Credit Card Skimmers

Credit Card Fraud

- Credit card and debit card fraud resulted in losses amounting to \$16.31 billion during 2014. (\$15 billion in 2015 from 13.1 million users) (Source: Nilson Report, July 2015)
- Report from Barclays states 47% of the world's credit card fraud happens in the United States, even though Americans only account for 24% of the total credit card volume.

In 2015 the U.S. had 780 data breaches with 177,866,236 pieces of data stolen

http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

How Thieves Steal Credit Cards

- ► Malicious software installed on point-of-sale devices remotely
 - ▶ This is the most common source of theft
- Network compromise at a company that processes transactions between credit card issuing banks and merchant banks
 - This is rare
- Hacked point-of-sale service company/vendor
- Hacked online merchant
- Crooked employee (hand held skimmer)
 - https://www.youtube.com/watch?v=oAP7sVh4sm
- ATM/Gas Pump skimmer
- Lost or stolen credit card

How Credit Card Readers Work

- Card is swiped, and mag strip electronically read
- Keyboard may or may not be used for security code
- Data is transferred from card reader and keypad to small board behind card reader
- Data then transferred via ribbon cable or wires to larger board which communicates with console and operates dispenser
- Data verified through credit card system at console and pump authorized
- As long as signal gets successfully to console, no way to suspect that data is being stolen

Magnetic Strip Information

- Mag strip contains 3 tracks (only 2 of 3 are used)
 - Both Track 1 and 2 contain enough basic information for processing payment card swipes. Most card readers will be able to read both Track 1 and Track 2 data, in case one of the tracks has become unreadable
- Track 1 contains 79 characters, Track 2 40 characters
- Data included: type of card, card #, name of card holder, expiration date, service code (types of charges that can be accepted, and discretionary data digits (pin #s or card codes)
 - ► No address or social security number

How Credit Card Skimmers Work

Two Types

- External Skimmer: Fits overs the outside of a card reader and reads the credit card information even before real card reader does. Used on ATMs or devices where it is hard to access interior of device
 - Easier to install
- Internal Skimmer: Reads the signal between the card reader and the main board. It copies the information but does not stop it reaching the board. Most common on gas pumps with easy access to the inside
 - ► Rare on ATM's
 - Can't detect without opening the cabinet

- ▶ Both types store stolen information.
- Both types may also transmit the information via Bluetooth so that the device never has to be removed



What happens to the data?

- Sold (Dark net markets like Alphabay, Valhalla, Dream Market, etc.)
- Used for online transactions (Currently about 40% of fraudulent credit card transactions. With EMV in use in Europe, the number has risen significantly and is expected to in the U. S. once EMV transition is complete. Estimates put it rising from the current \$9 billion to \$19 billion in 2018)
- Copied to fake cards using the same technology that makes hotel room keys; used to buy legitimate gift cards (name on card matches person's id but name on receipt is different)

External Skimmers

- Slide over the outside of the existing skimmer
- Are self-contained, no wires or connections to any other components
- Read the card and store the information without affecting real card reader.
- Can be quickly installed & removed without detection.







How to Detect External Skimmers

- Look for card readers that protrude more than the rest or look slightly different (does everything line up correctly, are all the lights lit, etc.)
- "Wiggle" card readers; loose external readers may actually pull right off.

Something else to keep in mind

https://www.youtube.com/watch?v=5b1axnNK-wl



Internal Skimmers

- Installation requires access to inner cabinet. Most model dispensers have common keys which are available to virtually anyone who wants them.
- Dispenser locks not very sturdy, designed to keep out the curious not the criminal
- Tangle of wires inside can camouflage skimmers from the untrained eye









How to Detect Internal Skimmers

- Check the board behind the credit card reader to see that there is nothing attached to the underside of the 7 pin connector or between the 7 pin connector and the ribbon tape.
- ▶ Look for loose or missing screws that show board has been replaced
- Do the same thing at the board which controls the pump's operation.
- Check the connection from the board on the card reader all the way to the board that controls the operation of the pump. Ribbon (or wires) should be unbroken from one connection to the other
 - Check if the ribbon or wires are different
- ▶ No objects along the ribbon
- Only one ribbon coming from the board



Other Common Devices

- ► Heaters
 - 2 wires only-do not connect to 7 pin connector



Battery in case of power outage

Chip Technology Protects

- Encrypted live communication between credit card company and card at retail location Random code exchanged to verify this is a legitimate card
- Even if card number is stolen, no ability to generate the new random code.
- Card is still vulnerable if used online or swiped at a reader which doesn't have chip technology









Ways to Deter and Detect before Chip Technology Installed

- Change the locks on Dispensers to Unique keys
- Control who has access to dispenser keys
- ► Install Security Seals
- ► Contact your service company:
 - ▶ Find out if your card readers can be encrypted
 - Power down if cable to card reader is interrupted
 - Shields installed to prevent access to boards
 - Alarm if cabinet door is opened

Security Seals

- Personalized
- Serialized
- Void if tampered with
- Place it strategically over opening to access boards (not on hinge side!)
- Over outside of scanner
- Checked daily (or even every shift), and don't have it be the same person every time
- Keep a log
- Checked after contractors











Monitoring is Forever

- ▶ Skimmers can be installed anytime
- ► Train ALL employees
- Serial numbers tracked on security seals
- Conduct daily inspections
 - Ability to detect if daily inspection not done
 - Consequences if daily inspection not done





















Credit Card Shimmers

From Krebs on Security (<u>https://krebsonsecurity.com/2017/01/atmshimmers-target-chip-based-cards/</u>)

- ► Targets chip-based credit and debit cards
- It acts a shim that sits between the chip on the card and the chip reader in the ATM or point-of-sale device — recording the data on the chip as it is read by the underlying machine
- Data collected by shimmers cannot be used to fabricate a chipbased card, but it could be used to clone a magnetic stripe card
- The chip contains an additional security components not found on a magnetic stripe

Credit Card Shimmers

- The reason shimmers exist at all is that some banks have apparently not correctly implemented the chip card standard
- The only way for this attack to be successful is if a card issuer neglects to check the CVV when authorizing a transaction

Credit Card Shimmers



Credit Card Shimmers



Credit Card Shimmers



One Last Question to Think About

How many of you check your car wash?