

## **PHISHING SCAM COMMON PHRASES**

If you see any of the following phrases in unsolicited emails, phone messages, or text messages, they should immediately alert you that someone may be attempting to deceive you into providing personal and/or account information. **DO NOT RESPOND** to these communications!

***"Verify your account..."***

Your credit union, other financial institutions, and credit card companies will never ask you to supply information via unsolicited communications that they already have - this also includes passwords and PIN numbers.

***"If you don't respond within 48 hours, your account will be closed..."***

This phrase is meant to convey a sense of urgency - legitimate companies will not arbitrarily close your account.

***"Dear valued customer..."***

Phishing attempts are often sent out in bulk (ie, email distribution list from an internet provider, phone number list from the phone book) and often do not include your first or last name.

***"Click the link below to gain access to your account..."***

***or***

***"Call this number and enter your account number..."***

Links or phone numbers contained in unsolicited emails, text messages, or phone messages often look like the real company website pages or sound like customer service automated systems but are actually fake and designed to trick you into supplying personal or account information - only utilize links and phone numbers from the actual company website or customer service, not those contained in unsolicited communications.