

## Understanding Various “Phishing” Attacks

There has been a general increase in “phishing” attacks that are focused on text message (smishing) or phone calls (vishing). The text message and phone calls are being sent to members and non members indicating they are from a credit union or a credit union league.

**Details:** The phisher focuses their efforts on sending out large phishing blasts via phone numbers and text messages. They have been successful in some cases as individuals have responded by providing personal and financial information. Phishing remains a leading fraud exposure to the industry in 2010. Although the delivery channel’s of the attacks has shifted from email links to text messaging and phone calls, they continue to occur daily. The following defines the recent phishing methods:

**LAND LINE TELEPHONE “VISHING”** Vishing, is the voice counterpart to phishing. Rather than being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's card number or other personal or financial information. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number or another area code within or outside of the United States. Because people are used to entering card numbers over the phone, this technique can be effective.

**TEXT MESSAGE “SMISHING”** Smishing is the mobile phone counterpart to phishing. Rather than being directed by e-mail to a Web site, a text message is sent to the user's cell phone or other mobile device with some ploy to click on a link. The link causes a Trojan to be installed in the cell phone or other mobile device.

### **In Order to Mitigate the Risk of “Phishing” Attacks:**

- Be aware that PFCU will never ask you for personal or financial information via text message or phone calls.
- Report the telephone number to your local carrier immediately in an attempt to shut down the telephone number.
- File a complaint with the Internet Crime Complaint Center [www.ic3.gov](http://www.ic3.gov).
- If you have doubts about who's on the phone, call back the number of record for your financial institution or Card Company.
- Be wary of any message, especially text or phone calls.
- Do not open unsolicited e-mails or text messages.
- Monitor your financial accounts on a regular basis.
- Immediately report any suspicious activity on your account to us.
- Never respond to text messages or phone calls asking for personal or financial information, regardless of who the sender appears to be.

Source: CUNA Mutual Group- Credit Union Protection Response Center  
March 24, 2010

