IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"An empirical study on trust factor due to rising fraud during COVID 19 pandemic."

Mrs. Jharna Sarkar

Assistant professor

Shri Chinai College of commerce and Economics, Mumbai-400 069, Maharashtra, India

ABSTRACT:

This paper aims to identify the common characteristics of pandemic-related fraud and any threats specific to pandemics and financial crises most similar to COVID-19 in modern times. The study's findings outline several novel crime types and tactics that have emerged during the 2020 COVID-19 pandemic and have never been seen before. Advances in technology, and operations by enforcement of law and government guardians. Many scams appear regardless of the state of the economy, but some specific scams, particularly internet scams, appear during pandemics. Similarly, economic crises uncover certain previously undetected scams, while economic crises drive scams that stem from and cause bankruptcies.

The report examines primary data and secondary data. Primary data was collected from the questionnaire method using online Google forms and circulated in the Mumbai region. Secondary data were collected from different government records, journals, books, etc.

What we can learn about the responses of individuals and organized crime to specific initiatives and other activities. These include social distancing, loan/mortgage freezes, retiree cash payments, capping cash payments in favor of contactless payments, greed for profit through the sale of health products, welfare fraud, identity abuse, IT fraud through data manipulation and telephone tariffs, corporate fraud payroll fraud, wage theft or dishonestly underpaying Employees, consumer fraud, insurance fraud and contractual dishonesty in non-return of deposits on bookings or non-repayment of government-guaranteed loans. The finding of the study investigates the trust factor of online payment and different fraud and we also measure the correlation between the trust factor and online payment.

Scams using phishing and supply. Scammers pose as health organizations and businesses to get personal and financial information, as well as offer counterfeit COVID-19 test kits, supplies, vaccines, and remedies.

Scams involving stimulus checks or economic help. According to reports, the government will assist in mitigating the virus's economic impact by giving money by check or direct deposit. The government, on the other hand, will not ask for a charge or personal or account information in exchange for the monies.

Scams involving charities. Fraudsters solicit funds for fictitious or non-existent charities. Malware distribution via "virus-tracking apps" or sensationalized news reports. Scams involving service providers. Scammers pose as doctors or hospital employees and call victims, claiming to have treated a family member or friend with COVID-19 and demanding payment. Bank workers falsely claim that banks are restricting deposit access or that bank deposits are unsafe. Scams posing as "research papers" claim that publicly traded corporations' products or services may prevent, diagnose, or cure diseases. COVID-19.

Keywords: COVID 19, scam, fraud, digital payment

INTRODUCTION:

WHO labeled the Novel Coronavirus Disease (COVID-19) outbreak a pandemic on March 11, 2020, and reaffirmed the need for countries to take prompt action and scale up the response to treat, detect, and reduce transmission to save people's lives. The first case was found in Kerala, India. This is a deadly infectious virus to control more spread, Government of India, took such corrective measures as wearing a mask, social distancing, and strict lockdown. Due to lockdown, people are unable to travel outside therefore majority of people preferring for online transactions. But there are certain challenges such as internet issues, lack of information and awareness, and lack of facilities. Since the commencement of the COVID-19 pandemic, WHO has noticed a substantial growth in the number of cyberattacks intended at its employees, email frauds aimed at the general public.

The World Health Organization is now transferring known vulnerabilities towards a more secure authenticated user. Scam artists imitating WHO in email messages have been increasingly targeting the public at large to divert donations to a phony COVID-19 Solidary Response Fund rather than the legitimate COVID-19 ideologically compatible Emergency Fund. The number of internet violence aimed at society has increased fivefold during the same time last year.

WHO is collaborating with the commercial sector to develop more secure internal systems and security measures, and also training employees about cyber security dangers.

WHO advises the public to be wary of phishing emails and to seek out accurate information about COVID-19 as well as other health issues from reputable sources?

Because the information was not recent, the hacked passwords did not place WHO systems in danger. The attack did, however, have an impact on an earlier extranet system that was used by present and retired employees and also partners.

1. **Harmful websites:** Throughout the COVID-19 pandemic, cyber threat actors have taken advantage of global interest in the virus's latest developments. By registering website domains related to COVID-19, these threat actors take advantage of internet users. Fake websites and apps often promise to give news, tests results, or other resources, but all they want is your passwords, bank account information, or malware on your devices.

Users may let their guard down and be more vulnerable to emails from unconfirmed senders while many firms and employees continue to work from home

2. Phishing Emails:

Expect phishing emails to be on the rise Cyber threat actors will utilize COVID-19 phishing emails in an attempt to convince the recipient to either reveal sensitive information (i.e. bank account information) or simply try to convince the recipient to open a malicious link or attachment, allowing them to potentially access your system.

COVID-19 vaccine-themed phishing emails may include subject lines such as the following:

- Vaccine registration
- Information about your vaccine coverage
- Locations you can receive the vaccine
- Ways you can reserve a vaccine

Vaccine requirements:

While some phishing emails might be easy for you to detect, never get complacent when reviewing your emails. Expect to receive well-composed phishing attempts that are impersonating well-known and trusted entities, such as government agencies, healthcare providers, or pharmaceutical companies. NEVER open any link or attachment from a source that you cannot identify as being legitimate!

In the past, email phishing attempts imitating the Centers for Disease Control and Prevention targeted state-level authorities (CDC). The receivers of these emails were instructed to click on links to see a secure message containing COVID-19 vaccine information. This kind of link can easily lead to a webpage that seeks to collect PII, such as a user's name, address, date of birth, driver's license number, phone number, and email address.

Here are several telltale signs that an email, text message, or phone call is a phishing attempt:

- Creating a sense of urgency for people to click on a link or offer information
- Is it extremely formal or worded in a convoluted manner?
- Requests that you evaluate a link or attachment or provide sensitive information.
- Users are required to follow an unusual or non-standard procedure.

3. Charities that aren't what they claim to be:

Threat actors will continue to attempt to start bogus charities to raise funds for illegal or non-existent groups as long as the pandemic exists. Fake charity and donation websites will aim to take advantage of people's good intentions, especially in these difficult circumstances. Always do your homework before contributing or disclosing any personal information.

4. Scams Relating to Unemployment:

As tax season approaches, be on the lookout for identity theft scams involving fake claims, particularly those involving unemployment benefits. This scam has grown in popularity during the COVID-19 pandemic when unemployment claims have been on the rise in general. The most common scams to be aware of (but not limited to) include claims that recipients have won contests, received a monetary prize, or are qualified for an award for filing for unemployment benefits.

5. Scams in Travel:

Scammers selling fraudulent COVID-19 travel insurance policies that claim to cover losses for any reason at no extra charge are new for 2020. Buyers learn the hard way that many policies do not give the coverage they anticipated. Travel insurance coverage does not cover claims resulting from "known, anticipated, or expected disasters, epidemics, government prohibitions, warnings, or travel advisories, or fear of travel."

Because COVID-19 is a pre-planned event, many travel insurance policies do not apply. Only a Cancel for Any Reason (CFAR) policy purchased directly from a licensed, reputable company will provide coverage for COVID-19-related losses. These policies are typically far more expensive than ordinary travel insurance coverage

Another type of travel scam involves the use of social media. Scammers use sites like Pinterest, Twitter, and Instagram to entice even the most seasoned travelers. You will be invited to either complete a survey filled with personal information or open your computer up to hidden dangerous malware after clicking the image, which draws clicks with the promise of a free trip or plane tickets.

Check to see if the social network account you're on is legitimate. All major airlines and travel sites provide direct links to their social media handles from their web pages.

Scams involving grandparents:

A fraudster appears as a scared grandchild in need of cash immediately away for some emergency—to get out of jail, escape a foreign nation, or pay a hospital bill—in grandmother scams. The COVID-19 pandemic has made convincing lies even simpler to sell: "COVID has landed me in the hospital. Please provide money as soon as possible."

Literature Review:

Rahul De', Neena Pandey**, and** Abhipsa Pal, (2020) study the Impact of digital surge during the Covid-19 pandemic: A viewpoint on research and practice the aut**h**or observed that Blockchain technology will become increasingly essential, necessitating design and regulatory studies. The number of contract workers and the sharing economy is anticipated to grow, generating concerns about job allocation, coordination, incentive, and elements of job strain and reduced absenteeism. Occupational surveillance and computer anxiety issues will become more prevalent with a rise in digital presence. Online scamming is predicted to increase, as is the study into security management. Monitoring of the internet, a critical resource, will be critical following the pandemic. Lockdowns in many countries have resulted in increased use of information systems and networks, as well as significant changes in usage habits and behavior. Employees are adjusting to new "normal" when meetings are conducted entirely online, office work is moved to the home, and new work patterns emerge. Most organizations, whether in industry, society, or government, have experienced these shifts. Changes have also arrived quickly, with little time for organizations and individuals to plan for, prepare for, and adopt new setups and arrangements; they have had to adjust, try, experiment, and find new ways that did not exist previously. Increasing digitalization, Work-from-home and gig workers, Workplace monitoring and technostress, Online fraud, Internet access and digital divide, Digital money. Further, the author concludes that we anticipate a significant shift in digital usage as a result of the Covid-19 pandemic, with implications for many sectors of business and life. How this transformation unfolds is mainly determined by our reactions to something and the shaping of emerging trends.

Ana Ferreira and Ricardo Cruz-Correia, (2020) study COVID - 19 and Cyber security: Finally, an Opportunity to Disrupt? The study investigates that COVID-19 has posed a challenge to cyber security to ensure the ultimate need of ensuring human privacy and security and health care and to raise awareness about the need for a paradigm shift in how cyber security is treated. As a result of the COVID-19 outbreak, there has been a considerable surge in fraudulent mail. These messages use misinformation, "fake news," fear, isolation, and a lack of awareness to make the limited population a vulnerable target for such attacks and induce victims to hand over money, personal information, and credentials (e.g., phishing, ransomware, bogus fundraising campaigns). Furthermore, when people are isolated, they are more prone to buy products online; as a result, attackers might use fraudulent product delivery alerts to their benefit. It's worth emphasizing that security data breaches that occurred during this period will not only be exploited today but

will also have a long-term impact, as exploitation will continue for a long time. Change is necessary, nevertheless, change is difficult to achieve

Cyber security knowledge and education are critical in any situation, especially during pandemics. However, today's times necessitate web-based, simple, quick, accurate, and objective information and education that is tailored and useful to the circumstance and context, and also to the target demographic. Humans are a crucial component and the main enablers of the amount of cyber security that each system may and will have because of the unpredictable nature of human cognitive behavior.

When properly given, education and information technology literacy are crucial; but, they are not a complete answer. Humans should seize this opportunity to address those issues before they add to the pandemic's toll. It is common in extreme situations to make exceptions to emphasize specific areas of society or infrastructure. This, however, must be done in a clear and controlled manner so that, after the extraordinary circumstance has passed, individuals can quickly reclaim their constitutionally protected right which has harmed far too many lives in the past. For a secure and healthy human population, we must also demand the right to trust technology, with more suitable and improved cyber security.

Scope of the Study:

This study would be undertaken to analyze in trust factor due to rising fraud during COVID 19 pandemic in the Mumbai region. Moreover, it would also help us to understand Different factors and methods of fraud that happened during the COVID 19 pandemic.

Research Methodology

Problems of the study:

The Study is on the trust factor due to rising fraud during this unprecedented crisis

Research objective:

1. The purpose of this study was to look at the trust factor during the COVID 19 pandemic.
2. To comprehend people's cognitive activity during the COVID 19 pandemic
3. To investigate public perceptions of digital payment fraud, scams, phishing emails, unemployment, and fraud vaccine.

Hypothesis:

H0= There is no significant difference in cognitive behavior in trust factors due to rising fraud before COVID19 and during the COVID 19 pandemic.

H1= There is a significant difference in cognitive behavior in trust factors due to rising fraud before COVID 19 and during the COVID 19 pandemic.

Research Design:

The present study is based on both primary and secondary data. The primary data were collected through a structured questionnaire from 50 respondents using Google form and secondary data was collected from different Journals, books, and government records. The collected samples using convenient sampling methods were validated and taken for further analysis. These collected data were analyzed with different statistical tools like correlation, mean, median, and paired T-test. Secondary data was collected from different Journals, books, and government records.

Area of the Study:

The sample data are randomly collected from Mumbai city and its suburban areas

Sample Technique:

A convenient sample (Non- Probability sampling method) of 50 consumers in the Mumbai region shared their information to the study and was requested to complete the questionnaire voluntarily. The study was done in December 2021.

Table - 1

Age, Gender, occupation, and Income wise Demographic Pattern of trust factor due to rising fraud during COVID 19 pandemic

Demographic Category of investor	Parameters	Number of Representatives	
		Total (50)	Percentage
Gender	Male	31	62%
	Female	19	38%
Age	up to 25 years	12	24%
	26 to 35 years	15	30%
	36 to 45 years	15	30%
	46 to 60 years	06	12%
	61 years and above	04	4%

Occupations (Employment)	Self-employed Professional	12	24%
	Entrepreneurs	05	10%
	Salaried employees	18	36%
	Student	15	30%
Annual Income	Up to 3 Lakhs P.A	25	50%
	Rs. 3 Lakhs to 6 Lakhs P.A.	12	24%
	Rs 7 Lakhs to 10 Lakhs P.A	10	20%
	10 Lakhs and above	03	6%

Interpretation:

Table 1 shows, 50 numbers of respondents, 38% of the respondents are female, 62% of the respondents are male. 24% of the respondents up to 25 years, and 30% of the respondents 26-35 years age group, 30% of the respondents 36-45 years and 12% of the respondents 46 – 60 years and above 61 years age group 4% respondents.

In our investigation we also found that 24% of the respondents are Self-employed professionals, 10% of the respondents are Entrepreneurs, 36% and 30% of the respondents are salaried employees and students.

In income parameter, we found that 50% of the responded Up to 3 Lakhs P.A and 24% responded from Rs. 3 Lakhs to 6 Lakhs P.A. group, 20% responded from Rs 7 Lakhs to 10 Lakhs P.A and more than 10 Lakh 6% responded.

Table - 2

t-Test: Paired Two Sample for Means		
	Before COVID -19	*During COVID -19*
Mean	96140	60200
Variance	18723959592	7649020408
Observations	50	50
Hypothesized Mean Difference	0	
df	49	
t Stat	3.257404919	
P(T<=t) one-tail	0.001022438	
t Critical one-tail	1.676550893	
P(T<=t) two-tail	0.002044876	
t Critical two-tail	2.009575237	

Significant at 5% (P0.05) -Accepted

Interpretation:

Table 2 shows, the p-value of the trust factor due to rising fraud during the COVID 19 pandemic was less than 0.05, therefore, our null hypothesis was rejected and the alternative hypothesis accepted. It may also be said that there is a significant difference in cognitive behavior in trust factors due to rising fraud before COVID 19 and during the COVID 19 pandemic.

Conclusion:

From the study it has been highlighted the numerous cyber security challenges related to COVID-19; but, none of the known challenges square measure new however has been exacerbated by the pandemic. Therefore, the issues existed before the pandemic, and still no adequate solutions measure on the market, modification, and disruption got to occur at the core of human-device interactions and relations, with a spotlight on trust and on however humans have thrived with one another over thousands of years, even in threatening things. We should take this chance to face those challenges before they pile on high of the pandemic toll. In extreme things, it's traditional that exceptions got to be created to place specific elements of society or infrastructures. However, this has to be accomplished in an exceedingly clear and controlled approach so when the exceptional scenario subsides, individuals will simply take back their basic right to privacy, the loss of that has affected such a big amount of lives within the past. We end to should additionally claim the proper trust in technology, with additional acceptable and improved cyber security, for a safer and healthier human population.

REFERENCES:

1. Ahmad, Tabrez, Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cyber security Available at SSRN: https://ssrn.com/abstract=3568830 or http://dx.doi.org/10.2139/ssrn.3568830.

2. Agarwal S., Sengupta D., Kulshrestha A., Anand S., Guha R. The Economic Times; 2017. Internet users to touch 420 million by June 2017: IAMAI report. https://economictimes.indiatimes.com/wealth/spend/how-to-disable-international-transactions-on-your-credit-card/articleshow/66375034.cms

3. Ferreira A, Cruz-Correia R. Cyber security in pandemic times: challenges and opportunities. 2020 Jul 21 Presented at 12th International Conference on e-Health;

4. John Waggoner and Andy Markowitz,Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Stimulus Payments, January 18, 2022

5. L. Rocher et al. Nature Commun. COVID-19 digital apps need due diligence - Nature Research, 10, 3069; 2019 https://media.nature.com/original/magazine-assets/d41586-020-01264-1/d41586-020-01264-1.pdf

6. Policy paper on COVID-19 vaccines and corruption risks, https://www.unodc.org/documents/corruption/COVID-19/Policy_paper_on_COVID-19_vaccines_and_corruption_risks.pdf

7. WHO reports fivefold increase in cyber attacks, urges vigilance, World Health Organization, https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

8. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic, figshare , May 12, 2020, https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792

9 aic.gov.au (04.05.2021): Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19, Reso; https://reso-infoportal.de/2021/05/04/aic-gov-au-04-05-2021-fraud-and-its-relationship-to-pandemics-and-economic-crises-from-spanish-flu-to-covid-19/

10 Effect of public corruption on the COVID-19 immunization progress; Nature News, December 06, 2021; https://www.nature.com/articles/s41598-021-02802-1