Personal Information Theft Using Text Messaging

SMISHING

consumer *brief*

WHAT IS SMISHING?

SMiShing (pronounced "Smishing") is an electronic threat targeting cell phone and mobile device users. Similar to email phishing scams, con artists use text messages in an attempt to get wireless customers to divulge personal or account information or to download malicious software.

The term SMiShing is derived from a combination of the term phishing and SMS (Short Message Service), which is the technology used for sending text messages.

In a typical SMiShing scam, wireless customers receive a text message requiring them to give immediate attention to the message and telling them to access a particular website or to call a specific phone number to address the problem. The message may appear to come from the customers' financial institution, utility company or other trusted source, and indicates that an account has been suspended, deactivated, locked, etc., and provides a phone number to call to reactivate it.

The danger is that unsuspecting customers may call the phone number in the text message and provide personal information such as an account number, Social Security number, user ID, password, and/or Personal Identification Number (PIN) to a person or to an automated service thinking that they are talking to their financial institution. In reality, this information is given to the perpetrator of the SMiShing scam and may be used to access their accounts or to open new ones in their name.

COMMON SIGNS TO LOOK OUT FOR

Although SMiShing messages are designed to be nearly impossible to distinguish from legitimate text messages, there are some common signs you can look for:

- An urgency for the customer to take immediate action;
- The mention of negative consequences if the customer does not act; and
- The lack of a telephone number showing the point of origin of the message.

DO NOT respond to any suspected message that may be a SMiShing scam. DO NOT text a response, DO NOT call the supplied phone number and DO NOT go to the listed website. Instead, contact the alleged source of the text message directly and inquire if an actual problem with your account really does exist.