International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1838100

Rising Cyber Fraud through Card Cloning : Global Concern in the Banking Industry

Satyendra Sharma[1], Prof. (Dr.) Triveni Singh[2]
[1]Senior Manager (IT), Cyber Crime Monitoring Cell, Fraud Risk Management Division, Head Office, Punjab National Bank, New Delhi, India
[2]Indian Police Service, Superintendent of Police, Auraiya District, Uttar Pradesh, India

ABSTRACT

Nowadays, cyber crime is a serious problem in the world including banking industries wherein card cloning is the greatest concern. In various countries, banks are giving magnetic stripe card to their customers, which is not secure because card cloning of magnetic stripe card is very easy and cyber criminals can make cloned card easily using an electronic device known as skimmer. There is strong need to eliminate magnetic stripe cards from banking industries and issue chip based card to the bank customers so that their money can be secured in the banks. In this research, it is suggested that banks should use chip based card to fight against cyber fraud which happens using cloned card.

Keywords : Cyber Crime, Cyber Security, Skimming, Card Cloning, Cyber Criminals, Banking, Cyber Fraud

I. INTRODUCTION

At the present time, card cloning is the greatest concern in the banking industry worldwide. In various countries, banks are giving magnetic stripe card to their customers, which is not secure. Cyber criminals easily capture the data of card magnetic stripe using a device known as skimmer and the process of capturing the data using skimmer is known as card skimming in cyber world. After capturing the data from targeted plastic cards (debit/credit cards), cyber criminals write the same into the magnetic stripe of other plastic cards and prepare cloned card which is used to debit the bank account in fraudulent manner through ATM (Automated Teller Machine) and POS (Point of Cell) machine.

Some ATM skimming schemes employ fake keypads in lieu of cameras to capture PIN numbers. Just like the card skimmers fit over the ATM's true card slot, skimming keypads are designed to mimic the keypad's design and fit over it like a glove. If you notice that the keypad on your ATM seems to protrude oddly from the surface around it, or if you spy an odd color change between the pad and the rest of the ATM, it could be a fake [1].

II. METHODS AND MATERIAL

There are two types of transactions can be done using debit/credit card.

Card Present Transaction: In this type of transaction, physical appearance of card is compulsory. Without physical appearance, this type of transaction is not possible.

Card Not Present Transaction: In this type of transaction physical appearance of card is not

required. For this type of transaction card number, expiry date and CVV2 (Card Verification Value2) is required so that we can use the same at the time of online payment for shopping or payment of bills or fees etc.

Skimmer:

The typical ATM skimmer is a device smaller than a deck of cards that fits over the existing card reader. Most of the time, the attackers will also place a hidden camera somewhere in the vicinity with a view of the number pad in order to record personal identification numbers, or PINs. The camera may be in the card reader, mounted at the top of the ATM, or even just to the side inside a plastic case holding brochures. Some criminals may install a fake PIN pad over the actual keyboard to capture the PIN directly, bypassing the need for a camera [2].

Card Skimming:

It is the theft of credit and debit card data and PIN numbers when the user is at an automated teller machine (ATM) or point of sale (POS). Card skimming allows thieves to steal money from accounts, make purchases and sell card information to third parties for the same purposes. Generally, the exploit involves modified payment card reader hardware that fits over an existing genuine payment device or ATM. The phony reader collects and passes on payment card information for retrieval by the thief. PIN numbers may be retrieved with a keypad overlay or a hidden camera [3].

Card Cloning:

Cloning is the copying of stolen credit or debit card information to a new card. Cloning, also called skimming, requires copying information at a credit card terminal using an electronic device or software, then transferring the information from the stolen card to a new card or to rewrite an existing card with the information [4].

Card cloning refers to the process of extracting data from genuine debit/credit cards and transfers this information onto other card for making cloned card and later used by the cyber criminals for making fraudulent payment with these clones at real point-of-sale terminals [5].

Working of ATM Card Skimmer:

ATM skimming is the identity theft for debit/credit cards: Cyber criminals use an electronics device known as skimmer to steal the information stored on your debit/credit card and capture your ATM PIN using pinhole camera or keypad overlay. Skimmer can be easily installed over ATM card slot. When you swipe your card into the ATM card reader, your card passes through skimmer in which card writer is present which is used to capture and store the data of magnetic stripe of card.

In addition to that, for capturing ATM PIN, cyber criminals use tiny spy camera which position is nearby keypad so that PIN can be clearly captured.
After capturing the data from debit/credit cards, cyber criminals transfer these data into other magnetic stripe cards. These cards are known as cloned card and used by the fraudsters to do the fraudulent transactions in the account of targeted bank customers through ATM/POS machine.

Security Measures to Prevent Card Cloning:

- Always inspect the ATM/POS you are using. Skimmers (capturing device that captures data of card magnetic stripe) can be easily spotted on ATM/POS machine. If some parts around the slot for inserting the card do not seem right, please do not swipe your card and immediately inform to the bank or police.
- Always shield the keypad when entering ATM PIN. It will protect your PIN otherwise, if pinhole camera is deployed nearby ATM/POS, your ATM PIN may be easily captured. In

absence of ATM PIN, no ATM/POS transactions can be done in India.

- Do not use magnetic stripe card. Always use EMV (EuroPay, MasterCard and Visa) chip card which is more secure than magnetic stripe card.
- At present, even banks are giving EMV chip card but magnetic stripe are also present which is vulnerable and card is easily cloned using magnetic stripe. Hence inspect the ATM card reader and POS machine before swipe your card so that you can protect your card if skimmer is installed.
- One of the biggest security risks is that when your debit/credit card goes out from your sight at the time of paying the bill. Always ensure to swipe your card in front of you.
- Do not give your debit/credit card to strangers otherwise your card may be swapped or cloned

III. RESULTS AND DISCUSSION

Case Study:

A prolific credit card scammer who continued his crimes from behind bars is now serving a lengthy sentence thanks to a multi-agency investigation into his card-cloning operation.

From 2014 to 2016, Syracuse, New York, resident Daquan Rice, 23, and several associates purchased credit card numbers online from hackers in Russia, Pakistan, and Ukraine, who sell the information they steal. Rice also bought credit card numbers from a friend who worked at a Syracuse restaurant who had skimmed numbers from customer credit cards on Rice's behalf.

Rice had an associate in New York City with a credit card cloning machine, and he would provide the numbers to the person to make new cards for him. Rice and his accomplices then used these cards to buy gift cards, which they would convert into cash or money orders.

"It's unfortunately not that hard or complicated to get your hands on stolen credit card numbers," said Special Agent Brandon Mercer of the FBI's Albany Division, who investigated this case along with the U.S. Postal Inspection Service, New York State Police, and local law enforcement in the Syracuse area. "This information is readily available on the dark web from hackers and other criminals."

There was nothing a merchant could have done to stop the fraudulent transaction, because the thieves put the fake cards in their own names. So even if a cashier asked for identification, the name on the credit card would have matched their IDs.

"It was a numbers game. They would print out hundreds of these cards. They would go to the register and swipe, and if it didn't work, they would just throw it away and use the next one," Mercer said. "A lot of these cards were only able to used once because the cardholder noticed the fraud and shut down the card."
The fraudsters made about $80,000 over two years.

After his 2016 arrest for credit card cloning, Rice tried to continue his scheme—from his jail cell. In 2017, he worked with an accomplice, who was not in prison, to put more than $8,000 in funds stolen through credit card fraud on Rice's prison commissary account. Rice tried to use that account to write large checks, but the prison shut down his account for the unusual activity and contacted the FBI.

Rice pleaded guilty to wire fraud, money laundering, and aggravated identity theft, and in October, he was sentenced to more than 11 years in prison. Several accomplices have also been sentenced for their roles in the scheme [6].

Cyber crime remained an area of concern from the city police as they registered 3,286 in 2017 as compared to 2,402 in 2016. According to the data compiled by the Gurugram Police, Haryana, India. According to police officials, there were 1,954 complaints pertaining to online banking credit, Debit card fraud and cheating through mobile phones in 2017. Apart from it, 278 complaints were related to Facebook frauds and several other cases were registered under the Information Technology (IT) Act. In 2016, the online banking frauds were 1,345 and 151 Facebook complaints [7].

The U.S. Secret Service is warning financial institutions about a recent uptick in a form of ATM skimming that involves cutting cupcake-sized holes in a cash machine and then using a combination of magnets and medical devices to siphon customer account data directly from the card reader inside the ATM.

According to a non-public alert distributed to banks this week and shared with KrebsOnSecurity by a financial industry source, the Secret Service has received multiple reports about a complex form of skimming that often takes thieves days to implement.

This type of attack, sometimes called ATM "wiretapping" or "eavesdropping," starts when thieves use a drill to make a relatively large hole in the front of a cash machine. The hole is then concealed by a metal faceplate, or perhaps a decal featuring the bank's logo or boilerplate instructions on how to use the ATM [8].

Security Suggestion to Protect Debit/Credit Cards from Cloning

- By default, in all debit/credit cards, ATM/POS transactions should be disabled.
- Before disabling ATM/POS transactions, bank should inform to the customers well in time (at least two months before disabling) through SMS/Social media/News Paper/Television/Radio etc. with the following message "to register/update mobile number in the bank for continuing ATM/POS transaction facility".
- To enable ATM/POS transactions in debit/credit card, a missed call should be given on the specific number of bank using registered mobile number of the customer to enable ATM/POS transaction facility.
- After giving missed call, a message (mentioning that you are allowed to do ATM/POS transactions for today) should be delivered on the customer's registered mobile number immediately and customer should be allowed for transactions for same day only and when customer do the first transaction on that day, thereafter consecutive transactions should be completed within 15 minutes after first transaction. After 15 minutes of first ATM/POS transaction, the ATM/POS transaction facility should be disabled automatically.
- If customer wants more transactions on same day after disabling ATM/POS transaction facility then he may give missed call again on specific number to enable further transactions. But after 15 minutes of first ATM/POS transaction, the ATM/POS transaction facility should be disabled automatically.

If banks accept aforesaid suggestion, bank customers will never duped by the cyber criminals due to card cloning because by default ATM/POS transactions will be disabled and only genuine customer can enable transaction facility using his registered mobile number.

The present research is comprehensive as it deals with almost all the aspects of card cloning, security measures and preventive steps to avoid card cloning.

It also deals with the method of card cloning which is used by cyber criminals for stealing the money of customers from their bank account. Using card cloning cyber criminals are duping the bank customers daily around the globe.

The main reason of card cloning is the magnetic stripe which contains the card number, expiry date and CVV1 (Card Verification Value1). CVV1 is encoded within the magnetic stripe of card which is used at the time of card present transaction. CVV1 is different from CVV2 (Card Verification Value2). CVV2 is present on the back side of card which is used at the time of card not present transaction. Using cloned card, "card not present" transaction is not possible because in case of cloning CVV1 is captured through magnetic stripe not CVV2.

In many countries including India, magnetic stripe card is used. Banks in India have also given EMV chip card to their customers but facility of card swipe using magnetic stripe is also available on that card. Hence, any card having magnetic stripe is vulnerable and very easy to clone by the cyber criminals at ATM and POS machine. It is also found that majority of bank customers do not shield the ATM/POS keypad while entering the PIN (Personal Identification Number).

The main reason of this is the unawareness of customers regarding banking cyber security. Reserve Bank of India has made ATM PIN mandatory for card present transactions within India. However, for international POS transactions, ATM PIN is not required. If customers shield the keypad at the time of entering PIN at ATM/POS machine, then cyber criminals can not capture their ATM PIN and as a result instead of card cloning, card present transactions can not be done without ATM PIN within India. However, international POS transactions can be done without ATM PIN if bank has provided international transaction facility to that card.

Punjab National Bank (India) has disabled international transaction facility in debit cards as well as credit cards. If customer wants to enable international transaction facility in credit card, he can request to bank using online mode or through branch. If customer wants international transaction using debit card, in this case customer can request for separate international debit card [9].

Many banks in India and other countries provide international transaction facility in debit card and credit card to all their customers without their knowledge. Debit card is using by all segment of customers whereas credit card is used by limited customers. Hence, disabling of international transactions in debit card for all customers is a good initiative.

IV.CONCLUSION

- International transaction facility in debit card/credit card should be disabled by the bank for all customers.
- International transaction facility should be enabled only if customer gives his request to the bank. It will prevent fraudulent international transactions using cloned card.
- Banks should issue EMV chip based card to their customers to prevent from cloning.
- Bank should use anti skimmer device in ATM.
- To avoid such type of cyber fraud, cyber security awareness can play an important role.
- On the basis this research, we found that majority of bank customers are not aware with skimming and cloning and easily duped by the fraudsters.
- Banks should deliver basic banking cyber security training to their customers to prevent banking cyber fraud.

V. REFERENCES

[1]. Wesley Fenlon (November 2010) "How does ATM skimming work?" https://money.howstuffworks.com/atm-skimming.htm

[2]. Max Eddy (February 2018) "How to Spot and Avoid Credit Card Skimmers" https://in.pcmag.com/software/48978/how-to-spot-and-avoid-credit-card-skimmers

[3]. Margaret Rouse (January 2017) "Card Skiming" https://whatis.techtarget.com/definition/card-skimming

[4]. Julia Kagen (July 2018) "Cloning" https://www.investopedia.com/terms/c/cloning.asp

[5]. Michael Roland and Josef Langer "Cloning Credit Cards: A combined pre-play and downgrade attack on EMV Contactless" (2013) https://www.usenix.org/system/files/conference/woot13/woot13-roland.pdf

[6]. Brandon Mercer, special agent, FBI Albany (December 2018) "Credit Card Cloners Stole Thousands" https://www.fbi.gov/news/stories/credit-card-cloners-sentenced-120318

[7]. The pioneer (January 2018) Cyber Crime on rise, 3,286 cases reported in Gurugram https://www.dailypioneer.com/2018/delhi/cyber-crime-on-rise-3286-cases-reported-in-gurugram.html

[8]. U.S. Secret Service (September 2018) "Secret Service Warns of Surge in ATM 'Wiretapping' Attacks" https://krebsonsecurity.com/2018/09/secret-service-warns-of-surge-in-atm-wiretapping-attacks

[9]. Punjab National Bank (India)

Cite this article as :

Satyendra Sharma, Prof. (Dr.) Triveni Singh, "Rising Cyber Fraud through Card Cloning: Global Concern in the Banking Industry ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 3 Issue 8, pp. 357-362, November-December 2018. Available at
doi : https://doi.org/10.32628/CSEIT1838100
Journal URL : http://ijsrcseit.com/CSEIT1838100

Disclaimer: "All content presented in this paper is personal view of authors. This content can not be treated as an official view of the authors."