# Aging And The Threat Of Vishing

business customers risk management

**Summary:** Vishing, the fraudulent tactic of phone calling for personal information, is on the rise. Make sure your bank customers aren't fooled.

To get a better idea of when you might want to consider yourself getting old, look no further than a survey by Pew Research. It asked people this very question and ranking at the top were when you: turn 85 years old (79%), can't live independently (76%), can't drive a car (66%), turn 75 (62%) or frequently forget familiar names (51%). No matter your age, at least you now know a bit more about what others may be thinking, as you edge past certain mile markers in life.

In community banking too, certain mile markers should be more closely monitored than others perhaps. This is especially true when it comes to cyber thieves and phishing attempts. But, what about voice thieves and what is now known as vishing?

Dictionary.com defines vishing as *"the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers."*

Vishing (or voice-phishing) is simply the telephone version of phishing. But, it is not always as simple to detect. Here's a typical scenario. Unsuspecting individuals receive a phone call from a person or an automated message that leads them to a live person. They answer the call that appears to be from a familiar toll-free number associated with the person's bank or credit union. The scammer tells the customer there's been fraud detected on their account and asks them to confirm account details. Once the unsuspecting customer provides the information, the thieves are off to the races.

Even savvy customers can be fooled by scammer antics. Armed with just a little bit of personal information about the individual (which can be purchased), scammers can sound legit and usurp a treasure trove of secure information that can then be used to make off with people's money.

The problem isn't isolated or likely to go away soon. Data and mobile carrier company, First Orion predicts that by next year nearly 50% of all calls to mobile phones will be scams. Of those, the majority will use caller ID "spoofing" (person acts as though it were legit) such as the kind we just described.

To combat the problem, banks need to be aware and get even more defensive. This means warning customers as soon as you hear about a new scam designed to usurp personal information. It also means reaching out repeatedly to customers using bank signage, mailings, email and personal communications. Customers must be warned over and over that under no circumstances will bank representatives solicit personal information over the phone or through email.

Another step is to inform customers that if they are ever in doubt, the proper course is to hang up immediately, call the bank directly and speak to a manager. Customers should **never** use the contact number provide by anyone to confirm validity, but instead should use their own records and contacts. Banks should also encourage customers to ignore calls from unknown numbers.

Savvier thieves require stronger barriers. For this reason, community banks and customers need to work together to keep all security protections from aging too quickly perhaps.

## INTERNATIONAL SERVICES FOR COMMUNITY BANKS

Our international services are designed for community banks to help you capture more customers and fees. Contact us today for more information.