

FRAUD ALERT!

Vishing – The Newest Security Threat

A new type of phishing scam is called "vishing." Vishing scammers typically use VoIP (Voice Over Internet Protocol) phone numbers to trick Internet or telephone users into giving their private information. It is fairly simple to get a VoIP number anonymously, which is not the case for normal telephone numbers. That makes it easier for scammers to carry out these vishing scams.

In some ways, vishing may be even more dangerous than phishing scams, because consumers are used to entering private information into automated phone systems. Therefore, it is easy to imagine that a LOT of people are going to wind up victims of identity theft and suffer financial losses from these vishing scams.

Action: Never provide personal information to an automated system (speaking or pressing numbers) – unless YOU make the initial contact with a company with which you are a customer. Even then, call the telephone number from your bank or credit card statement, the toll free number on the back of your credit card or from the telephone book. If the automated message provides a telephone number, do not call the number. Your private information should be just that, private.

Phishing – Chase and Citibank Customer Survey Spam

The subject line of the email is: *Customer Survey – Get \$50 Reward* and the text reads: *The Chase Online Department kindly asks you to take part in our quick and easy 5-question survey. In return, we will credit \$50.00 to your account - Just for your time!*

It goes on to describe how the survey will only take two minutes and that your answers will help Chase (or insert your bank's name here) with customer service and satisfaction. The email and webpage look quite authentic, and the initial questions are well thought out and professional. Of course, the spam does not really take you to your bank's website because you are directed to the scammer's site.

The catch, of course, is that they say that in order to deposit your \$50 reward, they need your Chase User ID and password, as well as your credit card number, expiration date, three digit security number, Social Security number, ATM PIN number, zip code, mother's maiden name and email address.

The ploy of using a \$50 reward for a customer service survey is quite effective. Scammers count on your need or desire for an extra \$50, especially in this economy.

Action: Never click a link in a spam email OR enter your private information into a website link. Just because the email or link has the word "Chase," does not mean it will take you to your account, you will just go to the fraudulent site. **DO NOT** give your private personal or financial information online, over the phone or in a mailer. The companies you currently conduct business with, already has your private information.

ScamBusters Newsletter #368

BUCKS COUNTY CRIMES AGAINST OLDER ADULTS TASK FORCE

Bucks County District Attorney's Office

215-348-6344

Bucks County Area Agency on Aging

215-348-0510

Bucks County Coroner's Office

215-348-3852

Network of Victim Assistance (NOVA)

1-800-675-6900

A Woman's Place (AWP)

1-800-220-8116

Bucks County Office of Consumer Protection

215-348-6060

Bucks County Register of Wills

215-348-6265

US Dept. of Health and Human Services

Investigations, Office of the Inspector General

www.crimesagainstolderadultsbucks.org

24 - HOUR HOTLINE: 1-800-490-8505