

Watch What You VISH For

“Vishing” or Voice Phishing – the latest financial scam

Losses due to financial scams have been increasing every year, the only way to prevent various types of fraud is through education, awareness and common sense; knowing more about possible scams may keep a person from becoming a victim. Similar scams commonly called Phishing and Pharming have been in the news; Vishing is the latest twist on financial fraud, it stands for “Voice phishing.”

What is Phishing?

Phishing (pronounced fishing) is an attempt to steal a person’s financial information through fraudulent e-mails and websites designed to appear as though they were generated from a legitimate financial institution.

Like phishing, the vishing scam begins when a scammer sends a legitimate looking e-mail stating that there is a problem with the person’s account. The vishing twist is that, instead of instructing the recipient to click on a link to a phony website, the person is to call a bogus telephone number. Once the call is placed, it is answered by an automated response system that tells the victim to provide confidential information over the phone. Vishers may be sophisticated enough to select a phone number located in the same area code as the victim, helping to dispel suspicions.

The visher assumes that a person may be disinclined to click on an impersonal link, but that people have become accustomed to automated telephone systems asking them to key in account information and other details before speaking with a live representative. Just like other scams, this gives the criminal enough information to access financial accounts or make fraudulent purchases. The best defense is to always be cautious of anyone who seeks your personal financial information. Consumers are advised to follow these steps to protect yourself from becoming a victim:

- 1.** Do not respond to e-mails asking for personal information of any kind.
- 2.** Do not follow links sent by e-mails that you suspect to be fraudulent.
- 3.** Do not dial the number provided in the e-mail to investigate the situation.
- 4.** Do not ignore potentially valid warnings. At times, financial institutions will indeed contact customers if they suspect fraudulent activity. However, they will NEVER send e-mails requesting personal information.
- 5.** No legitimate institution will ever ask a person to “verify” information through e-mail. If a person receives an e-mail claiming to be from their financial institution, do not hesitate to call a valid number to confirm it.
- 6.** Only use phone numbers on statements, on the back of a credit card, or in the phone book.
- 7.** Decline to answer identifying questions if they seem suspicious.

The bottom line is: Never give out any confidential information to an unverified source.