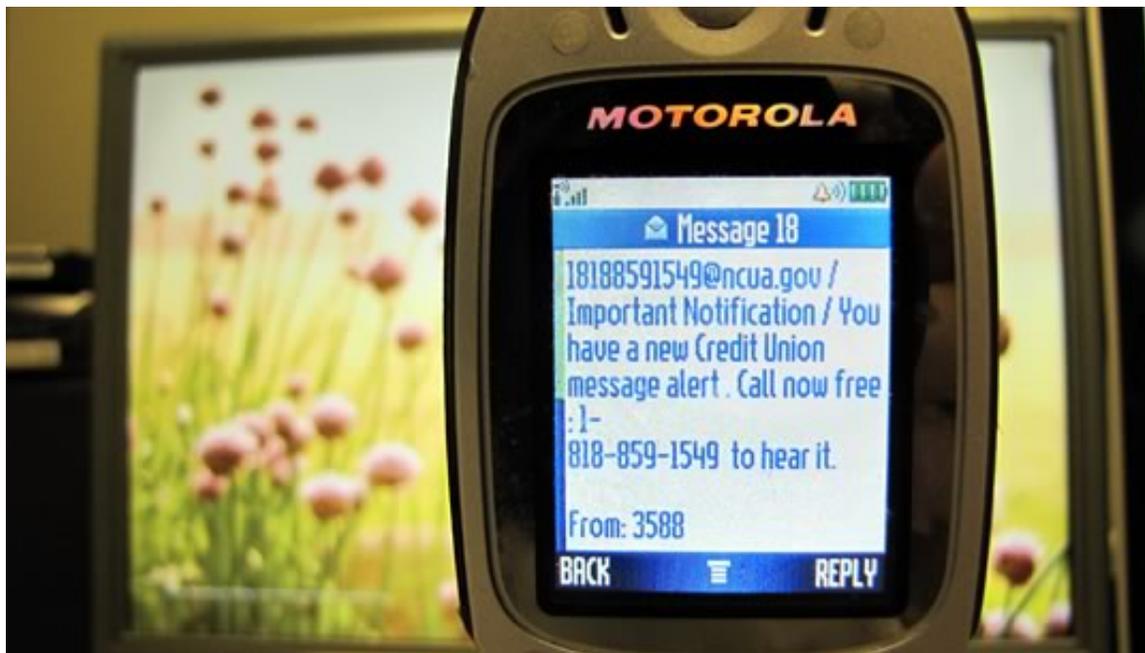


SMiShing is a scam using cell phone SMS text messages to deliver the "bait" to get you to divulge your personal information. The "hook" (the method used to actually "capture" your information) in the text message may be a web site URL. Smishing messages may threaten the recipient about an impending charge that can be cancelled only if the user visits a phony Web site displayed in the message.

Another common "smishing" scam directs the text message recipient to call a toll-free number to complete or cancel a financial transaction. An "operator" at the number will helpfully take the caller's credit card or debit account number – and use that information to defraud the caller if they are part of a scam. In this call, they are trying to capture a credit card number, expiration date, PIN, and card security code. With this information they will attempt to make purchases online with your card, pull money from your account with an ATM, or possibly create a fake card containing your information.



"SMiShing recipients should not respond to the sender. In fact, they should not call any telephone numbers provided in the text message – nor should they click on any Web links. Activating Web links that appear in unexpected text messages may direct users to fraudulent Web sites or allow identity thieves to capture users' sensitive personal information. Legitimate financial institutions do not call or e-mail customers seeking this information.

Examples of fraudulent SMiShing messages:

- Credit Union N.A. Please call us immediately at 1-888-xxx-xxxx regarding a recent restriction placed on your account. Thank you.

Your North Island CU web service is expired, for renewal please login using WWW.MYISLANDWEB.COM ASAP

Similar to “smishing”, **phishing** is an e-mail scam that attempts to trick consumers into revealing personal information - such as their credit or check card account numbers, checking account information, Social Security numbers, or banking account passwords.

From: North Island Credit Union [<mailto:renewvsr@union.net>]
Posted At: Thursday, October 25, 2007 6:32 AM
Subject: North Island Credit Union Security Info

Dear Client Of North Island Credit Union

As part of our security measures, we regularly screen activity in the North Island Credit Union system. We recently contacted you after noticing an issue on your account. We requested information from you for the following reason:

A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID North Island CU Online Expired on 10-07-2007. if you want to continue using our service you have to Renew your online if not your online will be deactivated and deleted

To continue Please Click The link below:

<http://www.northislandcus.com/>

Please notice that your debit card issued by North Island Credit Union 4337-79XX-XXXX-XXXX will be disabled until you verify your online service due to security of your payments.

Steps to Take:

If you receive a text or e-mail message that asks for sensitive information:

- Do not reply to the message.
- Do not click on any of the links that may be embedded in the message.
- Delete the message.
- Contact your bank or financial institution directly to determine if they sent you a legitimate request.