

How to Avoid Credit Card Skimmers

Think Twice Before You Swipe

By Andy O'Donnell, About.com Guide

You rarely let your credit card out of your sight, so how do bad guys get your credit card information? Some may get it from a friend waiting tables at a restaurant, but many credit card thieves get your card info using a device called a credit card skimmer.

A credit card skimmer is a portable capture device that is attached in front of or on top of the legitimate scanner. The skimmer passively records the card data as you insert your credit card into the real scanner.

Credit card thieves will often temporarily affix the card skimmer device to gas pumps, ATMs, or other convenient self-service, point-of-sale terminals. The bad guys like gas pumps and ATMs because they are easy to retrieve their skimmers from and they generally receive a lot of traffic.

Skimmer technology has become cheaper and more sophisticated over the years. Some skimmers capture the card information using a magnetic reader and use a miniature camera to record you typing in your PIN number. Some skimmers will even go so far as to place a secondary keypad over top of the actual keypad. The secondary keypad captures your PIN number and records it while passing your input to the real keypad.

How can you detect and avoid having your credit card skimmed at the ATM or gas pump?

1. Inspect the card reader and the area near the

PIN pad

Many banks and merchants realize that skimming is on the rise and will often post a picture of what the real device is supposed to look like so you will see that there is something attached that is not supposed to be there if a skimmer is present. Of course, a card skimmer could put a fake picture over the real picture so this isn't a fail-safe way to spot a skimmer.

Most skimming devices are designed to be temporarily affixed to the ATM or gas pump so they can be easily retrieved by the bad guys once they've collected a batch of cardholder data.

If you think the scanning device doesn't look like it matches the machine's color and style, it might be a skimmer.

2. Look at other nearby gas pumps or ATMs card

readers to see if they match the one you are using.

Unless skimmers are running a large operation, they probably are only skimming at one gas pump at a time at the station you are using. Look at the pump next to yours to see if the card reader and setup look different. If they do then you might have just spotted a skimmer.

3. Trust your instincts. If in doubt, use another machine somewhere else.

Our brains are excellent at recognizing things that seem out of place. If you get a sense that something looks off about the ATM you are about to use, you might be better off using one that you feel more comfortable with.

4. Avoid using your PIN number at the gas pump.

When you pay at the pump with your debit/credit card, you usually have the option to use it as a credit or a debit card. It's best to choose the credit option that allows you to avoid entering your PIN in sight of a card skimmer camera. Even if there is not a card skimmer camera in sight someone could be watching you enter your PIN and could subsequently mug you and take your card to the nearest ATM to withdraw some cash.

When you use it as a credit card you usually only have to enter your billing ZIP code as verification which is much safer than putting in your PIN.

5. Keep an eye on your accounts

If you suspect that you might have had your card skimmed. Keep an eye on your account balance and report any suspicious activity immediately.