

SOMETHING VISHY
Be Aware of a New Online Scam

02/23/07



It's one of the latest breakthroughs in telecommunications—**Voice Over Internet Protocol, or VoIP**, which enables telephone calls over the web.

And guess who's hopping on the VoIP bandwagon along with millions of legitimate customers? Criminals, that's who. They're using the technology to hijack identities and steal money. It already has a name: "vishing."

New wine, old wineskins. Vishing is really just a new take on an old scam—phishing. You know the drill: you get an e-mail that claims to be from your bank or credit card company asking you to update your account information and passwords (perhaps, it says cleverly, because of fraudulent activity) by clicking on a link to what appears to be a legit website. Don't do it, of course. It's just a ruse, nothing more than an illegal identity theft collection system.

Vishing schemes are slightly different, with a couple of variations.

- In one version, you get the typical e-mail, like a traditional phishing scam. But instead of being directed to an Internet site, you're asked to provide the information over the phone and given a number to call. Those who call the "customer service" number (a VoIP account, not a real financial institution) are led through a series of voice-prompted menus that ask for account numbers, passwords, and other critical information.
- In another version you're contacted over the phone instead of by e-mail. The call could either be a "live" person or a recorded message directing you to take action to protect your account. Often, the criminal already has some personal information on you, including your account or credit card numbers. That can create a false sense of security. The call came from a VoIP account as well.

Vishing, as you might imagine from these scams, has some advantages over traditional phishing tricks. First, VoIP service is fairly inexpensive, especially for long distance, making it cheap to make fake calls. Second, because it's web-based, criminals can use software programs to create phony automated customer service lines.

But if the thieves are giving out their phone numbers, they should be easy to track, right? Wrong. Criminals can mask the number they are calling from, thwarting caller ID. And in some cases, the VoIP number belongs to a legitimate subscriber whose service is being hacked.

So how prevalent is vishing? Hard to say, due to reporting difficulties. "A lot of would-be victims are reporting this as SPAM or phishing," says Dan Larkin, chief of the FBI's Cyber Initiative and Resource Fusion Unit. "But we know it's out there. It's happening."

Don't let it happen to you. Larkin recommends greeting a phone call or e-mail seeking personal information with a healthy dose of skepticism. If you think the call is legit, you can always hang up and call back using the customer service number provided by the financial institution when the account was opened.

And please contact [the Internet Crime Complaint Center](#) if you think you were either a vishing victim or received a suspicious call or e-mail.

Resources:

- [More "Be Crime Smart" advice](#)
- [More Cyber Crime stories](#)
- [The FBI's Cyber Division](#)
- [Looks Too Good to be True website](#)