Vol. 6 No.11
November 2014

BUSINESSinsights

Beware of the newest telecom scam — Vishing

In 1991, one of today's most popular telecom features was introduced — Caller ID. Seeing who's calling before picking up the phone has helped your business better respond to customers and be better prepared to answer solicitations and other annoying calls.

It's one of the valuable features available using VoIP telecommunications. Unfortunately, VoIP and Caller ID have opened up a new door to criminals.

Just as people use email and other technologies for criminal purposes, they've found a way to use your VoIP phone systems to scam businesses and consumers by faking Caller ID. What you've known as phishing — where you receive fake emails looking like they are coming from your bank or credit card company — is now being done by phone. Because it's the voice system being used, this new scam is called Vishing.

Internet-telephone services do not require some of the verification checks used by traditional telephone companies; they provide telephone numbers with a choice of area codes that can bear no relevance to the scammer's actual location. Criminals can fraudulently display a number of their choosing on your Caller ID display or Interactive Voice Response (IVR) system. Armed with this capability, scammers pretend they are representatives of banks, credit card companies and government agencies in an attempt to solicit personal account information and money. The fake Caller ID display makes people trust the call.

A typical scam involves using VoIP with a modem to call phone numbers in a given area. When a person answers the phone, an automated recording states that the person's credit card is showing fraudulent activity. The person is directed to call a specific toll-free or local phone number immediately. The number dialed may show a spoofed caller ID for the financial company the scammer is pretending to represent. When the call is made, the recording on the other line asks you to enter your credit card number and three-digit code, which is exactly what the scammers are after.

In some cases, the thief already has your credit card number and will only ask for the three-digit code on the back of the credit card. This makes the call seem even more legitimate. Usually within 3 days of the call, the telephone line is disconnected. This, of course, makes it almost impossible to track the offender.

Sadly, a quick search for "fake Caller ID numbers" brings up a number of companies that provide this service. So anyone with Internet access and some money can pay to get and use fake caller ID numbers.

There is legislation pending to make this practice illegal. But this is still a big threat. If you and/or your employees use your business' credit card or handle business financial information, they need to be educated on this scam and understand what to do.

Here are some guidelines on what you should know and tell your employees:

- Stop trusting the information showing on Caller ID.
- If a call appears to be from your bank, credit card company, or other official business and requests financial information, end the call. Then look up the official number of that business and call them back on that number.
- Never provide company credit card or other financial information over the phone unless you are already acquainted with the representative calling.

Until now, no one ever questioned the accuracy of Caller ID displays. As much as it has helped business operations, what the display indicates is no longer reliable. Protect your business by being aware of this problem and making sure your employees are, too.

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

©Independent Distributors Assn., LLC 2014