ATM Skimming

What is ATM skimming?

- ATM skimming is identity theft for debit and credit cards. Fraudsters use hidden electronics, such as cameras, to steal the personal information stored on a card, and to record the owner's PIN number to access the hard-earned cash in a member's account.

How can you protect yourself from ATM skimming?

- Be vigilant and aware of your surroundings when utilizing an ATM. Be sure the ATM does not appear to have been tampered with. Be prepared to conduct your transaction when you approach the ATM. Have your card ready and know what transaction or transactions you want to conduct. If someone takes an interest in your transaction, then leave the area and report suspicious behavior to the police. When using a drive-through ATM, keep all doors locked and all windows up, except as needed.

Here are four tips to help prevent skimming and to keep you protected:

Protect Your PIN and Your Money

Hidden cameras are often used to steal your PIN. Covering the keyboard as you enter your PIN is a simple way to help avoid theft. Never give your PIN or account number to anyone, especially over the phone or over a cell phone. Always assume someone is watching. Choose a PIN that is unique. Do not choose an obvious number. Never write down your PIN, especially in your checkbook or on your cards. Remove your cash, receipt, and card after every transaction. Never leave receipts behind. Have any deposits prepared before you approach the ATM. Make sure the ATM envelope has been accepted. Secure any cash you withdraw before leaving the machine.

Stay Away from Unfamiliar ATMs

Check out the environment as you approach the ATM. The safest ATMs are those with the logo of your credit union. Lightly tug on the card reader to see if it is loose or moves around. Look for anything new on or immediately around the ATM. Do not use any ATM with a card reader that appears altered. Avoid facilities in dark or remote places. Avoid free standing ATMs on street corners. Avoid ATMs in areas where bystanders seem to be loitering rather than conducting business. If there is a perceived problem with the ATM, do not use it. Do not help anyone who says they may be affected by any such problem. Instead, leave the area and contact the police immediately as this person is most likely a fraudster who is attempting to obtain your card information, or to cause you financial harm.

Check Your Balances Frequently

Check your accounts daily and verify all transactions. Examine your statements promptly to identify unauthorized transactions. If you notice something wrong, then use the contact number on the back of your card to report any fraudulent activity.

Remember

All accounts at credit unions are insured. If you believe that your card and/or PIN has been lost, stolen, compromised, captured by an ATM, or that someone has transferred or may transfer money from your account without your permission, do not accept help from anyone who may offer it. Instead, leave the area. Contact your credit union immediately if you see any suspicious activity or unauthorized transactions and your credit union will assist you in canceling your card as needed.