

The purpose of this fraud alert is to inform our credit union members about a recent phishing attempt to obtain member credit card account numbers, expiration dates, and electronic signatures. In cases reported to NCUA (National Credit Union Administration), the perpetrator(s) sent fraudulent e-mails, representing to be from the NCUA, to credit union members and the general public. The emails state the NCUA will add \$50.00 to the member's account for taking part in a survey. The link embedded in the message directs members to a counterfeit version of NCUA's website with an illicit survey that solicits credit card account numbers and confidential personal information.

NCUA or the Credit Union will never ask members or the general public for personal account or personally identifiable information as part of a survey. Any email that alleges to be from NCUA and asks for account information is fraudulent and should be treated as suspicious. NCUA has taken steps to shut down this site, but members should remain alert to possible variations of this fraudulent e-mail.

If you have clicked on any of the e-mail links, please consult with a computer security or anti-virus specialist to assess the need to re-install a clean image of the computer system. You are encouraged to also take the following additional precautions:

- Scan affected computers using updated anti-virus software
- Enable automatic updates for anti-virus software and computer operating systems.
- Install security patches for common software applications promptly.
- Be aware that phishing e-mails frequently have links to Web pages that host malicious code and software
- Do not open unsolicited or unexpected e-mail attachments.
- Do not follow Web links in unsolicited e-mails from apparent federal banking agencies, instead, bookmark or type the agency's Web address.
- Call the agency using a known and appropriate telephone number to verify the legitimacy of the message and attached file.

Members affected by this scam, and variants of this scam, should forward the entire e-mail message to [Phishing@ncua.gov](mailto:Phishing@ncua.gov). Additionally, formal complaints concerning any suspected fraudulent e-mail can be filed with the Internet Fraud Complaint Center at [www.ic3.gov](http://www.ic3.gov)