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, expiration dates, PINs and other web login credentials.

Below is a summary of items included on a valid fraud text message from CO-OP on behalf of a credit union and what items will not appear on a legitimate outbound message.

SMS/Text will include:

- CU abbreviated name
- Last 4 of Card #
- $ Amount in question (with dollar sign)
- Merchant Name
- Reply Options: YES, NO, STOP (to opt out)

SMS/Text 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

- Warn members of SMiShing and Vishing scams. Instruct members to be cautious when responding to SMS text messages as well as voice calls, even if they appear to come from the credit union.

- Advise members to call the credit union using a reliable phone number to question any SMS text messages or voice calls purportedly from the credit union.
- Inform members to never provide personal information in response to SMS text messages and phone calls purportedly 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.

If you receive any suspicious calls, emails, or text, contact Michigan Coastal Credit Union at 231-777-3620.