What is card skimming?

ATM skimmers place an electronic device on an ATM that steals information from a credit or debit card's magnetic strip whenever a customer uses that machine. The devices placed on ATMs are usually undetectable by users because they blend right into the ATMs façade. The device used is often a realistic-looking card reader placed over the factory-installed card reader. Customers then insert their ATM card into the phony reader, and their account info is swiped and stored on a small attached laptop or cell phone, or sent wirelessly to the criminals waiting nearby.

Skimming also involves the use of a hidden camera, installed on or near an ATM, to record customers' entry of their PINs into the ATMs keypad. Criminals have also been known to attach a fake keypad on top of the real keypad, which then records every keystroke as customers enter their PIN.

It's also important to note card skimming can happen anywhere – ATMs, gas pumps, retail merchants and restaurants, so it's important to be on the lookout at all times!

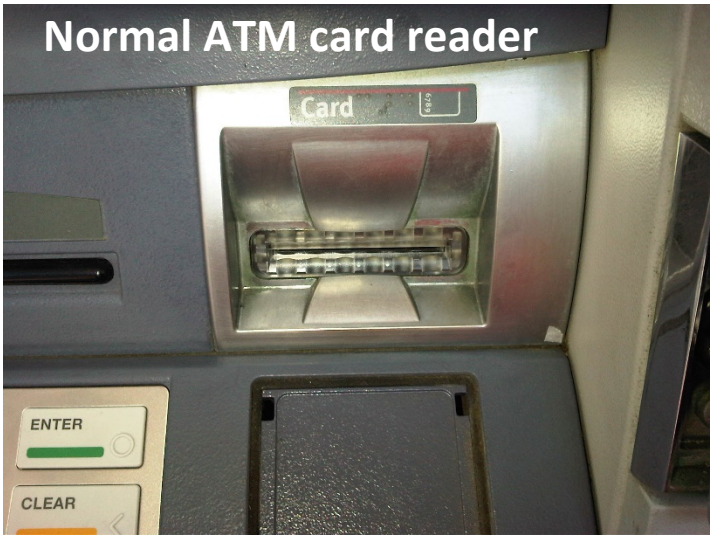
How can you avoid becoming a victim?

Since card skimming at ATMs and gas pumps are becoming the most common places for skimming to occur, here are a few tips to help prevent becoming a card skimming victim:

1. Inspect the ATM, gas pump or credit card reader before using it. Be suspicious if you see anything loose, crooked or damaged, or if you notice scratches or adhesive/tape residue.
2. When entering your PIN, block the keypad with your other hand to prevent possible hidden cameras from recording your number.
3. If possible, use an ATM at an inside location. These ATMs have less access for criminals to install skimmers.
4. Be careful of ATMs in tourist areas – they are a popular target of skimmers.
5. If your card isn't returned after the transaction or after hitting "cancel", immediately contact the financial institution that issued the card.

Source: https://www.fbi.gov/news/stories/2011/july/atm_071411

Below are some images to help you identify fraudulent card readers:



ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera

A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is "skimmed," or stolen, and usually stored on some type of electronic device.

3 Keypad overlay

The use of a keypad overlay—placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.

Source: https://www.fbi.gov/news/stories/2011/july/atm_071411