Beware of Voice Phishing—or "Vishing"—Calls

From the Office of Minnesota Attorney General Lori Swanson

It is difficult to ignore a ringing telephone. While fraudulent emails and unwanted mail can be deleted or tossed in the trash, telephone calls are tougher to tune out. And because telephone calls are still considered a secure form of communication, voice phishing scams take advantage of consumers' trust to steal money and personal information.

In voice phishing—or "vishing"—scams, callers impersonate legitimate companies to steal money and personal and financial information. And these scams are on the rise. In fact, the Federal Trade Commission reports that 77 percent of its fraud complaints involve contact with consumers by telephone.

Vishing calls are generally made via Voice over Internet Protocol ("VoIP"). Thousands or millions of VoIP calls can be made around the world in an instant. And because these calls are made over the Internet, they are nearly untraceable. Vishing scammers also use recordings and caller ID "spoofing" (falsifying caller ID information) to further avoid detection. Placing these calls is relatively inexpensive, so even a small fraction of responses can make the scam very lucrative.

As the prevalence of these scams increases, you should know what to look for. Here are a few examples:

"Card Services" scam. "Paul" receives several prerecorded calls each month that state it is his last chance to reduce the interest rate on his credit card. The calls prompt him to press "1" to speak with a representative. Paul called his credit card company, which stated that it did not place the calls. Rather, a "visher" was trying to get his financial information.

Phony debt collection scam. "Cindy" and her family members received calls from an individual who claimed she owed a debt. The individual demanded payment within 24 hours, but refused to provide any information about the debt in writing. Cindy checked her credit report and saw that the debt was satisfied. She told her family to ignore the fraudster's calls.

Medical alert device scam. "Maureen" received a recorded call that asked her to schedule the delivery of a medical alert device ordered by her doctor. She pressed "5" as instructed, and the representative asked for her credit card information. After hanging up, Maureen called her doctor's office, which told her the call was a scam.

Bogus gift card offer. "Bill" received a call from an individual who claimed to be associated with his bank and told him he could receive a $100 gift card and a free iPad if he paid a small shipping and handling fee. Bill told the individual that he wanted to double-check the offer with his bank. Bill called his bank using the telephone number listed on his account statement and sure enough, the bank said it wasn't giving anything away. Bill blocked the visher's telephone number on his phone.

Vishing for financial information. "Sonja" received an automated call that claimed her VISA card had been deactivated and instructed her to press "9" to speak with a representative. Sonja does not have a VISA card and hung up before the visher could try to steal her personal information.

High-tech computer scam. "Stan" received a call from an individual who identified herself as a computer technician and claimed Stan's operating system security needed updating. Stan allowed the individual to access his computer, but when she asked for his credit card information to pay a $200 fee, he hung up. Stan brought his computer to a trusted local technician the next day who told him his operating system security was already up to date.

Work-at-home scam. "Mary" received a call from a consulting company representative who offered her a

job operating a website. Mary provided her credit card information to pay the $600 start-up fee. After talking it over with her son, who found an alert for the company on the Better Business Bureau website, Mary called her credit card company to cancel the charge.

Government grant scam. "Meg" kept receiving calls from individuals who claimed she had been awarded $5,000 in government grants. Meg knew she hadn't applied for a grant, so she asked her phone company to block the calls from the vishers.

New Medicare card scam. "Robert" received a call from an individual who claimed he was due to receive a new Medicare card and asked him to confirm his Medicare number. Knowing that his Medicare number was the same as his Social Security number, Robert refused to provide it to the individual and thwarted an attempt to steal his identity.

Tips to Avoid Being a Victim of Vishing

- When a caller claims to represent a specific company, ask for his or her name or employee number and call the company back using an independent and trusted source, like your billing statement or the phone book. Do not call the number provided by the caller.
- Avoid providing personal or financial information over the phone, especially if you did not initiate the call.
- If someone claims you owe a debt, remember that both state and federal laws provide you certain rights when you are contacted by a debt collector, including the right to receive written verification of the debt.
- Remember that in general, you cannot win a prize if you did not enter a contest.
- If you are not sure about the legitimacy of a call, tell the caller you need time to think things over. Ask a friend or family member for their perspective, or conduct your own research by contacting the Better Business Bureau at (651) 699-1111 or *www.bbb.org/minnesota.*
- Don't be afraid to hang up if something doesn't seem right. If it sounds "too good to be true," it probably is.
- Never give out your Social Security number or Medicare number to an unsolicited caller. The Center for Medicare and Medicaid Services and the Social Security Administration will not call you to update your information or give you a new card. And remember that your Medicare number is the same as your Social Security number!

How to Report Vishing

- Notify the company or agency being impersonated so it can alert others.
- Report the call to the Federal Communications Commission, which enforces laws regulating caller ID spoofing and unwanted telephone calls, at *www.fcc.gov/complaints* or (888) 225-5322.
- Report the call to the Federal Trade Commission, which enforces the National Do Not Call Registry and takes action against deceptive business practices, at *www.ftcccomplaintassistant.gov* or (877) 382-4357.

Remember that "vishers" are criminals and typically do not honor the "Do Not Call" list. These criminals are bent on stealing people's money and information (a crime) and are not dissuaded by the fact that a person's number is on the "no call" list. That being said, it is important to report vishing calls to the agencies listed above.

For additional information, contact the Office of Minnesota Attorney General Lori Swanson as follows:

Office of Minnesota Attorney General
Lori Swanson
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
TTY: (651) 297-7206 or (800) 366-4812
www.ag.state.mn.us