

Remember, your credit union will never contact you via text message, e-mail, phone or any other way to ask for account numbers or passwords. If you suspect you've been a victim of smishing or any other form of ID theft, contact the credit union immediately.



United States
SENATE
Federal Credit Union

National Capitol Station
P.O. Box 77920
Washington, DC 20013-8920

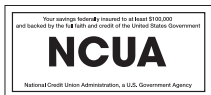
(202) 224-2967
(800) 374-2758

www.usfcu.org



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2008 National Association of Federal Credit Unions.



SF87-408

AN EMERGING ID THEFT THREAT



How to protect yourself from a growing form of fraud, "smishing," that targets cell phone users

IDENTITY THIEVES HAVE A NEW TARGET: CELL PHONE USERS

Recent media and government reports point to an identity theft threat for the nation's millions of cell phone users. The scam has been dubbed "smishing" (or "SMiShing"), a term derived from the SMS technology that's used for cell phone text messages.

Although wireless telephone companies are working to block unwanted text messages, users are reporting increasing numbers of "spam" messages and smishing attacks. Adding insult to injury is the fact that users must pay for the text messages they get on their cell phones.

HOW THE SCAM WORKS

The scam is similar to the deceptive e-mail and phone schemes known as phishing and vishing. In all these forms of fraud, scammers try to trick victims into revealing personal information like account numbers, Social Security number and passwords. The personal information is then used to withdraw money from victims' accounts or obtain credit in victims' names.

In smishing scams, cell phone users receive a text message that seems to come from a legitimate source, such as a bank, e-commerce site or other financial institution. The message seeks to dupe users into clicking on a link via the phone's Internet connection, or into calling a certain phone number. Both the link

and phone number are fraudulent, and lead to requests for personal information that can be used for ID theft. Once your identity has been stolen, it generally takes much time and effort to try to regain your lost funds and your good name.

HOW TO PROTECT YOURSELF

Now that you're aware of the problem, it's wise to take a few simple precautions to protect yourself from this growing form of fraud.

- Never respond to unsolicited requests for personal financial information received via text message – even if the request appears to come from a legitimate institution that you do business with. This includes requests to "confirm," "verify" or "update" your information.
- Always be sure of who you're dealing with. Don't click on links in text messages, or call numbers listed in text messages. Verify contact information independently, and key in Web addresses yourself.
- Put passwords on all your financial accounts.
- Monitor your credit record regularly for signs of irregularities. You are entitled to one free credit report from each of the three major credit reporting agencies annually. Visit www.annualcreditreport.com, call 1-877-322-8228, or write to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.