

Jax Federal Credit Union Phone Scam Alert (Vishing)



September 22, 2008

We have received numerous calls from members and non-members reporting automated calls beginning Sunday evening, September 21st from 11:30 pm - 1:30 am. The message states "your Jax Card has been suspended. Please enter your debit card number to re-activate."

According to CUNA, multiple phishing scams posing as various credit unions have begun circulating. In some of these scams, members and non-members are receiving e-mails and cell phone text messages or phone calls informing them that their online account access, credit card or debit card has been suspended. Recipients are asked to enter the card number or are provided with a phone number to call to re-instate their online access (this is how the fraudsters steal their account information and potentially withdraw funds.)

Vishing mimics phishing by trying to trap you into divulging your account numbers. (Phishing is the act of sending an e-mail to a user, falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.)

But 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're then asked to dial a fake 800 number with another voice that asks you to confirm your account details and credit card number.

All this is possible because of Voice over Internet Protocol (VoIP), the new technology that makes possible inexpensive and anonymous Internet calling. And industry analysts are concerned that it's becoming more difficult to tell phish and vish from actual attempts to contact customers.

Take steps 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 the call was legitimate, the provider will know it.

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 that the caller's phone number appears to be a regional telephone number--it could have been spoofed, which is easy to do using VoIP.

Be suspicious of any phone or e-mail contact that doesn't use your first name or surname.

Never dial a call return number--or reply to an e-mail--regarding any financial matter.

When it comes to scams, knowledge is your best defense. ***Jax Federal Credit Union will NEVER contact you to obtain your personal financial data via any means, including email, phone, instant message and mail.*** If you're a member, we already have it. So if you receive any type of solicitation asking for personal financial information, do NOT provide it — it's a scam.

