



ABA News to Use

Keeping banking's frontline personnel informed

Watch What You Wish For

Now there's a new electronic scam to watch out for: "Voice phishing," or simply "vishing."

It starts out in phishing fashion. A potential victim receives an e-mail that looks like it comes from an authentic source, but which says there's a problem with the person's account. The vishing twist is that, instead of instructing the recipient to click on a link, the person is to call a telephone number.

Once the call is placed, it's answered by an automated response system that tells the victim to provide the confidential information over the phone. Afterward, like with old-fashioned phishing, that information may be used for nefarious purposes, such as identity theft.

The visher relies on the assumption that while a person may be disinclined to click on an impersonal link, he or she may be persuaded to talk to what sounds like another human being.

According to reports, such an attack recently targeted the customers of a community bank in Southern California. As an indication of how sophisticated these vishers were, they selected victims located in one area code. The number the victims were to call had that same area code, helping to allay suspicions.

That doesn't necessarily mean the crooks were located anywhere near Southern California. With voice over Internet protocol, it's relatively easy to establish a phone number with any area code without the verification normally needed for regular phone lines.

Security experts say the main ways to combat this scam are the same as for phishing -- awareness, education and common sense. Everybody should be told that such scams exist and how they're carried out. Also, for vishing as for phishing, consumers should never give out any confidential information to an unverified source.

For information about ABA News to Use, or to suggest subjects for future articles, please contact ABA's [Brian Nixon](#).