

# STATE OF NEBRASKA

---



Dave Heineman  
Governor

## DEPARTMENT OF BANKING AND FINANCE

**John Munn**

*Director*

Suite 400, Commerce Court  
1230 'O' Street  
Lincoln, Nebraska 68508-1402

**DATE: September 19, 2005**

**CONTACT:** Nora Tallmon, Public Information Officer

Kelly Lammers, Information Technology Review Examiner

**FOR IMMEDIATE RELEASE**

**PHONE: 402-471-2171**

####

### Skimming and Phishing Hits Alert Nebraskans

Due to citizen scrutiny and prompt response to authorities, the Nebraska Department of Banking and Finance (NDBF) was recently notified of unauthorized Automated Teller Machine (ATM) withdrawals posted to Nebraskans' accounts.

"Loss was minimized because a couple of Nebraskans took the time to closely examine their bank statements and reported the illegal withdrawals of their funds," said Kelly Lammers, NDBF Information Technology Review Examiner. "There are many ways criminals across the globe can get personal information that allows access to others' money, but a few simple precautions will usually keep your information and your money safe."

Lammers explained that an ATM requires the presentation of a debit or credit card and a Personal Identification Number (PIN). A PIN is similar to a signature. "I can't overstate the importance of never sharing your PIN number—the only people who know that number should be those you would trust with all of your money," he said.

According to Lammers, access to your money isn't always gained by obvious tactics. Criminals have conjured complex, new ways to con citizens out of personal information, including account and PIN numbers. Any time there is even a slight variation to your normal cash withdrawal or payment process you should be suspicious.

"One active scam is referred to as skimming. Skimming occurs when information from the plastic card is copied and used fraudulently by others," said Lammers. Automated skimmers may be placed or glued to the front of an ATM, usually covering the card slot only. They are small and often not easy to spot—look closely each time you visit your regular ATM, so you are very familiar with what it looks like.

During a skimming scam, cards pass through the illegal skimming device prior to going into the ATM. Be wary if you are instructed to swipe your card more than once at an ATM or checkout. A secondary concern—skimming gets the card numbers but not the PIN number—another collection process is necessary to get the PIN. Some criminals use concealed cameras, while others use two sets of key pads.

Another scam works as you pay for items at a store. When asked to enter your PIN number on a key pad as you pay, if the employee says that particular key pad isn't working and asks you to enter it again on a second key pad, be very wary. Report it immediately to store management, as well as to your financial service provider.

A second type of financial fraud is phishing. These types of fraud may occur in a survey on the street, over the telephone, in the mail or in e-mail. Regardless of the delivery method, citizens are asked for financial identifiers such as debit card or credit card numbers and the PINs. They rely on your trust, often impersonating fund raisers or bank employees. Use caution when providing payment or confirmation information to anyone, know who you are paying and investigate who you are giving information to before you do it. Never provide your PIN number. If, after a high pressure contact you realize you gave out financial identification information, contact your financial service provider immediately.

Lammers said, "Your best defense against fraud is awareness and diligence. Always promptly retrieve your mail, send outgoing mail that contains checks or credit card information at the Post Office, and make an inquiry anytime you receive mail at your address but not with your name. Always carefully examine your bank statement, notifying your bank immediately of any unauthorized activity. If you have online banking, check your account balance and activity frequently. The earlier crime is reported, the better chance of catching those that tried to steal from you."

Nebraskans are encouraged to contact NDBF or their financial institution if they have questions about this issue or any investing or banking matter. Call the NDBF Consumer Hotline toll free at (877) 471-3445, or visit online at [www.ndbf.org](http://www.ndbf.org).

####