Financial Fraud on Online Social Networks in India Along with Preventive Measures

Mr. Pratik Gaikwad
Department of Computer Science and Engineering,
Sanjay Ghodawat University,
Kolhapur, India.

Abstract **– In today's era people are associated with huge number of social networks like Facebook, Instagram, Twitter, Whatsapp etc. Indian Financial fraud on the Internet is an obvious form of cybercrime that has been affected by the global revolution. With respect to cyberspace, anonymous servers, hijacked emails and fake websites are being used as a tool and medium for fraud by cyber scammers. This paper presents the financial frauds due to online social networks and presents a small survey of some popular ways of financial frauds committed in the recent years in India. This Paper explores the different ways and methodologies used by Cyber criminals to carry out financial frauds through social network. Although new techniques and regulations are constantly being implemented to combat and eradicate various forms of fraud, cyberspace is also providing new tools that facilitate the commission of these scams. As a result, the purpose of this paper is to address and analyse some issues concerning the use of cyberspace for fraud by cyber scammers, particularly financial fraud, and the techniques employed.**

Keywords – Cyber Security, Online Finacial Frauds, Cyber Crimes, Social Engineering.

I. INTRODUCTION

Financial fraud is a situation in which the legal and ethical management of financial resources does not occur. Financial fraud affects ordinary people, commercial organizations, and has a negative impact on the entire economy and social system by causing money and wealth to be lost. Fraudulent actions such as identity theft and financial fraud are performed through the use of the internet to carry out such crimes. Attackers are using social media networks to choose their target and with help of methodologies like phishing and sniffing they will complete their modus operandi. The ultimate goal of these attackers is to get from the victim. In the era of digital social network everyone think that they are secure but in cyber security, it is just an illusion. In this paper we are going to explore the financial frauds from social media networks and its preventive measures.

The Organization of paper is as follows:

Section I presents Introduction. In Section II Methodologies of Financial Frauds are described. Section III presents the case studies for mentioned methodologies. Section IV describes the preventive measure for above scenarios, and we conclude this paper in section V.

II. METHODOLOGIES

A. *Phishing and Spoofing*

Phishing: it is a type of social engineering attack that is frequently used to steal user information such as login credentials and credit card numbers. It happens when an attacker poses as a trusted entity and tricks the victim into opening an email, instant message, or text message. The recipient is then duped into clicking a malicious link, which can result in malware installation, system freezing as part of a ransomware attack, or the disclosure of sensitive information.

With help of phishing Attacker can fool any person that they are visiting genuine site but in reality the site they are visiting is attacker controlled duplicate website of original site. Spoofing: Spoofing is a broad term for the type of behavior in which a cybercriminal poses as a trusted entity or device in order to trick you into doing something beneficial to the hacker — and harmful to you. Spoofing occurs when an online scammer disguises their identity as something else. Phishing and Spoofing are very common and most easy techniques in cyber security in order to carry out online frauds. In most of the cases Attacker, Clone the websites and sends the link of cloned website to user with help of spoofing as we discussed earlier spoofing can pretends the authenticity of the user, it pretends that the message is coming from authorized center only, if victim opens that cloned site and fill the credentials, as a result attacker can get that details and he can use the same details for his modus operandi. There are multiple types of phishing, Attacker can not only clone the websites but also they use Email phishing for such things. Criminals hope to fool you into thinking these faked emails are genuine, leading you to download malicious software, transmit money, or reveal personal, financial, or other data.

B. *Remote Access Softwares*

Remote Access Software: Remote access is the ability for an authorized person to connect to a computer or network from a remote location via a network connection. Remote access allows users to connect to the systems they require even when they are physically separated from them. Attacker uses this technology for cybercrime especially for financial frauds. In this type of cases attacker asks to install the Remote access software with help of social engineering. Attacker can spoof victim that they are calling from customer support team and they will resolve some issues via connecting this types of remote access software. Once the victim installs Remote access software, attacker is able to control the device of victim as the technology is made for the same. After getting access attacker will either install malware or he can use our browser cache and log in to our banking applications. If attacker installs malware he is able to receive the OTP from bank directly.

In Recent, the number of cases are increased where attacker is using this remote access software for online frauds. There are multiple case scenarios where attacker is pretending as they are calling from ISP [Internet Service Provider] and asking for KYC [Know Your Customer] for SIM updating process. For the same attackers used to request to install same Remote access software.

It has been discovered that the trend of online theft using screen-sharing applications began in 2020, when major financial transactions began to be conducted online. Many businesses are hesitant adopting Remote Access applications due to the danger involved. Because This Applications are notoriously unstable, most businesses have chosen to avoid it. On the screen is a code that, when shared, grants complete access to your screen. It has proven to be problematic for many businesses. "Every single day of this year, we have had at least one or two examples of remote sharing Applications. Utilized for stealing money," a cybercrime cell official who maintains data for the cell said. Because these Applications are frequently used to steal and misuse card data, they are classified as bank and card frauds. While individual amounts are always minor in comparison to other hacking methods, the total sum is significant considering the number of occurrences."

C. Identity Theft

Theft of another person's personal or financial information in order to commit fraud, such as making unauthorized transactions or purchases, is known as identity theft. Identity theft can take numerous forms, with the most common consequences being damage to a victim's credit, wealth, and reputation.

In pandemic where everything almost everything is shifted online identity theft frauds are increased by a huge number, where attacker is Steals identity of well-known person in society and creates a new Digital identity of the same person. Later on he use the cloned account and contacts the friends and relatives of that person for asking financial help, ultimately his modus operandi will be completed.

There are multiple types to do the identity theft here are some mentioned –

1. Clone Victims social media account, upload some pictures of him and ask financial help.
   In Such cases we don’t know who is messaging us, unless and until we confirm through Phone call. From 2020 such types of attacks are happens twice in day in cities like Mumbai and Delhi.
2. Pretending Victims that you are calling from Bank and Asks for CVV
   In Such Cases, peoples get trapped because the attacker is telling some details like last 4 digit of ATM Card which is not a big deal to get for them. They pretend like they are genuine bank employees by giving details like Our first and last name, dates on ATM cards and Last four digits of ATM card. According to research some attackers made some templates like Call for ATM Card Update, Call for ATM Card Expiry and KYC etc.

III. CASE STUDIES OF FINANCIAL FRAUDS

In this Section, Here are some latest case studies for recent financial frauds from India.

Case Study 1: Naptool Identity Theft

the customer purchased a bed sheet from Naaptol, an online buying service. He received a mail from the portal in July informing him that he had won a lottery ticket. On the occasion of its 10th anniversary celebrations, Naaptol had organized a lucky draw for its consumers, according to the letter. The claimant discovered he had won Rs 12 lakh after scratching the lottery ticket.

He called the phone number included in the letter to claim the $1,000 prize. The man was subsequently asked to pay Rs 5.47 lakh in taxes, GST, processing fees, and other miscellaneous costs on several times. He continued to pay the money till August 14th. However, when the fraudster demanded an additional Rs 58,000 in service tax, he realized he had been duped.

Case Study 2: Remote Access Application Fraud

while attempting to seek a refund on a cancelled flight ticket, a 54-year-old woman from Pune was scammed of Rs3.2 lakh. When she was trying to receive a refund on a flight she had booked from Chennai to Pune on October 20, she looked up the airline's phone number online and dialed it. However, the individual who answered the woman's call forced her to download two apps that enabled him remote access to her phone and kept her bank information. He asked her to send a message after she downloaded the applications, and by doing so, he was able to drain money from three bank accounts belonging to the complainant and her family members.

IV. PREVENTIVE MEASURES

People are still falling victim to scam by exchanging OTPs and passwords over the phone. Nobody has the right to ask for an OTP or a bank password over the phone, thus it should never be shared. One should also be careful not to fall victim to the words of those befriended only through social media with no background check.

A. Use Apps that are smart and verified Only

Mobile applications are convenient for accessing a number of services. However, not all applications are safe. As a result, be cautious about the applications you download on your phone and make sure they are authentic and validated. Established Fintech companies are developing countermeasures to avoid financial fraud in India using smartphone apps.

B. Make use of encrypted internet connections.

Signing on to an insecure public Wi-Fi connection might also be an issue since it makes your phone vulnerable to cyber criminals on the lookout. To perpetrate fraud, they can track your behavior and acquire access to your computer or smartphone. As a result, whenever you make an online payment or exchange critical personal financial information, make sure you do so over a secure private connection.

C. When using the card, be cautious.

When paying at a store, restaurant, or receiving home delivery, you should never take your card out of your sight. Check whether the POS equipment that reads cards is legitimate or a card skimmer that grabs everything.

The information needed to take your hard-earned cash only use the international transaction option while you're out of the country. Payment in India requires two-step verification.

D. Never provide any sensitive personal information.

Never give out your personal information to a stranger or a third party acting as a bank or financial institution representative. Do not reveal any personal or financial information over the phone, SMS, or email.

Bank officials would never contact you for such sensitive information. Never, ever share any sensitive personal information on social networking sites. Never transmit payments without first authenticating the identity of the individual requesting such information.

V. CONCLUSION

Online social networks have become an integral part of our daily routine. Users of social networks have access to a wealth of features and opportunities, such as sharing photos, stories, and experiences, as well as online conversing and entertainment. Though most of these are good, a select handful may pose a risk to users' data by exposing it to hackers and attackers. The frequency of attacks on social media platforms is steadily growing. It may be anything like online frauds. It is critical to instruct or guide individuals about their safety and security in order to avert these assaults. It's also crucial to educate them about the many types of hacking assaults and the implications of each. In this paper we explored how fraudsters can steal our money with help of our data only. The preventive measures regarding privacy and safety of data and applications which inturn helps to enhance security are suggested. An extensive case study analysis has been carried out to reveal potential threats in online social networks. Users must stay

Attentive while posting information on social networks and make sure about the privacy of data.

REFERENCES

[1] Introduction of Cyber Crimes [wikipedia.com]

[2] Phishing and Spoofing [Online] Available: https://www.imperva.com/learn/application-security/phishing-attack-scam.

[3] Remote Access Softwares [Online] Available: https://www.biocatch.com/blog/remote-access-scam-protect-customers

[4] Identity Theft [Online] Available : https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/identity-theft-fraud/

[5] Case Studies [Online] Available https://indianexpress.com/