



## **New Phishing Scam Sounds like Official Telephone Call**

*November 24, 2008*

With the holiday season approaching, shoppers increasingly use their credit and debit cards to make purchases at the mall, on the Internet, or over the telephone. When plastic card use increases this time of year, so do the scams.

A new twist on phishing aims to obtain the three-digit security code printed on the back of VISA and MasterCard credit and debit cards. The phishers are trying to get enough information to perform fraudulent card-not-present transactions (Internet, telephone, and mail-order purchases).

Under this scam, a telephone call is placed to a legitimate cardholder. The caller claims to be a representative from VISA or MasterCard informing the cardholder of suspicious card activity. The caller provides details of an unusual transaction and asks if the cardholder made this purchase, which, of course, the cardholder did not. The cardholder is then asked to verify possession of the card. To do so, the cardholder is asked to read the three-digit security code on the back of the card. The fraudster then provides a control number in the event the cardholder needs to call back with questions, making the call seem legitimate.

The caller does not ask for the credit or debit card number, and that is why some members are fooled into believing the call is legitimate. But the fraudster already has the card number; what they don't have is the three-digit security code from the back of the card, and that is what they are after with this scam.

The three-digit code on the back of the Visa or MasterCard card is a security tool used for non face-to-face transactions. When conducting transactions that are not face-to-face, many merchants will ask the shopper for the three-digit code to complete a card authorization. If the criminal obtains this three-digit number and already has your member's card number, card expiration date, and billing address, the criminal may be able to obtain authorization for fraudulent transactions.

Never give out the three-digit number on the back of your card to someone contacting you by telephone, Internet, or mail. This security tool is used when a card-not-present transaction is performed, and during the transaction the merchant may ask for the code to complete the authorization process. Be sure you are the person initiating the transaction.

Never respond to any email, telephone call, voice message, text message, or letter received through the mail that requests personal and financial information, including the three-digit number on the back of the card.