ATM Skimmers Explained: How to Protect Your ATM Card

An “ATM skimmer” is a malicious device criminals attach to an ATM. When you use an ATM that’s been compromised in such a way, the skimmer will create a copy of your card and capture your PIN.

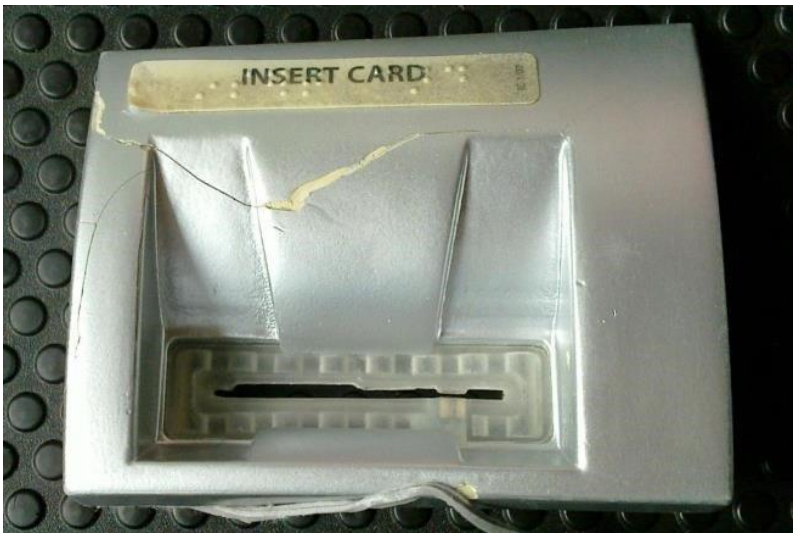
If you use ATMs, you should be aware of these attacks. It’s often possible to spot ATM skimmers, or at least to protect your PIN so ATM skimmers won’t be able to capture it.

How ATM Skimmers Work

An ATM skimmer has two components. The first is a small device that’s generally inserted over the ATM card slot. When you insert your ATM card, the device creates a copy of the data on the magnetic strip of your card. The card passes through the device and enters the machine, so everything will appear to be functioning normally –but your card data has just been copied.

The second part of the device is a camera. A small camera is placed somewhere it can see the keypad — perhaps at the top of the ATM’s screen, just above the number pad, or to the side of the pad. The camera is pointed at the keypad and it captures you entering your PIN. The ATM appears to be functioning normally, but the attackers just copied your card’s magnetic strip and your PIN.

The attackers can use this data to program a bogus ATM card with the magnetic strip data and use it in ATM machines, entering your PIN and withdrawing money from your bank accounts.



ATM skimmers are becoming more and more sophisticated. Instead of a device fitted over a card slot, a skimmer may be a small, unnoticeable device inserted into the card slot itself.

Instead of a camera pointed at the keypad, the attackers may be using an overlay — a fake keyboard fitted over the real keypad. When you press a button on the fake keypad, it logs the button you pressed and presses the real button underneath. These are harder to detect. Unlike a camera, they're also guaranteed to capture your PIN.

ATM skimmers generally store the data they capture on the device itself. The criminals have to come back and retrieve the skimmer to get the data it's captured. However, more ATM skimmers are now transmitting this data wirelessly over Bluetooth or even cellular data connections.

How to Spot ATM Skimmers

Here are some tricks for spotting ATM skimmers. You can't spot every ATM skimmer, but it won't hurt to take a quick look around before withdrawing money.

- **Jiggle the Card Reader**: If the card reader moves around when you try to jiggle it with your hand, something probably isn't right. A real card reader should be attached to the ATM so well that it won't move around — a skimmer overlaid over the card reader may move around.
- **Look at the ATM Machine**: Take a quick look at the ATM machine. Does anything look a bit out-of-place? Perhaps the bottom panel is a different color from the rest of the machine because it's a fake piece of plastic placed over the real bottom panel and the keypad. Perhaps there's an odd-looking object that contains a camera.
- **Examine the Keypad**: Does the keypad look a bit too thick, or different from how it usually looks if you've used the machine before? It may be an overlay over the real keypad.
- **Check for Cameras**: Consider where an attacker might hide a camera — somewhere above the screen or keypad, or even in the brochure holder on the machine.

If you find something seriously wrong — a card reader that moves, a hidden camera, or a keypad overlay — be sure to alert the bank or business in charge of the ATM. If something just doesn't seem right with the machine, go find another ATM machine.

Basic Security Precautions

You can find common, cheap ATM skimmers with tricks like attempting to jiggle the card reader. But here's what you should always do to protect yourself when using any ATM machine:

- **Shield Your PIN With Your Hand**: When you type your PIN into an ATM machine, shield the PIN pad with your hand. Yes, this won't protect you against the most sophisticated skimmers that use keypad overlays, but you're much more likely to run into an ATM skimmer that uses a camera — they're much cheaper for criminals to purchase. This is the number one tip you can use to protect yourself.
- **Monitor Your Bank Account Transactions**: You should regularly check your bank accounts and credit card accounts online. Check for suspicious transactions and notify your bank as quickly as possible. You want to catch these problems as soon as possible — don't wait until your bank mails you a printed statement a month after money has been withdrawn from your account by a criminal. Tools like Mint.com — or an alert system your bank might offer — can also help here, notifying you when unusual transactions take place.