

Consumer Corner

Avoiding A New Identity-Theft Scam

(NAPSA)—Consumers should be on the lookout for a new type of scam that uses Internet phone services.

The scam, known as “vishing,” involves criminals using Internet phone services (called VoIP) to trick consumers into revealing information about their bank accounts and credit card numbers over the phone.

Here’s how it works: A criminal calls you at home or sends an e-mail that asks you to call a local number. In either case, the criminal pretends to be someone from your bank or financial institution. Because the phone number on your caller ID or in your e-mail appears to be a local one, you might feel safe in calling it. However, the truth could be that the scam artist is using VoIP technology to “own” a local phone number and that he actually lives in a different state.

Fortunately, it can be easy to avoid vishers. The following answers to some frequently asked questions can help:

Q: Do people frequently fall victim to vishers?

A: Unfortunately, they do. For instance, customers of one bank received e-mails telling them that their online accounts had been disabled due to unauthorized access attempts. They were given a local phone number to call to remedy the problem. Those who called were prompted to give account information. Unfortunately, people who called the number were not talking to their bank. They were talking to a visher.

Q: How can I avoid vishers?

A: Smart safety precautions



Vishers are con artists who attempt to steal personal information using Internet phone services.

can protect you from vishers. For example, don’t give your credit card numbers, checking account numbers or Social Security number to unknown callers. Also, be suspicious of any e-mails that appear to be from your bank or financial institution. Usually, they will never contact you by e-mail.

Q: How do I know if my bank really is trying to e-mail me?

A: If you think your bank is really trying to contact you, don’t respond to any e-mails and don’t talk to anyone who calls you. Instead, call the main number for your bank found on your bank statements, in the phone book, or on the back of your credit card or check-card. The safest option is to visit your bank and ask them in person whether or not they are trying to contact you.

This information comes from the experts at Geeks On Call, who provide on-site computer services to homes and businesses across America. To contact them, visit www.geeksoncall.com or call (800) 905-GEEK.