COLUMBIA COLLEGE
TECHNOLOGY SERVICES

Tuesday TechTip:

Vishing for information: Don't fall prey!
Vishing (short for voice phishing) is one of the newest forms of fraudulent activity to acquire sensitive information such as a credit card number, bank account number, and/or social security number using pirated recordings of telephone services from well-known financial institutions.

The message:
"Please notice that your VISA card is now disabled and you will not be able to use it. ... This is a security measure made by your bank. ..."

The message may come in the form of either an email or a telephone call. The message warns that your credit card has been used fraudulently, provides a toll-free number to call which then asks you to enter your 16 digit account number, and may even be asked to enter the security code (CVV) on the back of the credit card. Most recently, there is a new variation calling to confirm local bank account numbers.

How it works:
Using VOIP (Voice Over Internet Protocol) technology, criminals are able to create a phony automated customer service line, spoof the caller-id to display a specified "fake" toll-free number and leave a message. The setup looks real, sounds real, but very likely may not be real.

Protect Yourself

- Only the phone number on the back of your credit card or on your bank statement should be called with issues related to your credit/bank card.
- Be extremely cautious in providing a card's three digit CVV (Card Verification Value) code or bank account number to anyone.
- Question, verify, and ask to call the financial institution or credit-card company back at a number you are familiar with. A legitimate operation will understand.
- Be skeptical.

For additional tips, check out the Technology Solutions Center self-service portal at http://help.ccis.edu