

New Vishing Spree Strikes U.S.

Fraudsters Targeting Mobile Devices, Smaller Communities

Featured on bankinfosecurity.com

In July, two phone-based phishing, or vishing attacks, hit residents in Provo, Utah. In August, 10 additional attacks were reported, incorporating a combination of vishing and text-message-based smishing scams, aimed at various communities scattered throughout the United States. The common factor: Perpetrators targeting customers of community banking institutions.

"Recently, we've seen them pop up in low-fraud, small places," hitting markets where consumers might not be so savvy or prepared for a socially engineered attack, says John Buzzard, who oversees client relations for FICO's Card Alert Service, which provides decision management and predictive analytics solutions for card issuers.

Vishing and smishing have replaced the traditional e-mail phishing attacks that were more prevalent three years ago, he says. Since January, the documented number of traditional e-mail or phishing attacks has significantly dropped. "What's replacing them are these new waves of text and person-to-person scams," Buzzard says, "and they're not being tracked."

Latest Spree

August's vishing and smishing schemes hit residents in Elgin, Ill.; Long Island, N.Y.; Binghamton, N.Y.; New York's Chautauqua and Cattaraugus counties; Bend, Ore.; Arkansas City, Ark.; Rocky Mount and Henry County, Va.; Auburn, Ala.; Texarkana, Texas; and Central Falls, R.I. Rather than being generic, in most cases, the calls and texts identified specific institutions by name.

In Elgin, residents received automated telephone calls from fraudsters claiming to be with KCT Credit Union and First Community Bank. In New York's Chautauqua and Cattaraugus counties, calls were posed coming from Cattaraugus County Bank and Mt. Vernon Money Management; in Binghamton, N.Y., it was Empower Federal Credit Union. In Arkansas, Union State Bank was targeted. In Virginia, Martinsville DuPont Credit Union was named; and in Auburn, Ala., Auburn University Federal Credit Union took the hit. The other attacks were not so targeted, either naming several institutions within a certain region or area code or, as was the case in Rhode Island, the calls came from individuals feigning to be travel agents who were giving away trips.

As e-mail spam filters have become more sophisticated, fraudsters have turned to other socially engineered methods that prey on consumers' trust. The common use of mobile devices makes smishing an easy scheme. SMS/text-based banking, which is quickly growing to become a mainstream mobile banking service, is helping to set the stage for smishing, says Ray Spreier, chief information officer for Mid Oregon Federal Credit Union. The Bend-based credit union, with \$140 million in assets, was one of the institutions targeted in August.

On Aug. 17, Mid Oregon FCU members reported receiving suspicious texts and phone calls from sources claiming to be with the credit union. Spreier says it was the first time Mid Oregon FCU had been specifically named in a vishing or smishing scam. Luckily, he points out, the credit union has focused attention on member education. "You will never receive an SMS message from us saying, 'Your card has been breached, call us.' Getting that word out has made a big difference."

Spreier says fewer than three of the credit union's 20,000 members responded to the calls and/or texts. "That education effort we have in place goes across multiple fronts, and we over-communicate it constantly," he says.

As more people sign on for text-based banking, Spreier says, fraudsters will be more likely to target it as a channel for fraud. "I think we can expect to see the look and the feel of these (text) attacks to get better, making it hard for the member to recognize the difference between what is coming from the credit union and what is not."

Fighting Back

Robert Siciliano, a McAfee security consultant and founder of IDTheftSecurity.com, says constant and consistent consumer education is the only effective way to fight vishing and smishing. "Consumers should not respond to any request that comes through on the phone to provide any information that could compromise their identity in any way," he says.

Vishing, because it hooks the consumer directly, through a landline or mobile phone, is hard for a financial institution to detect and control. "Vishing is a relatively low-tech crime," Siciliano says. But perpetrators of this type of crime are getting more organized than they've ever been before. In some cases, Siciliano says, fraudsters are getting actual phone lists of banking customers by means as simple as old-fashioned dumpster-diving. "To throw away a list of phone numbers in a dumpster can compromise your existing client base," he says Siciliano's advice:

- Understand all the ways in which fraudsters can compromise call centers via landlines and VoIP lines;
- Continually enhance consumer education efforts to keep up with the latest attacks;
- Ensure databases that store customer and member contact details are secure.

James Brooks, director of product management for Cyveillance Inc., which provides detection solutions that help institutions and business identify online compromises, agrees that phishing and vishing are evolving to target mobile devices. Educating consumers about secure mobile-use is the best way to fight back. Cyveillance works with the National Association of Federal Credit Unions and several of the NAFCU's member institutions.

As more consumers access e-mail via mobile browsers, it's much easier for fraudsters hit their phones with malware that's hidden in an e-mailed link," Brooks says. "Consumers are a little more trusting with their mobile phones when accessing information, even over email, than they are when it comes to accessing that same information on a PC," he says. "It's really more about user behavior than anything."