Tips on detecting ATM/POS skimming devices

ATM/POS Skimming involves the attachment of electronic devices on or around the ATM/POS for the purposes of capturing both the magnetic strip data contained on the back of a debit card as well as the PIN number that is entered by the customer when using the ATM/POS. The devices used to capture the information will vary in shapes, sizes and designs but are made to be unobtrusive or mimic legitimate devices.

When using an ATM machine, people are advised to follow these suggested safe banking practices to reduce the risk of being a victim of skimming:

1. **Inspect the door access device prior to opening the lobby doors** (Most counterfeit devices are installed with double sided tape and are installed over the original door access device).
2. **Use a different card to open the lobby doors** (Most door access devices will open with many different cards that have magnetic stripes gift cards, store cards, credit cards, etc. all work to open the door.)
3. **Inspect the machine** for items that were installed over or around the PIN pad of the ATM. (Customers should be looking for an attachment on the ATM that contains a small PIN hole that is pointed in the direction of the PIN pad.)
4. **Lightly tug the area of the card slot**. (Most skimming devices are attached with double sided tape for quick removal by the crooks).
5. **Cover the keypad with you other hand** while typing your PIN. (This is the best way to ensure that your PIN number is not recorded by a PIN Capturing Device!)

    - When using a POS device, inspect the pin pad for any attachments where you swipe or insert your card. Also take the precaution and cover the key pad while typing in your PIN.
    - **It is strongly suggested to change your PIN every three months. This can be done at the Ste. Rose ATM or in branch at both locations.**

The following indicators may indicate ATM Skimming Activity is or has occurred at the location and should be reported to bank employees if the branch is open. If the bank is not open, the local police department should be notified:

1. Card slot of the ATM is loose or has fallen off, or other parts of the ATM machine have dislodged from the ATM.
2. The presence of double sided tape on the ATM machine or presence of glue or pry marks around the card slot of the ATM.
3. If the door access device at the lobby door has been removed or is not securely attached to the wall.
4. Observation of person(s) attaching or removing or tampering with parts of the ATM machine.
5. Subjects who are using the ATM and are intentionally covering their faces to avoid being depicted (ex. ski masks, hats, scarfs and sunglasses during nighttime use at the ATM).
6. Person(s) using multiple cards one after another in order to withdraw funds from an ATM (may be using counterfeit cards from a skimming incident).
7. Subjects spending long periods of time outside ATM machines and periodically inspect the machine but do not conduct transactions.
8. Police advise customers to not remove any of the skimming devices if detected, but are encouraged to contact the bank manager and local law enforcement.