

The Ins & Outs of Skimming Scams

With a small device called a skimmer, fraudsters can quickly read a card's information and use it to access your account fraudulently. Your card's information gets stored so that criminals can easily get to it later.

Skimmers may be installed on ATMs, as well as gas pumps and other credit card readers, and sometimes, you can't even notice them. A small device goes over the normal card reading slot and reads your card's magnetic stripe.



Here are a few tricks to help you avoid getting caught in a skimming scam:



- **Cover the ATM keypad** as you're entering your PIN—just in case there's a hidden camera around.
- **If something looks suspicious, find another ATM**—skimming devices will stick out a few extra inches from an ATM. Don't fall for a poor fitting device (or a sticker or sign that says "Swipe Here First," or "Use This Machine Only").
- **Call the financial institution**—report it immediately if a machine keeps your card.
- **Don't accept "help" from anybody hanging around the ATM**—they may say they were also having trouble and you just need to enter your PIN again.

Article courtesy of about.com

