In the News: October 2019

Protect Yourself Against Fraud

Be aware that fraudulent activity and intermittent scams are now happening through text message communication. You should not be receiving SMS text messages from the credit union unless you have signed up for text alerts. Never respond to or click on any link in a message if you aren't sure it was something you authorized.

Below are a few tips on what you should look out for, so that you are not a victim of a fraudulent scam.

Criminals in possession of member card details and other forms of personally identifiable information (PII) are imitating credit union phone numbers (spoofing) in an effort to fool credit union members into thinking that text messages are actually from the credit union. Fraudsters are sending text messages with the reason of trying to validate recent card activity and are including hyperlinks within some text messages. Fraudsters are also using text messaging to deceive credit union members into providing card-related data and login credentials.

Attacks to obtain personal information from credit union members are known as SMishing (SMS text phishing) and Vishing (Voice phishing). A typical SMishing occurrence can begin with a member receiving a text message inquiring about a suspicious transaction on an account. In reality, the fraudster is looking to obtain other information from members such as debit card numbers, CV2 codes (security code on the back of the card), expiration dates, PINs and other web login credentials. A legitimate request for validation from your credit union would NOT ask for this information!

SMS/Texts from you credit union will NOT include:

- Requests for CH data, such as card numbers, PINs, CV2 Codes, Expiration Dates
- Vague reference of "Merchant" Transaction details should be included
- Hyperlinks to unknown websites
- Phone Numbers as Hyperlinks

In another scenario, fraudsters are posing as credit union employees in order to obtain One Time Passcodes (OTP) from members. While on the phone with a member, the fraudster logs into a credit union online banking site. When the OTP is sent to the member's phone, the fraudster asks the member to provide the OTP as a means to validate the member. When the information is shared with the person the member believes is a credit union employee, the fraudster uses the OTP to finalize access to online banking, which is typically followed by changing the online banking password and transferring funds from member accounts.

Suggested Best Practices for Members

- Always be cautious when responding to SMS text messages as well as voice calls, even if they appear to come from the credit union.
- Call the credit union using a reliable phone number (best to use a published number such as found on your credit union website) to question any SMS text messages or voice calls supposedly received from the credit union.
- Never provide personal information in response to SMS text messages and phone calls supposedly received from the credit union.
- Do not click on links included in text messages from unknown sources. Legitimate requests to validate card activity will request a simple response of YES or NO. They will NOT include hyperlinks to other websites or ask for any personal info.