Security Tips: Detecting ATM Skimming Devices

ATM/POS Skimming involves the attachment of electronic devices on or around the ATM/POS for the purposes of capturing both the magnetic strip data contained on the back of a debit card as well as the PIN number that is entered by the customer when using the terminal. The devices used to capture the information will vary in shapes, sizes and designs but are made to be unobtrusive or mimic legitimate devices.

When using an ATM machine, people are advised to follow these suggested safe banking practices to reduce the risk of being a victim of skimming:

Know What to Look For

Skimmers are small electronic devices that fit over the slot you swipe (or push) your debit and credit cards into, which steal your card details. If anything seems out of place on the machine, unusually bulky, or poorly affixed to the machine, gently tug on it. If it moves or comes away from the ATM, it may be a skimming device. Check for scratching around the card slot, adhesive tape or glue residue, and if the device can be removed. If you believe a device is installed, you should alert bank staff at 877-487-2977 during business hours. After hours please contact the local police Department. Do not attempt to remove the device.

Look for Hidden Cameras

Skimming is a two-step process because criminals can also obtain your PIN. This is often done with a pinhole camera hidden on or near an ATM. Look for anything that may have a tiny hole or slot for a camera to be placed inside, especially if it is aimed at the keypad. These devices may be stuck to the top or side of the machine or placed inside light fixtures above it. They are also likely to be temporarily affixed, so check any unusual components to see if they move or seem poorly applied. Many ATMs will also have security cameras attached to them, and these are usually much more obvious and permanent.

Check the Keypad

Some criminals have also used keypad overlays instead of cameras to capture customers' PINs. These devices record keystrokes electronically, so check for anything that seems to have been placed over the top of the keypad that moves, seems unusual, or does not match the ATM.

Protect Your PIN

Always use your hand to shield your PIN as you enter it and be aware of anyone standing too close who may be attempting to watch. Never write down your PIN down; memorize it.

bankprov.com Copyright © 2022 BankProv. All rights reserved. Member FDIC • Member DIF

Know Your Surroundings

Machines with many customers, especially in tourist areas, are the most likely to be targeted by criminals. Look for an ATM that is inside a bank or within the sight of a security camera, where scammers would be less likely to take a risk. Be wary of anyone loitering by machines, especially when using an ATM, and do not let strangers help you with supposedly "broken" machines. It is not just ATMs that can be compromised, gas stations that allow customers to pay at the pump are also at risk. Scammers have been especially active on holiday weekends and have often been targeting machines on the outside of bank branches.

The Federal Trade Commission (FTC) has more advice on how to stay safe on vacation: consumer.ftc.gov/blog/scam-free-vacation

Check Your Statements Regularly

It is important to check your statements and accounts regularly to detect fraudulent transactions. If you do not already use online banking, it is worth considering. Being able to quickly access and search through your statements could help you to identify these transactions and allow you to report them much sooner.

To set-up your Online Banking relationship, visit bankprov.com.

bankprov.com Copyright © 2022 BankProv. All rights reserved. Member FDIC • Member DIF