

PROTECT YOURSELF – READ THE FOLLOWING FROM THE WISCONSIN CREDIT UNION LEAGUE

More Wisconsin credit unions have reported that residents in their area have received bogus telephone calls notifying them that their debit card has been deactivated. Similar messages have been reported by other financial institutions around the country in recent months.

These calls seem similar to those that The League described in an October 2009 *Scam Alert*. One of the Wisconsin credit unions reports:

Over the weekend an automated call has been calling members and nonmembers. The system states that the credit union has been shut off and to press one to reactivate. One of our members did press one to find out what would happen and it asked for their debit card number. He hung up.

One member said they got two calls, one saying her debit card was shut off at one credit union and another one saying her debit card at her other credit union was shut off.

This call has been going out to nonmembers as well. Our switchboard has been ringing off the hook all day. We are beginning to think the entire city of got calls. As of right now all calls have been going to landlines, however at least one was to a cell phone.

Another Wisconsin credit union has posted a warning on its website urging members not to respond to the calls:

We have been made aware of a new cell phone scam that is targeting people with debit cards. Some members have received automated cell phone messages stating that "All [credit union] Debit Cards have been DEACTIVATED" or something similar. The members are instructed to respond to the alert in order to reactivate their cards. This is a scam. If you receive this automated phone message, please ignore it. Please be assured that your card has not been deactivated.

Law enforcement officials in other states have encountered similar calls and advise:

- In this scam consumers receive a phone message or call, stating their card has been deactivated.
- The consumer is instructed to call a toll free number to reactivate the card. Upon calling the number, consumers are instructed to enter their debit or credit card number and their PIN. After entering the numbers, consumers are told the card has been reactivated.
- Responding to this phone message could result in identity theft and financial loss. Debit and credit card companies and banks do not request consumers to provide their personal identification number (PIN) or personal security information over the phone, through email or text messages.

Phishing has many forms

The phone call is a "phishing" scheme aimed at gaining access to consumers' financial information.

Most phishing attempts so far have used email or VoIP telephone calls to pass on a bogus message. Some credit union members and the general public are also getting fraudulent text messages, which some call "smishing." In smishing, a text message tries to lure a recipient into giving personal information via SMS, the communications protocol used to send text messages to a wireless device.

Member Education

It is important to be proactive and educate your members through media such as your webpage, newsletter articles, and statement stuffers on security basics such as:

1. Do not respond to phone calls, text messages or emails from financial institutions or other seemingly legitimate parties unless you initiated the contact.
2. Contact your financial institution before responding to any request regarding financial accounts and debit or credit cards, unless you personally initiated contact with the institution.

3. Do not provide your personal or financial information including account numbers, passwords, PIN numbers, or social security number by phone, either verbally or by touchpad, in emails or at internet sites that are not secure. (Look for the “s” in https:// to be sure the site is secure.) Such messages asking for such information in connection with credit union accounts are fraudulent.

4. Report that you received a “phishing” cell phone call seeking access to your personal information to your financial institution, and to your cell phone carrier.

5. Contact the credit union immediately if you have given out your account or financial information in response to a suspicious phone or text message.

Members can list their personal cell phone numbers and land line numbers on the Do Not Call list at www.donotcall.gov and file complaints with the Federal Trade Commission at www.ftc.gov and the Federal Communications Commission at www.fcc.gov.

The Wisconsin Credit Union League
N25W23131 Paul Road, Suite 500
Pewaukee, WI 53072-5779