FRAUD ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **January 2008** **Fraud ALERT NO.: 08-Fraud-02**

TO: **Federally-Insured Credit Unions**

SUBJ: **Fraudulent Activity - Vishing**

Dear Board of Directors:

The NCUA has warned numerous times[1] about "phishing" scams in which crooks send e-mails claiming to be from legitimate financial institutions, companies, or government agencies asking consumers to "verify" or "re-submit" confidential information such as bank account and credit card numbers, Social Security Numbers, passwords, and personal identification numbers. A variant on that approach using telephone systems, vishing, is increasingly being used to obtain this information from unwary consumers.

Consumers are becoming more aware that an e-mail they receive containing a link or other contact information could be malicious in nature. So criminals are moving away from primarily using email as a method to gain confidential information to using methods victims are more familiar with, like calling a number.

In essence, vishing is the criminal practice of using social engineering and Voice over Internet Protocol (VoIP) telephony to gain access to private personal and financial information from the public for the purpose of financial reward. The term vishing is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations, are known to the telephone company, and are associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing thus providing anonymity for the criminal caller. Vishing is attractive to criminals because VoIP service is fairly inexpensive, especially for long distance, making it cheap to make fake calls. In addition, because it's web-based, criminals can use software programs to create phony automated customer call center service lines.

[1] NCUA Letters to Credit Unions #05-CU-20 and #04-CU-12; NCUA Risk Alert 05-RISK-02; NCUA Media Advisory, June 15, 2006; various NCUA News Letter articles.

An example of a vishing scam is when a consumer receives a recorded message telling them that their credit card and/or financial institution account has been breached and to immediately call a number provided in the recorded message. The phone number provided in the message leads the consumer to a "fraudulent call center" established by the perpetrator of the fraud. The perpetrator then attempts to obtain confidential account information and login credentials in order to access the account. A twist on this scam is when the recorded message provides the address of a fraudulent website for the consumer to access (instead of a telephone number) and to provide certain information to reinstate the supposedly affected account(s).

Vishing is very hard for authorities to monitor or trace. To protect themselves, consumers are advised to be highly suspicious when receiving messages (telephone, email, or otherwise) directing them to call and provide personal, confidential, and/or account related information. Rather than provide any information, the consumer should contact their financial institution or credit card company directly to verify the validity of the message using contact information they already have in their possession (i.e. do not use contact information provided in the suspicious message).

Where appropriate, management must ensure they file a Suspicious Activity Report in accordance with 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. Management should also contact and file a report with local law enforcement authorities.

NCUA will continue to follow this issue and provide you with additional information as warranted. In the meantime, if you have any questions, please contact your District Examiner, Regional Office, or State Supervisory Authority.

Sincerely,

David M. Marquis
Director of Examination & Insurance