

“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."

Details:

Credit unions across the country are reporting that their members 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.