

## **Risk Alert May 2010**

### **NCUA Phishing Scam**

Reports of an email supposedly coming from the NCUA have been made by local consumers. These emails appear to be “phishing” for credit card information. These emails claim that the consumer’s card has been deactivated and a telephone number is provided to reactivate the card.

It is currently believed that this is a “phishing” attempt trying to fool consumers into giving out account information which can be used for identity theft which may result in unauthorized transactions.

The following steps can help you to identify “phishing” attempts and to prevent you from becoming a victim:

- View any email request for financial information or other personal data with suspicion.
- When in doubt, don’t respond or click on any links within the message
- Contact the business that allegedly sent the email to verify if it is genuine. **Never use the telephone number within the email.** Use a telephone number of record.
- For phishing emails claiming to be from the NCUA, forward to [phishing@ncua.gov](mailto:phishing@ncua.gov).

### Signs of Phishing

- Emails may request personal information, such as bank account number, account password, credit or debit card number, PIN number, mother’s maiden name, or Social Security number. **Financial institutions and credit card companies will never ask you for this information by email.**
- Emails may not reference you by name or acknowledge the company with which you do business.
- Most emails play on a person’s emotions and have a sense of urgency, such as an alert that your account will be frozen or deactivated unless you verify your financial information.
- Emails may warn that you’ve already been a victim of fraud.
- Many times the email contains spelling or grammatical errors.

If you ever believe you have become a victim of a “phishing” attempt, contact your financial institution or credit card company immediately. For additional information about “phishing” view these websites:

<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>

<http://www.onguardonline.gov/topics/phishing.aspx>

<http://www.ic3.gov/crimeschemes.aspx>