What are credit card skimmers? (www.ksdk.com)

A skimmer is a device designed to steal credit card information by "skimming" the magnetic strips on cards swiped at ATMs or gas stations. They're often attached to the credit card slot on a gas pump or ATM, and sometimes they come complete with a camera that'll capture you punching in your personal Identification Number, or PIN.

Overlay skimmers

An overlay skimmer is one that fits over the card reader slot of an ATM or gas pump.

The skimmer is usually modeled, or in some cases 3-D printed, to look like the part it's covering. However, it might not be the same quality or color as the rest of the machine. Maybe it's protruding a bit too far or isn't installed straight. If it looks like it doesn't quite fit or is loose, then that's a possible warning.

You can also look around for additions to the machine that could hide a camera pointed at the keypad. This is often how crooks get your PIN. It might be installed on the ATM, or even on the wall above it. Hackers have hidden cameras in fake outlets, lights and other things that wouldn't immediately catch your attention.

For these types of skimmers, it's actually fairly easy to defeat them. Simply cover your hand when you're typing in your PIN and the crooks won't have all the information they need to clone your card.

Advanced skimmers

Unfortunately for us, hackers quickly spotted the weaknesses of skimmers and have come up with options that are more difficult to detect. Some are actually impossible for you to catch.

A good example comes from Brazil. It's an overlay skimmer, but instead of overlaying the card reader, the entire front of the ATM is fake.

The gas station thieves hid their skimmers inside the pumps. The skimmers were even equipped with Bluetooth so the thieves could drive by and extract the collected numbers and PIINs wirelessly.

Another type of skimmer is thin enough that it fits right inside the ATM or gas pump's card reader slot. There's no external sign it's there.

Unscrupulous employees of a restaurant or store might have handheld skimmers that you'll never see. Or, they might put out POS terminals that are really skimmers in disguise; and they'll even print out a receipt.

Anything look out of the ordinary?
Take a second at a gas pump or ATM and observe your surroundings-does the credit card slot or PIN pad look loose or out of place? Skimmers can be placed on top of the real credit card machine or inside the credit card slot. Try tugging at the payment terminal, sometimes skimmers come right off.

Check the other gas pump payment terminals-do they look like the one you're using? Do a quick scan for anything that looks like a camera pointing at the pump or PIN pad.

Protect your PIN, if you use it at all
It's best not to use your debit card with your POIN number at a gas pump if you can help it. If you must, cover the pad with your other hand while you punch in the digits, or simply pay inside. Fraudsters are less likely to tamper with a payment terminal at a clerk's counter.

Use bank ATMs, or those in well lit, busy areas
While skimmers have been found on bank lobby ATMs as well, it's less common. Thieves often target stations or ATMs that are off the main drag, or in badly lit areas.

Use a chipped card or other payment options
Almost everyone has a chipped, or "EMV" card nowadays, and having one significantly decreases your chances of getting skimmed, because the data on the card is constantly changing and is difficult to extract. Bad new, Hackers get smarter all the time and some point-of-sale terminals aren't updated to allow the use of EMV cards. While not 100 percent fail-proof, using an EMV card makes it much harder to steal your personal information.

Keep an eye on your accounts
In any circumstance, it helps to watch your bank accounts for any odd or unusually large charges.

Gas pump and ATM skimmers: How to spot and avoid them- (www.CreditCards.com)

1. ***Use your eyes: Look before you insert your card.***

Before you slide your card in a fuel pump or ATM, take a good look at the keyboard and card reader.

Bad guys can use 3-D printer to create a new keyboard to put on top of the real one. The keyboard might look different from the rest of the ATM, or the keys could look bigger.

With fuel pumps, is the seal broken? To place a skimmer inside a fuel pump, fraudsters must open the fuel dispenser door to insert the skimmer.

Station employees may place serial-numbered security tape across the dispenser door, so check to see if the tape has been broken. If there's no tape, check to see if the dispenser door looks as though it has been forced open.

Also, look inside the throat of the card reader to see if you can spot anything hidden there. A skimmer inside a gas pump or ATM can steal the information off the magnetic stripe of your credit card or debit card.

2. ***Use your fingers: If something doesn't feel right, move on.***

Wiggle the ATM card reader to see if it's loose. The crooks might place a card reader on top of the existing one.

You should also be wary if it's hard to insert your credit card or debit card.

3. ***Use your phone: Apps now can alert you to possible skimmers.***

A free Skimmer Scanner Android app (https://play.google.com/store/apps/details?id=skimmerscammer,skimmerscammer) released in September 2017 scans for available Bluetooth connections looking for a device with title HC-05.

If your smart phone detects a skimmer, use a different pump or go to a different gas station.

4. ***Use your common sense: Use fuel pumps and ATMs in safe places.***

Avoid gas pumps that are out of sight of the clerk and ATMs in areas with little traffic.

It's particularly important to be cautious at nonbank ATMs, such as those located at convenience stores or nightclubs.

Nonbank ATMs accounted for the majority of compromised devices in 2016.

At banks, on the other hand, security is tighter, with cameras recording transactions and more people coming and going.

At ATMs, always cover the keyboard when you type your PIN. There might be a new cardboard box containing literature next to the ATM, which crooks set up to conceal a pinhole camera. They use the camera to record you as you key in your PIN.