U.S. Department of State
Overseas Security Advisory Council

The Overseas Traveler's Guide To: ATM Skimmers & Fraud

August 2016

The ATM Attraction

A ubiquitous and easy target for criminals

Automated teller machines (ATMs) are commonly the first stop a traveler must make after arriving at an overseas destination, dispensing the local currency necessary for taxis, restaurants, and other business transactions. While these machines are vital to foreign travel, they are also highly exploited. Criminal actors view ATMs as an easy, unattended, and profitable target.

98 percent of losses from ATMs in 2015 were the result of skimming devices deviously installed on the cash machines to facilitate theft. These losses totaled over USD $2 billion – a number that is expected to continuously rise as skimmers become increasingly sophisticated. The majority of compromised machines are non-bank ATMs, that is, they are located in a convenience store, strip mall, or other public sites with heavy traffic but arguably less monitoring. For similar reasons, the majority of skimming attacks take place during weekend hours; when banks are closed but customers are frequent.

Criminals use a variety of tactics in their skimming operations. Skimmers can consist of hardware that is directly installed over the card reader and pin pad of the ATM, to pinhole cameras that record user activity, to malware that compromises the machine's digital interface. All of these malicious tactics enable criminals to record customer's account information and PINs, which are subsequently used to duplicate bank cards and steal money from victim's accounts.

OSAC constituents have previously reported falling victim to ATM skimmers. The best defense against ATM skimmers is awareness of criminal tactics, in order to avoid potentially compromised ATMs. Some reputable institutions – i.e. banks or hotels – provide users with a step-by-step tutorial to check the physical parts of the ATM for tampering before ever inserting their bank card. This OSAC guide also aims to inform constituents of commonly used tactics in an effort to avoid becoming a victim of a skimmer while on overseas travel.

Anatomy of an ATM Skimmer

How criminals grab your data

1. Hidden Camera

PINS are essential to skimming operations, and often captured by pinhole cameras installed on or around the ATM. These cameras are made to look like a legitimate part of the machine, and are often extremely difficult to detect. Verizon's 2016 Data Breach Investigations Report found that in over 90 percent of observed skimming breaches used a tiny hidden camera to steal the PIN.

2. Skimmer

Criminals affix a fraudulent card reader on top of the legitimate card reader to grab data from a card's magnetic strip. Over time, skimmers have been redesigned to evade detection, sometimes fitting snugly inside the card slot. Some of these "deep insert skimmers" are placed behind the shutter of the motorized card reader and completely hidden from the user.

3. Keypad Overlay

Keypad overlays are dummy look-a-likes placed over the original keyboard. Much like hidden cameras, these overlays are also used in an effort to record the user's PIN data. Overlays send a user's keystrokes to the real ATM, to ensure legitimacy of the transaction, but also records the keystrokes in the digital circuitry to be recalled and exploited by criminals at a later date.

Source: FBI

The Problem Persists

The Evolution of ATM Skimmers

Fake ATM Terminals

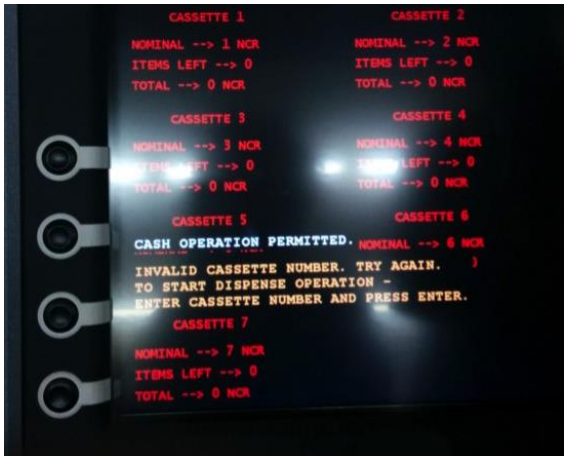
Seen in Brazil, a phony look-alike ATM was fitted directly on top of a legitimate cash dispenser. Victims inserted their cards into the fraudulent machines and entered their PINs, only to be left with repeatedly failed transactions. Instead of using a pin pad overlay or a skimming device that may show evidence of tampering, the completely fraudulent terminal enabled criminals to collect card data and PINs for fraudulent use.

Compromised Entry to an ATM

Although some ATMs are seemingly secure by requiring the user to swipe their card on a door to gain access to the machine, this also makes for an added easy target for criminals. Skimmers can be placed over the door's key card lock, and a camera can be hidden around the vicinity of the ATM. This makes for easy theft of card data and PIN numbers without tampering with the actual machine.

ATM Malware

Software-based attacks on ATMs continue to evolve in sophistication. The use of malware also enables criminals to steal card information with physical altering the ATM. Often, criminals infect terminals by uploading malware from USB devices or via a bank's internal network. ATM malware makes wads of cash available to criminals in one withdrawal, or allows them to intercept data from the machines, with a focus on customer bank account numbers and PINs.



Source: Krebs on Security

Best Practices

Protect your card information

- Use an ATM located inside of a bank branch, or hotel lobby rather than one located on the street.
- Be aware of the ATM's surroundings and any possible loiterers.
- Do not accept help from strangers when using an ATM.
- Do not use ATM machines that show possible signs of tampering.
- Inspect the machine for items that may have been installed over or around the PIN pad. Avoid ATMs with attachments pointed in the direction of the PIN pad. This may be used to house a camera and record your PIN.
- Lightly pull the card slot. Signs of tampering include a loose or detached card slot, or the presence of double-sided tape (used by many "skimmers" to ensure quick and easy removal).
- Use your free hand to guard your PIN while entering it on a keypad to prevent recording by pinhole cameras.
- If the credit or debit card is retained in an ATM, press the "Cancel" button to terminate the operation and contact the bank immediately.

Other Guides and Resources:

PC Magazine's: How to Spot and Avoid Credit Card Skimmers

Krebs on Security: All About Skimmers

FBI: Beware of Skimmers

Commonwealth Bank of Australia: ATM Card Skimming & PIN Capturing Customer Awareness Guide

U.S. Department of State
Overseas Security Advisory Council

CONTACT US:

Cyber & Information security:
osaccyber@state.gov

Middle East & north Africa:
osacnea@state.gov

East Asia & Pacific:
osaceap@state.gov

Europe & Eurasia:
osaceur@state.gov

South & central Asia:
osacsca@state.gov

Disease & Pandemic Outbreak:
osachealth@state.gov

Western hemisphere:
osacwha@state.gov

Africa:
osacaf@state.gov