

## SMiShing – The New Form of Phishing

SMiShing is a type of social engineering that uses cell phone text messages to persuade victims to provide personal information such as card number, CVV2, and PINs. The text messages may contain either a website address or more commonly, a phone number that connects to an automated voice response system, which then asks for personal information.

The following are examples of SMiShing messages:

- Text message originating from either [notice@abcbank.com](mailto:notice@abcbank.com) or [message@abcbank.com](mailto:message@abcbank.com):
  - ABC Bank has deactivated your debit card. To reactivate, contact 1.800.999.9999.
- This is an automated message from ABC Bank. Your debit card has been suspended. To reactive, call urgent at 1.800.999.9999.
- Text message originating from [sms.alert@visa.com](mailto:sms.alert@visa.com):
  - [Sms.alert@visa.com/VISA](mailto:Sms.alert@visa.com/VISA) Card Blocked Alert. For more information, please call 1.800.999.9999.

Although NBT may ask for personal information to confirm identification such as the account holder's name, security code words and/or last four digits of a social security number, you will never be asked for a CVV2 or a PIN either in person or via electronic methods.

If you become a victim of such phishing scam, NBT encourages you to call the phone number on the back of the card to have the card restricted.

