

BE ALERT! FRAUD SCAMS EVOLVE

As Americans continue to weather the financial crisis, scammer tactics evolve. Today, scammers clone financial web pages and use them for “phishing”. Phishing is fraud that normally involves email that seems to be legitimate to the user by using “safe” websites, company names and company logos. These recognized names and icons will give a sense of security when the misleading email informs a member their account has been fraudulently accessed and prompts them to call an 800 or 866 number or follow the link provided to a cloned agency or credit union website. At the cloned webpage, the member is prompted to submit private financial information such as their account number and PIN. With receipt of account information, the scammer proceeds to empty the member’s account from foreign ATM machines.

An increasingly common scam involves text messaging. Credit Union members receive a fraudulent text message announcing the unauthorized activity has occurred in their account. As with phishing emails, an 800 telephone number is provided. When the member calls, they are prompted to provide private financial information.

Geographical targeting is another method scammers use to enhance their efforts to obtain member trust and their account information. Scammers send emails and text messages to individuals within a 30-40 mile radius of a targeted credit union making the scam seem quite credible.

Scammers are also copying cashier checks issued by legitimate credit unions. They obtain an actual cashier’s check, photocopy it and print duplicates. The unsuspecting consumer who accepts an invalid check and deposits it soon discovers the check has bounced and loses whatever goods or services rendered for the check.

The SUNY Fredonia FCU will not ask members for personal account information and pin numbers via the Internet or telephone. Consumers should be leery if placed in this situation. We also recommend deleting fraudulent emails or text messages received to prevent “spyware” or “malware” from compromising computers and cellular phones. Please alert the Credit Union if you feel you are part of a potential scam.

-Information provided from the *National Credit Union Administration* November/December 2008 Newsletter