

Phishing E-mail allegedly from NCUA

March 26, 2007

Summary

phishing e-mails that appear to be sent from NCUA. The message includes NCUA's logo and is addressed to "Credit Union holder account."

State(s): All

Type of Alert: Phishing/Identity Theft

[Loss Prevention Recommendations](#)

CUNA Mutual alerts credit unions of this risk.

Details: NCUA Phishing Scam Email

Credit unions continue to report that members continue to receive phishing e-mails that appear to be sent from NCUA. The message includes NCUA's logo and is addressed to "Credit Union holder account."

The first paragraph states, "Your credit union has joined our Federal Credit Union (FCU) network. For both, our and your security, we are asking you to activate an online account on our database. After activation you can login on our system with your SSN and your Credit/Debit PIN number."

The message includes a link to the "FCU activation page" and concludes with "National Credit Union Administration Team apologize for any inconvenience."

An Internet/E-mail Fraud Alert is posted on [NCUA's Web site](#).

Loss Prevention Recommendations:

If you receive an unsolicited e-mail alleging to be from the **NCUA**, take the following steps:

- Remind your members that NCUA does not ask credit union members for personal account information.
- Anyone who has received a fraudulent phishing e-mail purportedly from NCUA should forward the entire e-mail message to Phishing@ncua.gov.
- Do not open any attachments to the e-mail, in case they contain malicious code that will infect your computer.
- If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.

- Educate your membership on “Phishing”.
 - Post “phishing warnings” on your web site, in newsletters and in your lobby.
 - Post a warning on your credit union's web site that you will never solicit personal/private information via e-mail.
 - Use the FTC (Federal Trade Commission) web site, www.onguardonline.gov.
 - Consumers can take interactive quizzes designed to enlighten them about identity theft, phishing, spam and online-shopping scams.
 - Elsewhere on the site, consumers can find detailed guidance on how to monitor their credit histories, use effective passwords and recover from identity theft.
- If a member is a victim of a "phishing email", take appropriate steps to help protect him/her.
 - Block and reissue the compromised credit/debit cards
 - Report to credit bureau
 - Order credit report
- A good resource for this topic is Anti-Phishing Working Group at <http://www.antiphishing.org>
- If you have been victimized by a spoofed e-mail or web site, you should contact your local law enforcement, US Postal Inspector, or FBI.

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.