

Online Security

Vishing (or Vhishing)

Vishing, a relatively new scam, is short for voice phishing. Perpetrators of fraudulent scams use Voice over Internet Protocol (VoIP) phones to steal personal information. A con artist sends a blast e-mail, carefully disguised to appear as though it's been sent from a financial institution, on-line payment service, or other business. It may even be so well crafted that it displays a company logo. Usually there is a report of a "security" problem and a request to call a telephone number to "straighten things out." When victims of this crime call the telephone number (an 800 or local number), they may reach an automated voice prompting them to enter account numbers, passwords, and other personal information for "verification." In another type of vishing, the visher "cold calls" victims by using an automated dialing program. Your caller ID device may show a local phone number or a legitimate-looking number to win your trust. You may speak to an "employee" or be guided by a pre-recorded message that claims your account has been compromised or needs to be updated or verified. Victims are asked to enter their account information. Any information provided is transcribed onto hard drive of the scammer's computer.

Protect Yourself!

- Exercise caution if you receive an e-mail which urges you to act quickly, verify account or personal information, and contains misspellings.
- If you receive a "vishing" phone call, hang up. Then, using the phone number on the back of your debit or credit card, call your financial institution and report the matter.
- Remember, banks do not use prerecorded messages to handle security issues. If they telephone you to report suspicious use of your card, they do not need to request identifying information because they already have that on record.
- Do not automatically trust a phone number based on its area code. Con artists can hack into Caller ID systems, and VoIP users can assign any area code to a phone number.