

**Fraud Alert – April 3, 2008**



The NCUA has released information about phishing attempts that are targeting credit union employees. The following information was received from NCUA. You may want to share this information with your staff.

**Phishing Attempts – Targeting Credit Union Employees – April 2008**

FRAUD ALERT

NATIONAL CREDIT UNION ADMINISTRATION

DATE: April 2008 Fraud ALERT NO.: 08-FRAUD-04

TO: Federally-Insured Credit Unions

SUBJ: Phishing Attempts – Targeting Credit Union Employees

Dear Board of Directors:

The purpose of this fraud alert is to inform you of a "phishing" scam that may pose a significant risk to your credit union. We have recently been advised by the Federal Bureau of Investigation of a new type of phishing attack targeting employees of credit unions. These phishing attacks differ from other types of attacks in that the criminals seek to infect the employees' computers with malicious software secretly recording their keystrokes.

These attacks are in the form of e-mails addressed to the employees by name at their credit union e-mail addresses. The e-mails appear to be official correspondence purportedly from either a governmental agency or a vendor of the credit union. The e-mails include an attachment appearing as an invoice or complaint letter. When the attachment is opened, malicious software is installed that records the users' keystrokes. Once downloaded, the software is designed to monitor username and password logins and record the activity entered on the compromised machine.

Credit unions should examine their computers for the presence of malicious password-stealing software and take necessary steps to eradicate such software. The failure to identify and disinfect any password-stealing software on a credit union's computer system presents a grave risk of compromising members' account information. Management should also warn and educate their employees against falling victim to similar phishing attacks in the future.

Persons affected by this scam, and variants of this scam, should be advised to 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 (IFCC) at [www.ic3.gov](http://www.ic3.gov). The IFCC is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.

Management must ensure they file a Suspicious Activity Report when required by established regulation. As specified by NCUA Rules & Regulations Part 748, management must provide notice to the appropriate NCUA Regional Director, and in the case of state-chartered credit unions, to their state supervisory authority.

Sincerely,  
David M. Marquis  
Director of Examination & Insurance