

The following are phishing techniques that fraudsters are using to capture members' personal and financial information:

- **Scam: Social Networks**
 - Members should be wary of clicking any links in emails or accessing social networking sites for holiday themes such as Halloween upon us. Holiday scams contain links that redirect members to an indirect site registered by the fraudster.
- **Prevention:**
 - Members should close their browsers if they see a link to download or install an application.
- **Scam: Call Forwarding**
 - Fraudster is call forwarding your members' landline or cell phone number to another telephone. In most cases, it's a prepaid cell phone.
- **Prevention:**
 - Members should place a password on their telephone numbers to prevent them from being call forwarded.
- **Scam: Text Messaging**
 - Fraudster sends a text message (smishing) and your members respond to the request.
- **Prevention:**
 - Credit unions should advise members to be alert when text messages appear on their cell phone, smart phone or PDA device. If the text message requests personal or financial information, members should contact the credit union immediately and not respond to the text message.
 - If a smishing attack occurs, proactively communicate to members via statement stuffers, website alerts and voice message alerts.
- **Scam: System Intrusions**
 - Fraudsters are focused on phishing your members to provide account numbers, passwords and user names to get into the home banking system. The industry has shown an up tick in system intrusions through unauthorized ACH and/or wire requests.
- **Prevention:**
 - Credit unions should implement multifactor authentication to prevent fraudsters from gaining access to systems.
 - Members should monitor their transaction activity daily to help identify any unauthorized activity. They should watch for unauthorized ACH or wire transfers.
 - Credit unions should communicate with members to never share their user names, passwords and any account information.
- **Scam: Voice Vishing**
 - This scam attempts to trick members into providing personal and financial information over the phone. Most vishing scams begin with an email or text message asking your member to call a toll-free number. When members call the number, they are led through a series of voice prompted

menus that ask for key financial information such as a card or member account and the PIN.

- **Prevention:**
 - Members should not call the telephone number. Rather, they should report this to the credit union and telecommunications carrier immediately. This number needs to be shut down to help prevent others from responding to the attack.
- **Scam: Spoofing Caller ID**
 - Members receive a call from either a live person or a recorded message with a spoofed caller ID. The caller ID may list a legitimate looking telephone number. Fraudsters have spoofed caller ID systems or assign any area code to a phone number so it appears to be an 800 number or a local number.
- **Prevention:**
 - Members should never provide any personal or financial information to the caller. Always hang up and contact the credit union to report this activity. Your credit union will not request personal or financial information from you via a telephone call.

Email, text message and phone calling are various forms of phishing. Fraudsters are asking for other types of information beyond card information to steal money from your members. Ongoing member education is critical since these types of attacks are not going away.