Preventive Measures To Overcome Financial Frauds During COVID-19

Chetana Patil
2nd Semester, M.Tech, CNE
Department of Information Science and Engineering
B.M.S College of Engineering
Bangalore, India
chetanapatil.scn19@bmsce.ac.in

Jamuna C J
2nd Semester, M.Tech, CNE
Department of Information Science and Engineering
B.M.S College of Engineering
Bangalore, India
jamunacj.scn19@bmsce.ac.in

Varsha R
2nd Semester, M.Tech, CNE
Department of Information Science and Engineering
B.M.S College of Engineering
Bangalore, India
varshar.scn19@bmsce.ac.in

Dr. Ashok Kumar R
Professor, CNE
Department of Information Science and Engineering
B.M.S College of Engineering
Bangalore, India
ashokkumar.ise@bmsce.ac.in

Abstract*—The beginning of the year 2020 realized a long conversation, the coronavirus group of infections and how they are affecting our day to day lives. There is a massive increase of cyber security attacks which indeed motivates the cyber criminals to utilize this pandemic in an effort to better themselves. This study used information gathering and analysis on various aspect of cybercrimes. It also includes case studies on public organizations within the same area to have a full understanding of the nature of financial frauds. Considerably, after inventing various methods to stop extortion, fraudsters are constantly attempting to discover new ways to commit crime. Thus, in order to stop these frauds, the study has been made to bring mindfulness among the social gathering with respect to finance related frauds that are been carried out during COVID-19. This serve study benefits the public to learn preventive measures from the past committed frauds and be liable of adapting to future new methods of frauds and be aware of such fraudulent activities. Eventually the approach passes on how individuals should take fundamental activities when they prey to digital assailants.

***Keywords*—fraudulent, coronavirus, ransomware, bitcoin, UPI ID, tracker**

I. Introduction

The Coronavirus Disease (COVID-19) is one of the major outbreaks throughout the globe, attacking the society at its core thereby destroying thousands of lives leading to global crisis. It has been characterized as a pandemic worldwide by the World Health Organization (WHO) on 11th of March 2020[1]. Even under such circumstances people are greedy enough to heist others money. In this regard many cases have been filed in the respective jurisdictions against financial frauds, in which most of the cyber criminals built the trust for them among the innocent people and tried to steal a huge sum. This led to the economic crisis among the vulnerable population that includes people with less knowledge about the technology usage, people with disabilities, older persons, well known organizations and companies, people under poverty, the young minds that is the youths who are threatened emotionally to perform some task, etc. A survey from the PwC on Global Economic Crime and Fraud mentioned that, around 47% of companies worldwide experienced a fraud in the past 24 months out of which, only 56% conducted investigation into their fraud incidents [2]. Also an article was published on CNBC which is an American based business news channel stating that, around $13.4 million have been lost by the Americans in the coronavirus related scams which is around 3% of the total scam that was reported to the Federal Trade Commission by the end of March 2020, that sum up to $432.4 million [3].

A study was made in this regard by considering few of the major scams that took place globally during COVID-19 pandemic. Even though the cyber security specialists have taken utmost care to protect the society, criminals are intelligent enough to breach the system's security environment either physically or with the help of technology. The study also predicts that how innocent people or an organization is prone to financial scams because of unawareness among the social population about the trending technology, incorporation of less advanced security systems and the loop holes that exists in them. Such limitations servers as an advantage for the cyber criminals to commit financial frauds among the social group. Further, the study is to bring awareness to the society about the scams committed and also to protect them from the cyber criminals to whom they could be victims in mere future. Finally, the study also reveals about the preventive measure to be taken against the fraudulent to be secure during the pandemic situation. Also, it includes valid proofs and evidences about the scams that were committed during this pandemic situation.

II. Literature Survey

The infection that is answerable for causing the COVID-19 has been characterized by the WHO as the Severe Acute Respiratory Syn-drome Coronavirus 2 (SARS-CoV-2). At this point in time there is as yet other continuous pandemics with respect to the Middle East Respiratory Syndrome (MERS) and HIV/AIDS. Ebola is the latest pandemic which has been esteemed as being leveled out. Ebola cases despite everything happen and the last outbreak has been accounted on the 1st of August 2018. Even Ebola outbreak had a few digital security dangers identified like Ebola spam mail. The increase in digital security danger is because of the society is with complete dependence on the online availability and system foundation of each nation and with the People, who are not really technically knowledgeable. So, humans are growing targets for cyber attackers during pandemics, which is as shown in Fig. 1 [1].

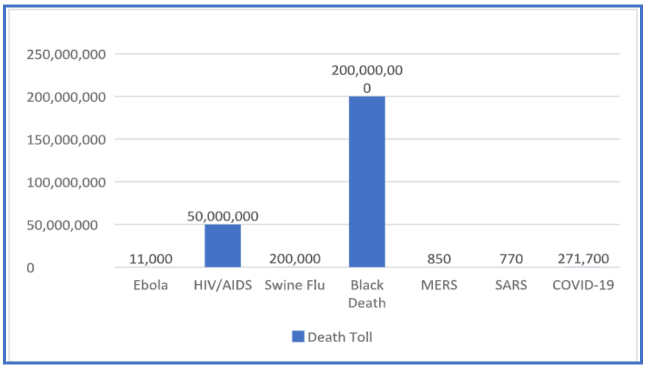


Fig. 1 Fatality rate during Pandemics

Almost all banks offer on the web and versatile financial administrations. Charge card, Master Card and other installment techniques are utilized for banking exchanges. ATM machines and other electronic channels utilized for these installments, is the principle focus of digital assaults and at that point in different divisions or sectors faces numerous difficulties because of different fakes and untrustworthy practices with respect to clients and workers of the banks.

Here are instances of banking extortion is increasing year by year, as shown in the Fig. 2 [10].

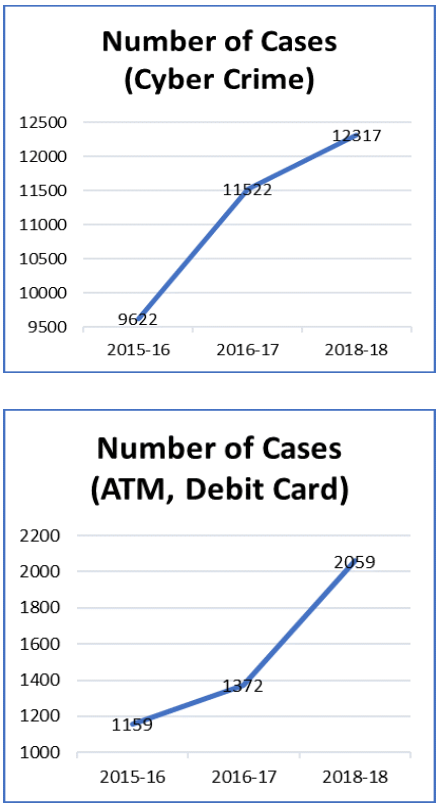


Fig. 2 Number of frauds increasing year by year

According to RBI information, during the period 2013-2017, 17,504 bank cheats revealed. Around 5,200 authorities were held for extortion in Public division banks during period 2015-2017. The examination shows that top bank in the rundown of cheats by bank authorities were State Bank of India (SBI), Indian Overseas Bank (IOB) and Central Bank announcing 1538, 449 and 406 cases individually, as shown in the Fig. 3.

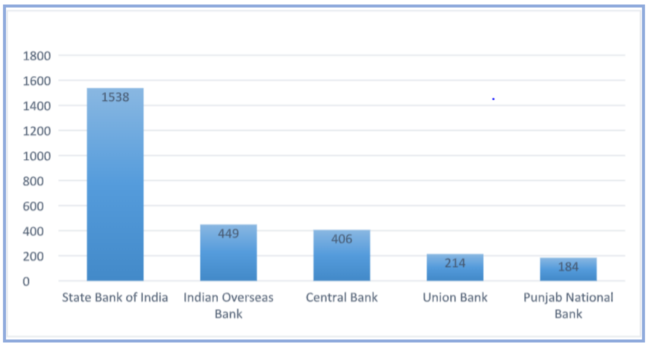


Fig. 3 Various cases involved Bank Officials

Implementing a productive way to detect the frauds for all Master Card giving banks to limit their misfortunes. Numerous advanced strategies dependent on Artificial Intelligence, Data mining, Fuzzy rationale, Machine learning, Sequence Alignment, Genetic Programming has developed in detecting different Credit card fraudulent exchanges [16, 17].

Several articles in the past has mentioned that scammers are using fake coronavirus stimulus payment sites to steal the money. As indicated by an examination by cybersecurity organization Check Point, scammers are focusing on individuals through improvement themed sites and messages for taking information and cash. In the month of March 2020, the US Congress passed a noteworthy $2 trillion upgrade bundle to help Americans to fight with impacts of the coronavirus pandemic. But cybercriminals are exploiting this circumstance to trap the individuals out of their cash. In these troublesome situations coronavirus related assaults have shot up from 14,000 assaults per day on normal in March 2020, to 20,000 assaults for every day. It included that an 94% of assaults in the previous fourteen days have been phishing, as shown in the Fig. 4 [7].

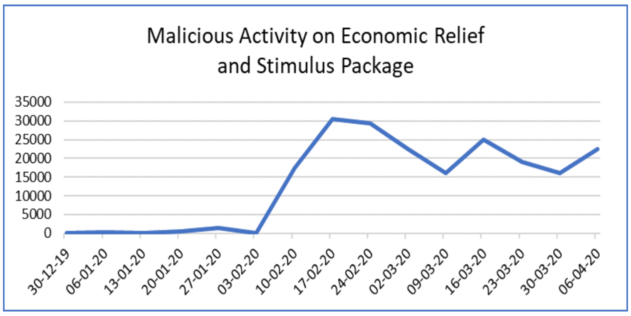


Fig. 4 Impact of Malicious Activity on Economic Relief

III. Case Study on Financial Fraud Proposed Work

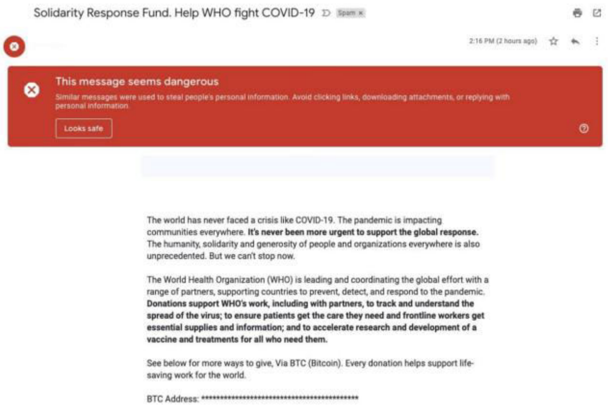
The main objective of this study is to spread awareness of the financial frauds undertaken by the fraudulent among the innocent people during the pandemic situation. This is the best example for crime against property where, a criminal is motivated to commit an illegal act to obtain money, property or any other benefits from the victim to fulfil one's personal desire. However, here are few of the outlines that were drawn during the crisis of COVID-19, each having few examples to show how criminals commit financial frauds by gaining trust of the people.

A. *Scams through E-mails*

E-mail has been a great communication tool during the lockdown period for a corporate and a social life. Hence this tool serves as an advantage for a scammer to steal money from the victims. As the virus have spread worldwide, while sending fake e-mails scammers claim to be from well-known organization such as WHO, Centre for Disease Control and Prevention, President of a Country or any Legal Body.

Scammers can send fake e-mails in the name of Tax-Authority, offering concessions for the victims on the tax payments (tax refunds) in order to help them to cope up with the pandemic situations [1]. The mail sent will also promise victim to protect against the virus by the usage of a new vaccine as mentioned or can prompt the victim to have a live conversation with the medical experts for an antiviral remedy. But in reality, the scammers are trying to obtain personal information, or install Malware, or some Ransomware into the victim's device through the false link that they create, that can lock the victim's system until they pay to the scammer [4].

There are many such real-time examples, but one of the scam mentioned here was regarding a fake email sent by the scammer, who impersonates to be an authority of WHO, seeking for the donation to ensure that patients get proper care, the frontline workers get essential supplies and also to accelerate research and development of the vaccine to the needy. The mail also provided with the banking credentials to deposit the money Via BTC (Bitcoin) which is as shown in the Fig. 5 [5].



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. **Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.**

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support life-saving work for the world.

BTC Address: **

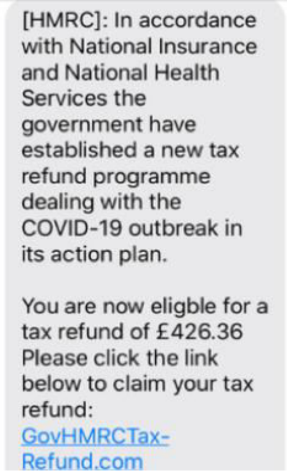
Fig. 5 An E-mail impersonates the WHO

Along with this the scammer can also try to harass the victim by sending mails that require immediate response from the victim as it mentions that, the scammer knows every single detail of the victim. Then they try to blackmail the victim by demanding a huge pay in order to avoid spreading of their personal information on the social media [6].

B. *Scams through Text Messages*

As cell phones have been an integral part of every individual, the attacker can easily use such means to fraud the people worldwide by sending simple text messages. Such scams have increased during COVID-19 where, an attacker sends fake and attractive messages to the victim. The content of the message indicates that they have approved with a grant, which will include any electronic gadget, cash prize, coupons etc. [9], due to the outbreak of COVID-19 to spend during the lock-down period or even as a goodwill to save from the crisis.

The scam was committed by spreading the misinformation in the name of HMRC (HM Revenue & Customs) where, the message stated that the government have established a new tax refund scheme in accordance with National Insurance and National Health Services due to the COVID-19 outbreak. It also notified the victim to claim the tax refund of 426.36 euros by navigating through the link given which is a shown in Fig. 6 [8]. Similarly, there were many such scams committed in the name of the well-known organization to fraud the people around the globe.



[HMRC]: In accordance with National Insurance and National Health Services the government have established a new tax refund programme dealing with the COVID-19 outbreak in its action plan.

You are now eligble for a tax refund of £426.36 Please click the link below to claim your tax refund:
GovHMRCTax-Refund.com

Fig. 6 Fake message claimed to be from HMRC

The message can also be sent by the attacker by impersonating any bank in which the victim conducts financial transaction. Such messages can intimate the victim about unauthorized access to the bank account, credit card, net banking, etc. [9] Hence this makes the victim eager enough to reply to the text messages or to navigate through the link sent along with the message to safeguard his amount thereby prone themselves to financial attack.

C. *Scams in the name of Recognized Organization*

Major fraud rates are in the name of the Banks, Fraudsters will always be cautious in gathering information about the victim's Bank where their frequent financial transactions happens. They try to boost in the confidence among the victims for them by posing as a Bank Representatives and inform the targets on the bank related issues such as, cheque bounce, loan moratorium, account block, credit or debit card failure, etc. In the process, they trick the innocent victims to provide their bank details and convince them to share the OTP (One Time Password) by giving the impression that, the OTP is the confirmation code to avail the services for which they had called [11].

As the World is fighting against COVID-19, the Prime Minister of India have introduced a PM CARES Fund (Prime Minister's Citizen Assistance and Relief in Emergency Situations) where, people of the nation can donate for the well-being of the Indian citizens. But the hungry fraudsters made a false UPI (Unified Payments Interface) ID's such as, pmcares@pnb, pmcares@hdfcbank, pmcare@yesbank, pmcare@ybl, pmcares@icici, pmcarefund@sbi, pm.care@sbi, pmcare@sbi, pncares@sbi ,and so on in contrary to the original UPI ID that is, pmcares@sbi as shown in Fig. 7 [11]. However, the fraudsters are so intelligent that by doing so they try to mislead people into sending money to a fake account by building an impression among the people that they have transferred the money into PM's relief Fund. This is because all these UPI ID's prove to be valid in all the payments app that is used to transfer the fund [12].

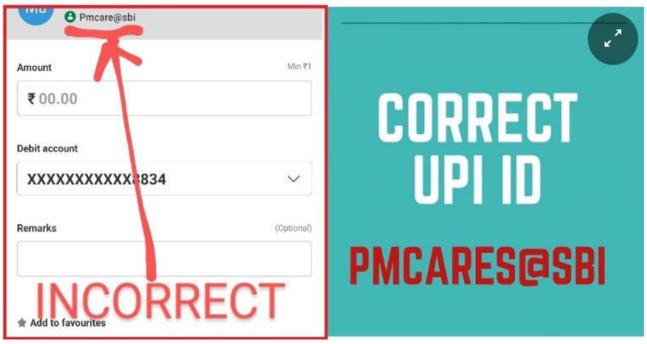


Fig. 7 False UPI ID in the name of PM's Relief Fund

The scam that took place in this regard caused the arrest of two men who tried to steal nearly 52 Lakh rupees in the name of PM's Relief Fund. The Fraudsters had opened two separate bank account, one in the Punjab National Bank and the other in the Union Bank of India at two different locations and tried to raise money by creating a fake website in the name of PM's Relief Fund [13].

D. *Scams through Phone calls*

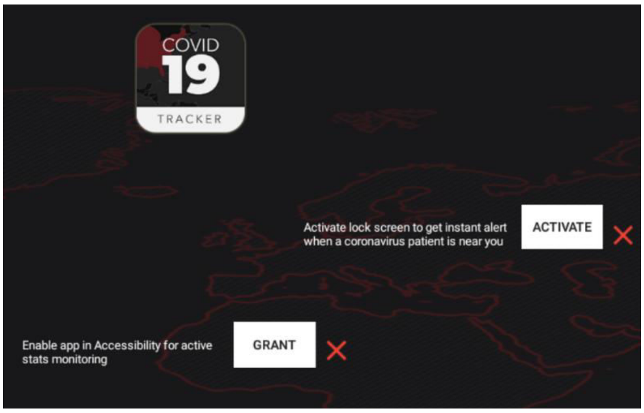
The calls that the targets receive from the cyber criminals can also mislead them in an assumption that, they have received the calls from the call-centres or from a genuine source. One of the audio transcripts of a Robo call in the United States surveyed by ABC news reported that, the audio insisted the victim to pay $79 by pressing 0 in order to conduct a full air duct cleaning and sanitization by their technicians to the loved ones. By this the victim can protect their loved ones against coronavirus [14].

The cyber criminals can also call the victims directly impersonating as Bank representatives or as a stranger and try to harass them mentally. Such calls can eventually hamper the strength of the victim to face the criminals and leads them to perform the desired tasks in panic, as mentioned by the cyber criminals.

E. *Scams through Applications*

During this pandemic period people have the tendency to watch their interested shows in the applications such as, Netflix, Amazon Prime, or Hot Star, etc. [9] Taking this as a platform, fraudster try to spread a fake message claiming to provide free service during the lockdown period or they can even demand a minimal amount for the subscription of the application. There were also few of the fake links that was sent to the targets in the name of WHO to know the status of the spread of coronavirus. As soon as the target clicks on the link his screen can be viewed, bank account, credit card and password details can be captured by the hackers [11].

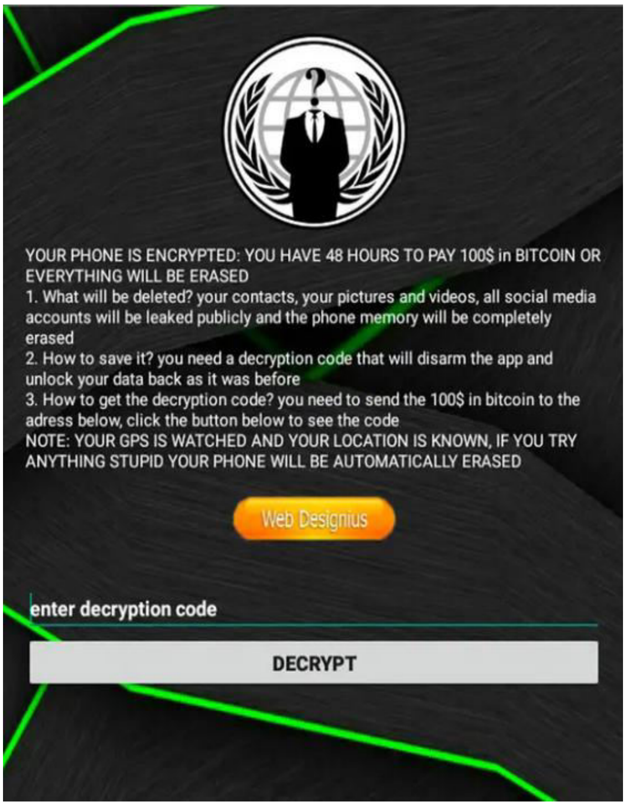
With this lockdown period around 4,000 new domains were registered in the name of COVID, corona, virus, etc. where most of them are used by the criminals to commit crime of stealing innocent people's money [11]. One such website named COVID 19 Tracker released by the fraudster that have the capacity to install ransomware into the victim's phone, making itself to map track the coronavirus spread. It infects the device by gaining permission from the victim for the lock screen and the device accessibility settings as shown in Fig. 8. Once the victim grants the permission, the ransomware locks or encrypts the device and demands the victim to pay $100 in Bitcoin to the hacker within 48 hours to unlock or decrypt the device with the code thereby saving their data from being erased as shown in Fig. 9 [5].



Activate lock screen to get instant alert when a coronavirus patient is near you

Enable app in Accessibility for active stats monitoring

Fig. 8 COVID 19 Tracker asking permission grants



YOUR PHONE IS ENCRYPTED: YOU HAVE 48 HOURS TO PAY 100$ in BITCOIN OR EVERYTHING WILL BE ERASED

1. What will be deleted? your contacts, your pictures and videos, all social media accounts will be leaked publicly and the phone memory will be completely erased

2. How to save it? you need a decryption code that will disarm the app and unlock your data back as it was before

3. How to get the decryption code? you need to send the 100$ in bitcoin to the adress below, click the button below to see the code

NOTE: YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN, IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED

Fig. 9 Blocking of victim's device by COVID 19 Tracker

Many fake websites also claim to give away free vaccine kits which were manufactured by WHO to protect themselves from the coronavirus. Initially they ask the targets to input the card details on the website to make a shipping payment [5]. By this the fraudulent will steal the victim's information to carry out fraudulent acts. Criminals have also spread false news of selling great monuments for an amount to raise money to fund a state to fight against COVID-19 [15].

F. *Scams through Facebook*

An explicit scam that took place through Facebook Messenger where, a customer received a message from his long-time friend enquiring about the $100,000 coronavirus pensioner grant from the government. Then he was guided by his friend to contact an unknown person claiming to be a co-ordinator of the government payment via Facebook Messenger. In order to process the amount, he was instructed to provide an identification document as a proof along with a deposit amount of $1,500 to an account. Later as the customer received another message in the need of more money for the grant processing, he contacted his friend directs for confirmation and both could realize that his friend's Facebook account has been hacked [21].

This scam was a strong example of how cyber criminals could trick the people even if they are knowledgeable about the internet and technology.

IV. Proposed Preventive Measures to refrain from Financial Frauds

A. *Vulnerabilities*

Describes how people get exploited (get hurt, get influenced or attacked) by frauds during pandemic situations. Fraudulent make use of this sensitive period to exploit people in a better and easy way. People are unaware of these vulnerabilities and becomes victims easily.

At present there is no vaccine found to cure covid-19 but fraudulent make use of people innocence and fear about the infection. They scam by proposing an offer about the vaccine, test kit, mask etc and convince them to buy these products. People become victims of such scam as they are more concerned about their health and their safety.

Scammers also take advantage of this situation and they claim to be a member of well-known charity or Foundation and convince people to donate money on humanity grounds to help such needy. But misfortune is that they make use of collected donation for their personal benefits.

Hackers are using a tactic to trick people into downloading paid/unpaid apps and claim that they can track the infected people around them. Also, they ask people to download certain applications or android app and in return get free surgical masks or test kits delivered to their doorstep.

Scammers also pretend to be representatives of WHO and other organization by sending out emails or messages to seek donations or in other case they send emails or messages stating that they are donating certain amount to an individual to overcome this situation but to claim the donation they ask people to pay small amount of deposit.

In pandemic situations government authorities create UPI accounts to receive donations from public. Scammers create fake UPI account similar to authenticated UPI account such that they mislead the public to donate to fake UPI account.

One of the biggest scams is fraudulent make rob call to people in the name bank customer care and ask for user credentials. Scammers make use of the credentials and steal money from the account.

B. *Preventive Measures*

Till today there is no vaccination discovered for covid-19 so, do not be in urge to buy vaccine online or from any pharmaceuticals. In other cases, be careful about the messages, emails or Robo calls received in the name of vaccine for covid-19.

Before doing any donations to charity or foundation, make sure that the charity or foundation is genuine by doing background checks like, checking details through google or seek suggestions from others to confirm whether it is genuine or not.

When you are downloading the app, which they claim to track the information about infected people around you, make sure that it is from trusted source as there are many fake and harmful apps. Downloading such apps allows hackers to access the personal information of the user including financial details from the phone. While downloading apps do quick research about the apps and authenticate it before downloading.

Whenever you are donating money through UPI account, verify it or double check the official name and logo of the UPI account given by the concerned government before donating. As many similar UPI accounts are created and fake bank accounts are attached to steal your money.

Whenever you get a Robo call in the name of the bank's customer care and if they ask for the banking details or OTP generated, never share any details. If they ask for these details its sure that it's a fake call, as no authorized banks will ask for the account details through phone calls or messages.

C. *Where to report about scams*

For all types of financial frauds, it is important to report the crimes to the appropriate agencies and law enforcements as early as possible. There are many ways to report a crime.

One can report to Cyber Crime Police about the crime or can report at Cyber Crime Reporting Portal, where one should provide accurate details while filing the complaint for the action to be taken against the crime and criminal. Complaint can be raised online at the online portal too.

All these government authorities and agencies are concerned to investigate such cybercrimes and is on high alert to stop the cyber criminals from committing scams.

V. Conclusion

The study reveals that there are many reasons of frauds to be committed, as people are facing economic crisis which motivate them to commit such frauds. So, this situation force scammers and fraudulent to create anxiety among people to steal their money. They also influence people to donate money in the name of fake organizations, charities and foundations by sending fake emails, messages and through Robo calls. Risk of frauds are increasing day to day, due to the usage of e-banking or internet. To overcome these issues, one should be aware about the vulnerabilities of such scams and educate people by creating awareness about such frauds so that they will not be victims of such frauds. If you are a victim kindly report to concerned organization so that the criminal is caught and punished.

REFERENCES

[1] Mouton, Francois & de Coning, Arno, (2020), “COVID-19: Impact on the Cyber Security Threat Landscape”. URL: https://www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

[2] PwC’s Global Economic Crime and Fraud Survey 2020, “Fighting fraud:A never-ending battle”. URL: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

[3] CNBC News, Personal Finance, Published Wed, 15 Apr 2020 by Greg Iacurci, “Americans have lost $13.4 million to fraud linked to Covid-19”. URL: https://www.cnbc.com/2020/04/15/americans-have-lost-13point4-million-to-fraud-linked-to-covid-19.html

[4] Washington State Office of the Attorney General, 19 March 2020, “AG Ferguson warns of scams related to COVID-19”. URL: https://www.atg.wa.gov/news/news-releases/ag-ferguson-warns-scams-related-covid-19

[5] RSA, 30 Mar 2020 by Heidi Bleau, “ Pandemic Fels Cybercrimes: 8 Scams to Watch For”. URL: https://www.rsa.com/en-us/blog/2020-03/pandemic-fuels-cybercrime-8-scams-to-watch-for

[6] The Guardian, International Edition, Published Sun, 29 Mar 2020 by Simon Goodley, “ Social disease:hoe fraudster adapt old scams to exploit coronavirus”. URL: https://www.theguardian.com/money/2020/mar/29/coronavirus-social-disease-fraudsters-adapt-old-scams

[7] TheNextWeb, Published Mon, 20 Apr 2020 by Ivan Mehta, “Scammers are using fake coronavirus stimulus payment sites to steal your money”. URL: https://thenextweb.com/security/2020/04/20/scammers-are-using-fake-coronavirus-stimulus-payment-sites-to-steal-your-money/

[8] YorkshireLive, Crime, Published Sat, 28 Mar 2020 by Nathan Hyde, “Cruel scammers cash in on coronavirus with scam text promising 400 euros tax refund”. URL: https://www.examinerlive.co.uk/news/west-yorkshire-news/coronavirus-tax-scam-text-difference-18001368

[9] Self, Articles, “ A Complete List of Coronavirus (COVID-19) Scams”. URL: https://self.inc/info/coronavirus-scams/

[10] Mamta Shah, “ A Case Study on Increasing of Banking Frauds in India”, Maharaja Surajmal Institute Journal of Applied Research, Vol 2. Issue 1; January-June 2019. URL: https://msi-ggsip.org/msijr/papers/vol2issue1/2_1_4.pdf

[11] Livemint, Personal Finance, Published Wed, 15 Apr 2020 by Tinesh Bhasin, “Covid-19-related frauds to shield yourself from”. URL: https://www.livemint.com/money/personal-finance/covid-19-related-frauds-to-shield-yourself-from-11586972212973.html

[12] Inda Today, News, Published Mon, 30 Mar 2020 by Arvind Ojha, “Delhi Police books fraudsters for making fake SBI account of PM’s Covid-19 Relief Fund”. URL: https://www.indiatoday.in/india/story/delhi-police-books-fraudsters-for-making-fake-sbi-account-of-pm-s-covid-19-relief-fund-1661272-2020-03-30

[13] The Times Of India, City News, Published Sat, 11 Apr 2020, “Two held for siphoning of Rs.53 lakh in name of donations to PM’s relief fund”. URL: https://timesofindia.indiatimes.com/city/ranchi/two-held-for-siphoning-of-rs-53l-in-name-of-donations-to-pms-relief-fund/articleshow/75087696.cms

[14] ABC7News, News, Published Sun, 22 Mar 2020 by By Michael Finney and Renee Koury, “Coronavirus: FCC, PG&E warn of risein scams playing on COVID-19 fears”. URL: https://abc7news.com/coronavirus-us-what-is-news-the/6033426/

[15] CGAP, Blog Series - Coronavirus (COVID-19): Financial Services in the Global Response, 09 APR 2020 by David Medine, “Financial Sams Rise as Coronavirus Hits Developing Countries”. URL: https://www.cgap.org/blog/financial-scams-rise-coronavirus-hits-developing-countries

[16] Delamaire, Linda & Abdou, Hussein & Pointon, John, “Credit card fraud and detection techniques: A review”, Banks and Bank Systems, Volume 4, Issue 2, 2009. URL: https://www.researchgate.net/publication/40227011_Credit_card_fraud_and_detection_techniques_A_review

[17] S. Benson Edwin Raj and A. Annie Portia, "Analysis on credit card fraud detection methods," 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), Tamilnadu, 2011, pp. 152-156, doi: 10.1109/ICCCET.2011.5762457. URL: https://ieeexplore.ieee.org/document/5762457