cardholder did not. The cardholder is then asked to verify possession of the card. To do so, the cardholder is asked to read the three-digit security code on the back of the card. The fraudster then provides a control number in the event the cardholder needs to call back with questions, making the call seem legitimate.

The caller does not ask for the credit or debit card number, and that is why some members are fooled into believing the call is legitimate. But the fraudster already has the card number; what they don't have is the three-digit security code from the back of the card, and that is what they are after with this scam.

The three-digit code on the back of the Visa or MasterCard card is a security tool used for non face-to-face transactions. When conducting transactions that are not face-to-face, many merchants will ask the shopper for the three-digit code to complete a card authorization. If the criminal obtains this three-digit number and already has your card number, card expiration date, and billing address, the criminal may be able to obtain authorization for fraudulent transactions.

It is critical that all members be aware of all plastic-card security measures, including the use and purpose of the three-digit code on the back of the card. You should never give that code to anyone who may contact you by telephone, Internet, or mail. This security tool is used when a card-not-present transaction is performed, and during the transaction the merchant may ask for the code to complete the authorization process.

Never respond to any e-mail, telephone call, voice message, text message, or letter received through the mail that requests personal and financial information, including the three-digit number on the back of the card.

WARNING - NEW Verified by VISA Phishing Scheme!

The Credit Union would like to advise you of a fraudulent email being sent to cardholders who participate in Verified by VISA.

The email claims to be from Visa and states that the cardholder was automatically enrolled in Verified by VISA. The email also states that the cardholder's Visa card may be temporarily disabled if they failed to update their Visa card.

This email is a phishing scam and did not come from Visa. Phishing is a form of fraud that attempts to

trick the cardholder into revealing personal information, such as their credit or debit account numbers, share draft (checking) account information, social security numbers, or online banking account passwords through fake websites or in a reply email.

Visa will NEVER ask cardholders to divulge account information or passwords via email. If you should receive any questionable emails, we ask that you DO NOT reply to them or contact the website referenced in the email.

The Empire One Federal Credit Union asks that you beware of any situation resembling this scam. If you notice anything out of the ordinary and/or suspicious, please notify our office immediately at 716 854-2458.

PHISHING - BE AWARE!

Phishing is a type of Internet piracy. Internet thieves are looking to obtain your personal financial information usually through an e-mail or, in some cases, a telephone call that appears to be coming from a reputable company. Here's what you can do to stop them and protect yourself?

NEVER provide personal financial information (i.e. Social Security number, account numbers, PIN numbers, passwords) if you did not initiate the contact.

NEVER click on a link provided in an e-mail you believe to be fraudulent.

IF you believe the contact may be legitimate, contact the financial institution yourself. The key is that YOU should be the one to initiate the contact.

DO NOT be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.

REVIEW account statements regularly to ensure all charges/activity are correct. You may want to take advantage of electronic account access (i.e. Virtual Branch Home Banking or E-Z Access Audio Response) to periodically review activity online to catch suspicious activity.

IF you fall victim to an attack, ACT IMMEDIATELY to protect yourself. Alert your financial institution. Place fraud alerts on your credit files and report suspicious e-mails or calls to the Federal Trade Commission (FTC). File a complaint at www.ftc.gov. You can visit the FTC's Identity Theft website at www.ftc.gov/idtheft to learn how to minimize you risk!

The Empire One Federal Credit Union asks that you beware of any situation resembling this scam. If you notice anything out of the ordinary and/or suspicious, please notify our main office immediately at 716-854-2458.
