Avoid becoming a victim of ATM Skimming

What is ATM skimming? For those who might not already know, it essentially involves a card-reading device placed over the real card slot on an ATM.

This device captures account information from the card. Meanwhile, the victim's PIN is captured, either with a small camera hidden on the machine or with a keypad overlay that can be removed later.

The criminal creates new card using blank plastic card stock (even gift cards that haven't been activated), which are then used to drain victims' accounts. All of these devices can blend in extremely well with the real ATM hardware and can be hard to detect.

So, how do you avoid ATM skimming? First, only use ATMs in well-lit areas, and that have security cameras installed. The machine outside a financial institution with a camera and a bank of floodlights is going to be a lot harder to retrofit than the one at the corner of a poorly lit parking lot.

Second, pay attention. Put the phone down when you're at the ATM. For one thing, you need to be alert for suspicious devices. For another, it's always a good idea to be alert to your surroundings any time you're handling a wad of cash in public (for your physical safety). You can't do either with a cell phone on your ear.

Before you even take out your card, check the machine and everything around it. Look for parts that seem crooked, or decals that are partially covered. This is just one possible sign of skimming. A reader that's a different color than the rest of the machine can also be a clue. However, some of these devices are small enough to only cover the slot itself. A lot of machines have lights around the slot; if these are not visible, it could mean a device has been attached. Basically, if something doesn't seem right, find a different machine.

Also, check out any brochure racks or other items on or near the ATM. Cameras can be hidden just about anywhere these days. As an extra precaution, when you're entering your PIN, cover your hand with your other hand.

Try jiggling the machine a little before inserting your card. Give the card slot a little tug to make sure there isn't any "bonus hardware". Don't attempt to rip the reader out of the machine. Just give it a little push to make sure it's part of the machine.

These devices are usually held loosely in place with glue or tape, as the thief must remove them later. Give the keypad a once-over. If it sticks out to far or looks strange, it could be a warning sign.

If you do this, and a skimmer detaches itself from the machine, either contact the financial institution (if it's nearby) or the police. Whatever you do, don't just throw it away or keep it. That would tend to make it look like you're the one running the scheme.

Skimming devices have also shown up on gas pumps as well as ATMs. If you are going to use your debit card for gas, make sure to look before you swipe.

Gas pumps are an easy place to stick a skimmer because card readers in this case vary from station to station, and many of them look like they're about to fall apart anyway. It's hard to tell what's legit and what isn't.

A few precautions and being alert while using an ATM can keep your information safe and guarded.

So the next time you visit an ATM, think about ATM skimming and beware so that no fraudster can take advantage of you.

Hercules Police Department
111 Civic Drive
Hercules, CA 94547
510-799-8260 (Office)
510-724-1111 (Dispatch)