

# Internet/E-Mail Fraud Alert

Recently, there have been multiple fraudulent e-mails and telephone calls directed to the general public and credit union members that appear to be from NCUA. False e-mails ask recipients to click on a link to confirm, verify or approve financial account information. If the recipient proceeds, the link directs them to a false website to verify or re-submit confidential information such as account and credit card numbers, Social Security number, password, and personal identification number, or to complete a member satisfaction survey and receive \$80.

A variant, “vishing” uses telephone systems. A vishing scam occurs when a consumer receives a recorded message telling them a credit card and/or financial institution account has been breached and to immediately call a number provided in the message. The phone number leads the consumer to a fraudulent call center where people are asked to supply or verify pertinent financial account, social security or credit card information.

NCUA does not ask credit unions members for personal information. Anyone who receives an supposed e-mail or phone call from NCUA that asks for account information should consider it a fraudulent attempt to obtain their personal account data for an illegal purpose and should not follow the instructions in the e-mail or phone call.

If you inadvertently respond and provide confidential account information, please notify your credit union immediately. You should change affected accounts and PINs, and take any additional action recommended by your credit union to protect your account.

If you feel that you have received a fraudulent NCUA phishing e-mail, please forward the entire e-mail message to [Phishing@ncua.gov](mailto:Phishing@ncua.gov)