

### **Con Artists Switch From Phishing To Vishing**

SOUTHBOROUGH, Mass. (7/27/06)--There's a new scam on the block, dubbed "vishing," and it's coming to a telephone near you (Networkworld.com July 12).

Vishing mimics phishing by trying to trap you into divulging your account numbers. But instead of being phished in an e-mail message, you may receive a telephone call from an automated random dialer, and the voice on the other end of the line may tell you your credit card has been used illegally. You're then asked to dial a fake 1-800 number with another voice that asks you to confirm your account details and credit card number.

If you give the information, you can count on your accounts being drained.

All this is possible because of Voice over Internet Protocol (VoIP), the new technology that makes possible inexpensive and anonymous Internet calling. And industry analysts are concerned that it's becoming more difficult to tell phish and vish from actual attempts to contact customers (USA Today July 12).

A similar attack recently imitated PayPal (The Wall Street Journal July 17). The fraudulent message urged victims to call a California-based phone number to update credit card account information "to prevent any fraudulent activity from occurring." The number was traced to an Internet-phone service and shut down.

Take steps to avoid being vished:

- If you get a phone call and someone asks you to give or confirm credit card or personal information, hang up. Then call your credit union or the financial institution that issued the card by using the phone number on the back of the card or on your statement and report the attempt. If the call was legitimate, the provider will know it (InfoWorld.com July 10).
- If you get a call from someone who claims to be from a financial institution you do business with, and who knows your credit card account number but wants the three-digit code on the back of the card, immediately hang up.
- If you get an e-mail message asking you to call a toll-free number to verify account information, delete the e-mail. Never provide personal information or account information based on an e-mail request.
- Don't be fooled by the fact that the caller's phone number appears to be a regional telephone number--it could have been spoofed, which is easy to do using VoIP.
- Be suspicious of any phone or e-mail contact that doesn't use your first name or surname.
- Never dial a call return number--or reply to an e-mail--regarding any financial matter.