

A safety awareness message brought to you by:



“VISHING” FRAUD ALERT

The NCUA (National Credit Union Association) has warned numerous times¹ 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.

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).

Always remember that AMOCO Federal Credit Union representatives will not contact you to collect confidential account information. If you receive a call from anyone claiming to be a representative from AMOCO Federal Credit Union attempting to collect account information you should be suspicious. Instead, end the call and contact AMOCO immediately to verify the callers request for information is valid. You may call us at any of the following numbers:

409.948.8541 - local

800.392.3813 - TX

800.231.6053 – US

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.