# Fraud Alert

## Phishing Information March 17, 2014

People's Credit Union has received notification that phishing scams have been attempted at multiple credit unions. Cardholders may receive what appear to be automated phone calls or texts, telling them that their ATM/Debit cards are locked.

The automated message requests call recipients to "Press 1" where they are to enter their 16-digit card number into their telephone key pad. Once this is entered, the scammers are then requesting the card's Personal Identification Number (PIN). The scam artists are attempting to obtain customer card numbers and PINs in order to gain access to customer accounts via ATMs or POS (point of ale) purchases.

Phishing is the act of attempting to acquire personal information such as passwords and credit or debit card details by masquerading as a trustworthy entity such as a credit union, bank or credit card company.

Criminals will use an email, telephone messages (vishing) or text messages on cell phones (Short Message Service or smishing) to trick recipients into disclosing personal and financial data.

Some phishing attempts ask e-mail or text recipients to respond with personal information; and others include links to what appear to be familiar Web sites but are really spoofed copies. Once the user clicks on the link to the spoofed site, all future online activity gets funneled through the phisher's system, giving him or her access to any account numbers and passwords the user enters online.

In phishing attacks, the criminal configures a dialer to call phone numbers in a given region or accesses a legitimate voice messaging company with a list of phone numbers stolen from a financial institution. A recording alerts the member that their credit or debit card has fraudulent activity or has been frozen and to call a phone number. When the number is called they are asked to enter a card number on the key pad, PIN, expiration date, SSN and date of birth. The phishers now have enough information to make fraudulent use of the card.

**How do you protect yourself from phishing attacks?**

**Educating yourself is the key to reducing losses from phishing scams.**
Members need to know exactly how **phishing scams** work and how to avoid becoming a victim.

1. NEVER respond to an e-mail asking you to verify or update your personal information
2. Never click on links in unsolicited e-mail that you receive
3. Delete any unsolicited e-mail in your e-mail accounts – don't even open them!
4. Never tell anyone your PIN and never write it down
5. Guard your PIN from being seen when you are completing a transaction at an ATM or in a store
6. Protect your passwords. Never write them down or enter them online unless *you* initiated the transaction.
7. Never give out your personal or financial information on the phone or online unless you initiated contact
8. Check your credit report at least once annually or sign-up for weekly or monthly alerts through credit management agencies
9. At home, use spam blockers, firewalls, virus protection, and adware & malware destroyers
10. Update your Operating System whenever security patches are available

**Please report any suspected fraud and / or phishing attempts to People's Credit Union at (337) 393-2495.**