

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

- The 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 yourself on "Phishing."
 - 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 you are a victim of a "phishing email," take appropriate steps to help protect yourself.
 - Request the compromised credit/debit cards be replaced
 - Report to the credit bureau
 - Order a 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.