

## 'Smishing' Scam Targets Credit Unions via Text Messaging

June 23, 2008

### Summary

Fraudsters are now sending text messages to Credit Union and other financial institution members' wireless devices to lure them into giving personal information. Because wireless devices use SMS, a communications protocol, to send text messages, this is called "Smishing."

State(s): All  
Type of Alert: Smishing

### [Loss Prevention Recommendations](#)



CUNA Mutual alerts credit unions of this risk. Please pass this information on to all appropriate employees. If your credit union has experienced a loss, contact our Credit Union Protection Response Center at 1-800-637-2676.

### **Details:**

Credit unions across the country are reporting that their member's are receiving unsolicited text messages. It's an attempt at Smishing, the latest form of phishing. In Smishing, an e-mail tries to lure a recipient into giving personal information via SMS, the communications protocol used to send text messages to a wireless device. The recent scam is targeting credit union and other financial institution members.

In smishing, the members receive a text message via cell phone warning that their bank account has been closed due to suspicious activity. It then tells them they need to call a certain phone number to reactivate the account.

Unsuspecting callers who dial the number provided in the text message will be taken to an automated voice mail box that prompts them to key in their credit card or debit card number, expiration date, and PIN to verify their information.

If you have a question concerning your account or credit/debit card, contact your financial institution using a telephone number obtained independently, such as the phone number from your statement, a telephone book, or other independent means.

## Loss Prevention Recommendations:

- **Educate** your membership on **“Phishing, Smishing, and Vishing.”**
  - Post warnings on your Web site, in newsletters, and in branch lobbies.
  - Post a notice on your credit union's Web site, stating that you will never solicit personal or private information via e-mail.
  - Be wary of any message received from an unknown sender.
  - Do not open unsolicited e-mails or text messages.
  - Do not click on any links provided in unsolicited e-mails.
- If a member is a victim of Smishing, take appropriate steps:
  - Block and reissue the compromised credit/debit cards.
  - Report the incident to the credit bureau.
  - Order a credit report.
- Don't display your wireless phone number or e-mail address in public. This includes newsgroups, chat rooms, Web sites, or membership directories.
- If you open an unwanted message, send a stop or opt out message in response.
- Check the privacy policy when submitting your wireless phone number or e-mail address to any Web site. Find out if the policy allows the company to sell your information.
- Contact your wireless or Internet service provider about unwanted messages.

If you are aware of a risk in your area, whether it has struck your credit union or not, please complete the [Report a RISK Alert](#) form.

The information contained in this RISK Alert is intended for the sole use of our Credit Union Bond policyholders to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

CUNA Mutual Group does not provide any warranties or guarantees with respect to the performance of services by any vendor, and is not liable for any products or services purchased from any vendor by any credit union. Each credit union is ultimately responsible for determining the products and services that it may require, selecting the vendor that best meets the credit union's needs (whether or not a preferred partner), and contracting directly with that vendor.