http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-11, Issue 09, September 2022

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-04

A Perspective on Prevalent Banking /ATM Frauds Focused on Types of Frauds, Methodologies Adopted And Suggested Preventive Measures / Solutions

Vishesh Bhatnagar[1], Dr Nischol Mishra[2]
M.Tech Student[1] (Cyber Forensics), Associate Professor[2]
[1,2]School of Information Technology *(SOIT)*, RGTU, Bhopal, M.P., INDIA
vb.eduportal22@gmail.com[1]

***Abstract*—With the increased dependency of our daily lives on technology, we are witnessing an evolving trend of increase in technology related crimes. Digital banking / financial frauds is a broad term that is used to define any form of fraudulent activity in which computers or computer networks are a tool, a target, or a place of fraudulent activity utilized for conduct of various category of frauds. Cybercrime is a general term that covers crimes like phishing, credit card frauds, banking frauds, Intellectual Property crimes, etc. In this paper we researched on several types of common frauds including SIM Swap frauds, Vishing, Smishing, Phishing, Money Mule, Trojan frauds and Fake Call Frauds.**

***Keywords*—SIM Swap, Vishing, Smishing, Phishing, Money Mule, Trojan, Fake Call fraudse.etc.**

I. INTRODUCTION

A. TYPES OF BANKING / FINANCIAL FRAUDS RELATED TO TECHNOLOGY

The ingress of technology into our daily lives has also created a parallel job industry flourishing on technology related crimes. The evolution of newer life tools / applications / gadgets, etc., ushers in newer vulnerabilities which become conduit for the perpetrators of digital crimes to exploit the same towards their advantage.

The various types of technology related crimes are as detailed under: -

a) **SIM SWAP.** Under this category the perpetrators essentially manage to get a duplicate SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, the fraudsters manage to get the One Time Passwords (OTPs), passwords, etc., required for making financial transactions through banking accounts.

b) **VISHING**. Vishing refers to the fraudsters' attempts to gather information relating to Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

c) **SIM SHING.** Smishing refers to the process of the perpetrator using mobile phone text messages to lure victim into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

d) **PHISHING.** Phishing refers to a type of fraud that involves stealing Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc., through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (Voice Phishing) and SMS(The ingress of technology into our daily lives has also created a parallel job industry flourishing on technology related crimes. The evolution of newer life tools / applications / gadgets, etc., ushers in newer vulnerabilities which become conduit for the perpetrators of digital crimes to exploit the same towards their advantage.

The various types of technology related crimes are as detailed under: -

a) **SIM SWAP.** Under this category the perpetrators essentially manage to get a duplicate SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, the fraudsters manage to get the One Time Passwords (OTPs), passwords, etc., required for making financial transactions through banking accounts.

b) **VISHING**. Vishing refers to the fraudsters' attempts to gather information relating to

Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

c) **SMISHING.** Smishing refers to the process of the perpetrator using mobile phone text messages to lure victim into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

d) **PHISHING.** Phishing refers to a type of fraud that involves stealing Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc., through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (Voice Phishing) and SMS

e) **MONEY MULE.** This term is used to describe category of frauds where innocent victims are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

f) **TROJAN.** The termessentially refers to a harmful piece of software that users are tricked into loading and executing onto their computers. Once installed and activated, the Trojans attack the computer leading to deletion of computer files, data theft, activation or spread of viruses. Trojans can also create backdoors.

g) **FAKE CALL FRAUDS.** Fake call frauds are related to Vishing and are also termed as Voice Phishing. Here, fraudsters essentially pretend to be calling from bank or is the bank's technical staff / representative. Sounding professional / convincing to the customer, the staff tricks the victim into giving away their personal and confidential data, such as: OTP, card numbers, CVV, Expiry Date, Security Password, ATM pin, Interne tanking login ID, password and other related information.

II. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING SIM SWAP FRAUDS

Fraudsters initially gather customer related information through Phishing, Vishing, Smishing or any other means.
Then, the fraudsters approach mobile operator and get the customer's SIM card blocked.

a) After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

b) The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

c) Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

III. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING VISHING FRAUDS

a) Fraudsters pose as an employee from the concerned bank or as staff from any of Government / Financial institution and ask for their personal information.

b) Fraudsters frame some authentic argument / reasons such as re-activation of account, en-cashing of reward points, sending a new card, linking the existing account with Aadhar, etc. to extract required information on customer

c) Details thus, extracted from the customer are than utilized for conducting fraudulent transactions, without the knowledge of the customer.

IV. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING SMISHING FRAUDS

a) Fraudsters send SMS intimating customer of prize money, lottery, job offers, etc., and requesting them to share their card or account details.

b) The innocent customer is made to visit a website, call a phone number, or download malicious content.

c) Details thus shared with the fraudsters (who initiated SMS) are fraudulent transactions on customer's account, causing them financial loss.

V. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING PHISHING FRAUDS

a) Fraudsters pose as bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

b) The link diverts the customer to a fake website that looks like the official bank website – with a web form to fill in his/her personal information.

c) Information so acquired is then used to conduct fraudulent transactions on the customer's account.

VI. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING MONEY MULE FRAUDS

a) Fraudsters approach customers through emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, offering attractive commissions, etc.
b) Once the account details are shared, the fraudsters transfer illegal money into the unsuspecting customer's account.
c) The customer is than asked to start a chain of transactions, culminating into the illegal money getting transferred into fraudsters account.
d) When such frauds are reported, the first customer & the chain (money mule) becomes the target of Police investigation.

VII. PROCEDURE FRAUDSTERS ADOPT FOR COMMITTING TROJAN FRAUDS

a) Fraudsters use SPAMMING techniques to send emails to numerous unsuspecting people.
b) Customers who open or download the attachment in these emails get their computers infected.
c) Whenever, the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.
d) These details are than utilized for conducting fraudulent transactions.

VIII. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST SIM SWAP

a) Keep your mobile number linked to bank accounts active and monitor the mobile number. In case, the number stops working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the scam.
b) Register for SMS and Email Alerts to stay informed about the activities in your bank account.
c) Regularly check your bank statements and transaction history for any irregularities.

IX. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST VISHING

a) Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email, etc.
b) Immediately report any attempted fraud / suspicious call on the Phone Banking number of your Bank / concerned financial regulatory body, etc.

X. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST SMISHING

a) Never share any personal OR financial information over the phone, SMS or email, etc.
b) Do not follow the instructions as mentioned in SMS sent from un-trusted source, delete such SMS instantly.

XI. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST PHISHING

a) Verify the URL of the webpage. The 's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption. Most fake web addresses start with 'http://'. Do not continue on such webpages.
b) Check for the prescence of Padlock symbol at the beginning of any URL / web address. Padlock designates the existence of a security certificate for the website, also called the digital certificate for that website. This is symbolic of accurate credentials which have been verified.
c) Establish the authenticity of the website by verifying its digital certificate. To do so, go to File / Properties / Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window, to check.
d) Check the web address carefully, before doing any transactions.
e) Type the website address in your web browser address bar, rather than going through search engines, voice search, etc.
f) Always check for the Padlock icon at the upper or bottom right corner of the webpage to be 'On'.
g) Install the latest anti-virus /anti spyware/ firewall/ security patches on your computer and mobile phones.
h) Always use non-admin user ID for routine work on your computer.
i) Never click on any suspicious link in your email.
j) Never provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard, etc.
k) Never open unexpected email attachments or instant message download links.
l) Never access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

XII. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST MONEY MULE

a) Do not respond to emails asking for your bank account details.

b) For any overseas job offer, first confirm the identity and contact details of the employing company.
c) Do not get carried away by attractive offers / commissions or consent to receive unauthorized money.

XIII. SUGGESTED PREVENTIVE MEASURES FOR PROTECTION AGAINST TROJANS

a) Never open e-mails or download attachments from unknown senders. Simply delete such emails.
b) Installing antivirus helps. It scans every file you download and protects you from malicious files.
c) Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.
d) Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan.
e) Download and use the latest version of your browser.
f) If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system.
g) If necessary, get your computer serviced.

XIV. FUTURE WORK

Future studies on the types of banking frauds / internet frauds including crypto currency, block-chain technology related products, frauds occurring though mobile applications like the recent loan based mobile application related frauds can be undertaken. Additionally, similar studies can be undertaken on technologies / products / applications relating to measures / products / tools / application of newer technologies like AI/ML being utilized to develop fraud prevention tools, etc.

REFERENCES

[1.] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=71614e8e7864
[2.] https://indiaforensic.com/certifications/cyber-crimes-india/
[3.] http://www.cybercelldelhi.in/netbanking.html
[4.] https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/90438911.cms
[5.] "Newsbank - The Sacramento Bee & Sacbee.com".
[6.] "What is Bank Fraud?". wiseGEEK.
[7.] "Home - JPMorgan Chase & Co".
[8.] Bell, Alexis (2010). Mortgage Fraud & the Illegal Property Flipping Scheme: A Case Study of United States v. Quintero-Lopez. Archived from the original on 2012-03-28.
[9.] "ATM deposit automation, ATM deposit processing, envelope-free deposits". Carreker.com. Archived from the original on 2009-02-04. Retrieved 2012-03-13.
[10.] "New U.S. Birth Certificate Requirement". Bureau of Consular Affairs, U.S. Department of State. Archived from the original on 24 April 2014. Retrieved 24 April 2014.
[11.] "Types of banking fraud | ANZ". www.anz.com. Retrieved 2016-05-17.
[12.] "Online fraud and scams - Australian Federal Police". www.afp.gov.au. Archived from the original on 2016-05-16. Retrieved 2016-05-17.
[13.] "How Prime Bank Frauds Work". US Securities and Exchange Commission.
[14.] Jump up to:a b Iguchi, Toshihide (April 2014). My Billion Dollar Education: Inside the Mind of a Rogue Trader. ISBN 978-988-13373-8-2.
[15.] Woods, Ian (1998). "Fraud and the Australian Banking Industry" (PDF). Australian Banker's Association.
[16.] 16.Department, Attorney-General's. www.ag.gov.au. Archived from the original on 2016-08-06. Retrieved 2016-05-17.
[17.] "China Daily News, 2012-7-17, Shi Yingying, "Man wins full pay-out in bank card fraud"".
[18.] "U.S. Code › Title 18 › Part I › Chapter 63 › § 1344 - Bank Fraud". Cornell Law School Legal Information Institute.
[19.] Shaw v. United States, 580 U.S. __, 137 S.Ct. 462 (2016).
[20.] Loughrin v. United States, 573 U.S. __, 134 S. Ct. 2384 (2014).
[21.] "Federal Deposit Insurance Corporation, Electronic Funds Transfers (Regulation E)".

ISSN(ONLINE):2278 - 3814

