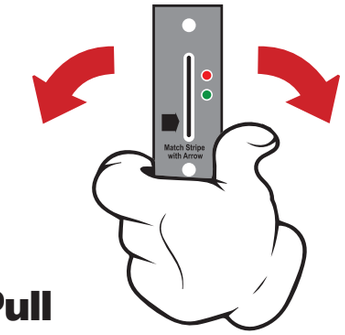
ATM Skimming

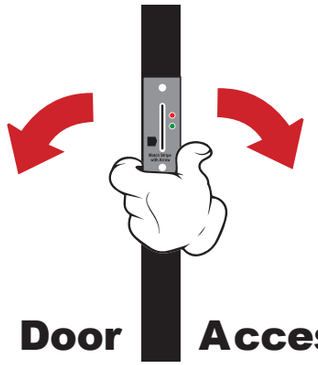
The Scam.

ATM “Skimming” occurs when a criminal attaches a specially designed card reading device (known as a Skimmer or Shimmer Device) over-top of, or inside of the 'real' card reader. While its most seen on ATM machines in a variety locations, these devices are increasingly found on gas station pumps. Most times, the skimming device looks identical to the real device; and is equipped with electronic recorders that will capture the financial information from your card. This data is later used by criminals in a variety of ways.



Pull

Devices are commonly attached with two sided tape or glue. By pulling or tugging on areas where the card must be swiped or inserted; you can often discover if a device is attached.



Door Access

Criminals can also affix these devices to the card reader at the entrance door to an ATM.

What You Can Do

Before Using

Pull / tug on the card reader. See anything seems loose or 'wrong.' Examine ATM machines, gas pumps, and other card readers before use. Do not insert your card if anything is loose, crooked, or damaged; if you notice scratches or marks; or see adhesive / tape residue.

Be Aware

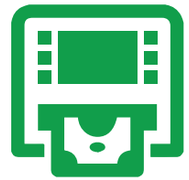
Be wary of ATM's in tourist areas, as well as remote locations - they are a popular target of criminals.

PIN Privacy

When entering your PIN, obscure or use your hand to cover the keypad - blocking the view of others; and preventing any hidden cameras from seeing your PIN.

Report It.

Immediately report any skimming devices to your financial institution and the local law enforcement by calling 911.



Cash Traps

Some criminals also use a device to accomplish "Cash Trapping." A device is attached to the cash dispensing portion of an ATM, whereby the dispensed cash is "trapped." When the customer leaves the machine, the criminal then removes the cash from the trap.

TSE
www.TSEonline.org