



United States Department of Justice Federal Bureau of Investigation

September 7, 2010

FBI, SPRINGFIELD DIVISION

<http://springfield.fbi.gov>

DEBIT CARD PHONE SCAM

A computer automated phone scam has impacted Central and Southern Illinois Bank customers. Debit card customers are receiving automated telephone calls stating their debit card account has been breached, and then told they will need to "reset" their information in order to use their account.

The "scam" works this way - The telephone rings, and the caller ID shows "not available" or "private number". An automated recording states "your debit card account has been breached. You need to reset your account by following these steps". The automated recording states to press "1" to begin.

By pressing "1" a computer system has been activated. The customer is then told to enter the sixteen digit card number, and the expiration date. The automated voice then asks for the three digit Customer Verification Value Code (CVV Code) located on the back of the card, followed by the four digit pin number. The perpetrators of the scam now have all the information they need to access the victim customer's debit card account.

It is important to remember not to give out personal information over the phone including passwords or pin numbers. Banks do not use an automated system to ask for this type of customer information regarding their accounts. Banks already have customer account information, and therefore do not need to ask for their information over the phone.

If you believe you have been contacted or unknowingly participated in this scam, you are urged to contact your bank immediately.

Brad Ware
Media Representative
Springfield FBI
(217) 757-3542
Bradley.ware@ic.fbi.gov