BioGecko

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

RATE OF CYBER CRIMES DURING COVID-19 IN INDIA: AN EMPIRICAL STUDY

Debalina Chatterjee
Ph.DResearch Scholar, SOA National Institute of Law, Siksha 'O' Anusandhan deemed to be University
Corresponding AuthorEmail: debalina340@gmail.com

Dr. Madhubrata Mohanty
Associate Professor, SOA National Institute of Law, Siksha 'O' Anusandhan deemed to be University

Dr. Jayadev Pati
Senior Professor, SOA National Institute of Law, Siksha 'O' Anusandhan deemed to be University

ABSTRACT
Cyber-crime is not a new issue in India. With technological advancement many shrewd and criminal minded individuals have ventured into the virtual world to commit crimes to make huge profits within short span of time by duping other people. It is also difficult to trace the cyber criminals. Cyber fraudsters operate at national and international level. So, it has become necessary to take adequate measures to address this issue. In this article doctrinal study has been done by using secondary data.This article analyses the increasing trends in cyber-crime in India amidst Covid-19 pandemic.Covid-19 has been used as a bait to dupe people. As the use of technology has increased manifold recently, so the menaces of misuse of internet have also increased. Cyber-crime has actually increased during lock down period due to unemployment and spending more time on social media. Many companies' system has been hacked. Cyber bulling and cyber stalking have also increased as people used their ample amount of time to do mischief on online platform as found out by various studies. This situation is new to everyone so these findings are relevant in the present context. Covid-19 pandemic effect is not limited to only socio-economic, health and human rights issues. It has had more impact on society, so this research is relevant to find out solutions to reduce cyber-crimes in a technologically advanced era by proper legal and administrative actions. The country is also going through financial crisis so this research is essential and novel as the results of this research will through some light on how pandemic has also become a cause behind increase in cybercrimes.

Keywords: Covid-19, Technology, Cyber-crime, Cyber criminals, Cyber fraudsters.

INTRODUCTION
Cybercrime is common to whole world. Cybercrime has become a major profitable illegal trade. In India the rate of cyber-crimes has been increasing during the past few years and this Covid-19 pandemic have added to this problem. Cybercrime is "a form of crime which is facilitated by using a computer or hardware device". Cybercrime includes phishing, online scams, cyber frauds, ransom ware attacks, insecure remote access to corporate networks, identity theft, cyber terrorism, cyber stalking, cyber bulling and harassment, etc. As the use of internet has increased a lot due to various reasons like work from home, online classes, online delivery of essential commodities etc., therefore the risk of cyber-crimes have also increased. The use of social medias has also increased as a result of which cybercriminals are getting ample opportunities to commit crimes. As most unemployed people are techs savvy and educated, so they can easily develop various hacking mechanisms to get access to important credentials and bank details of individuals. Once hackers get access to all bank details and important credentials they withdraw and use that money quickly to eliminate any kind of evidence.[1] Many people after being sacked from particular organizations are targeting the computer resources of those organizations and leaking important data. In 2019, cybercrime has been ranked by World Economic Forum among the five topmost risks around the globe. In 2015, at IBM Security Summit, IBM's chairman, opined cybercrime to be the major threat to almost all profession and companies around the world.[2]Employees who are

[1] Rennie Naidoo, A multi-level influence model of COVID-19 themed cybercrime, EUROPEAN JOURNALOF INFORMATION SYSTEMS 2020, VOL. 29, NO. 3, 306–321,(Mar.7,2022,5:30 P.M)

[2]Ibid

working from home must be aware of some cyber security measures failing which will lead to loss of money and important data. Education on work safety in cyberspace is lacking that's why individuals become exposed to phishing scams. The new-corona virus-themed links and pop ups to access latest information on covid-19 have duped many people during the last one year. Most of the websites regarding Covid-19are malicious and phishing scams. General public instead of being aware of such malicious websites are tricked to access those links after which important data become exposed which results in financial loss of the victims. Covid 19 and WHO related links are increasing cloned by cyber criminals nowadays which have escalated the rate of cybercrimes.[3] As technology encompasses almost every part of our lives so there is always a threat looming in cyberspace. So, in order to bolster cyber security for overall development of the country permanent solution is required. In spite of so many legislative provisions India is not able to reduce cyber-crimes. The previous literature reveals that study relating to cyber-crimes has been done at national and international level but still the risks in cyberspace cannot be mitigated. The pandemic has introduced more challenges and there lacks a grey area for exploring the reasons behind rise in cyber-attacks during pandemic. In this digital world where work from home has become a necessity it has become crucial to adopt essential measures to improve security in cyberspace.

Methodology

Doctrinal method is used in this paper to find out the drawbacks in cyber security in India which has increased the rate of cybercrimes during Covid-19 in India.In doctrinal research the researcher is concerned with books, articles, documents, rather than field study. In doctrinal research much importance is given to historical analysis of the subject of research so as to make the researcher comfortable with the area of research. It is the highly accepted form of research that gives least importance to field work in comparison to references from library and published articles which mostly satisfy the requirements of the study. The doctrinal study is justified by appropriate data from secondary sources. Descriptive-analytic method of study is being used in this paper to analyse the present menaces of cybercrime and to put forward some suggestive measures.

Rise of cybercrimes during Covid-19 in India

Cybercrime is essentially technological in nature but it also has a human componentalso as social engineering theory is used to trick individuals to break the “human firewall” i.e. to exploit human vulnerabilities by manipulating end users in disclosing confidential information. Cybercriminals impersonate social media accounts and mimic email accounts to target the victims. Individuals relying on the person or the organization being impersonated are most likely to comply with the instructions given by cyber criminals. For instance, some fraudsters send message to update Know Your Customer (KYC) related to mobile number which seems to be an authentic message once the link is opened that link leads to a page to make mobile recharge once the recharge process is initiated money automatically get deducted from the victim's account. This is one form of online fraud. During Covid-19 criminals have been motivated by the sudden and abrupt situational changes, the sudden discourse to remote working mode, rising unemployment, increase in online shopping, increase in online banking, need for leisure and entertainment, increase in the availability of relief funds, etc. Cybercriminals are increasingly targeting vulnerable people by social networking services as a result SNS scams have become very common nowadays. Top organizations like SNS, banks, IT firms, Government agencies and inter-governmental agencies have been targeted by cyber criminals. Many new domains have been registered to take advantage of COVID-19 situation. Approximately 43,000 new domains relating toCovid-19 sites have been registered from March 28 to April 20. Although many of these sites are legitimate, but there are an equally higher number of fraudulent sites.

Some suspicious domains are-

“whatkillscovid19.com;usacaresfundcovid19.com;windowcleaningcovid19.com”[4].

According to Delhi police data, cyber crime has increased during lockdown in 2020, for instance, “in January 2020, the numbers of reported cyber crime cases were 1,480 as against 4,188 cases in May, 3,372 in April, 3,239 in June, and 4,103 in July, 2020. According to the Delhi Police, a substantial increase in the rates of cyber crimes was there in Delhi

[3] Prof. (Dr.) Tabrez Ahmad, Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cyber security, SSRN Electronic Journal,(Mar.7,2022,7:30 P.M),DOI:10.2139/ssrn.3568830

during the lockdown period, like around 135 cyber crime related offences were recorded every day in May", based on an analysis of nearly about 33,000 cases filed up to November 2020[4].

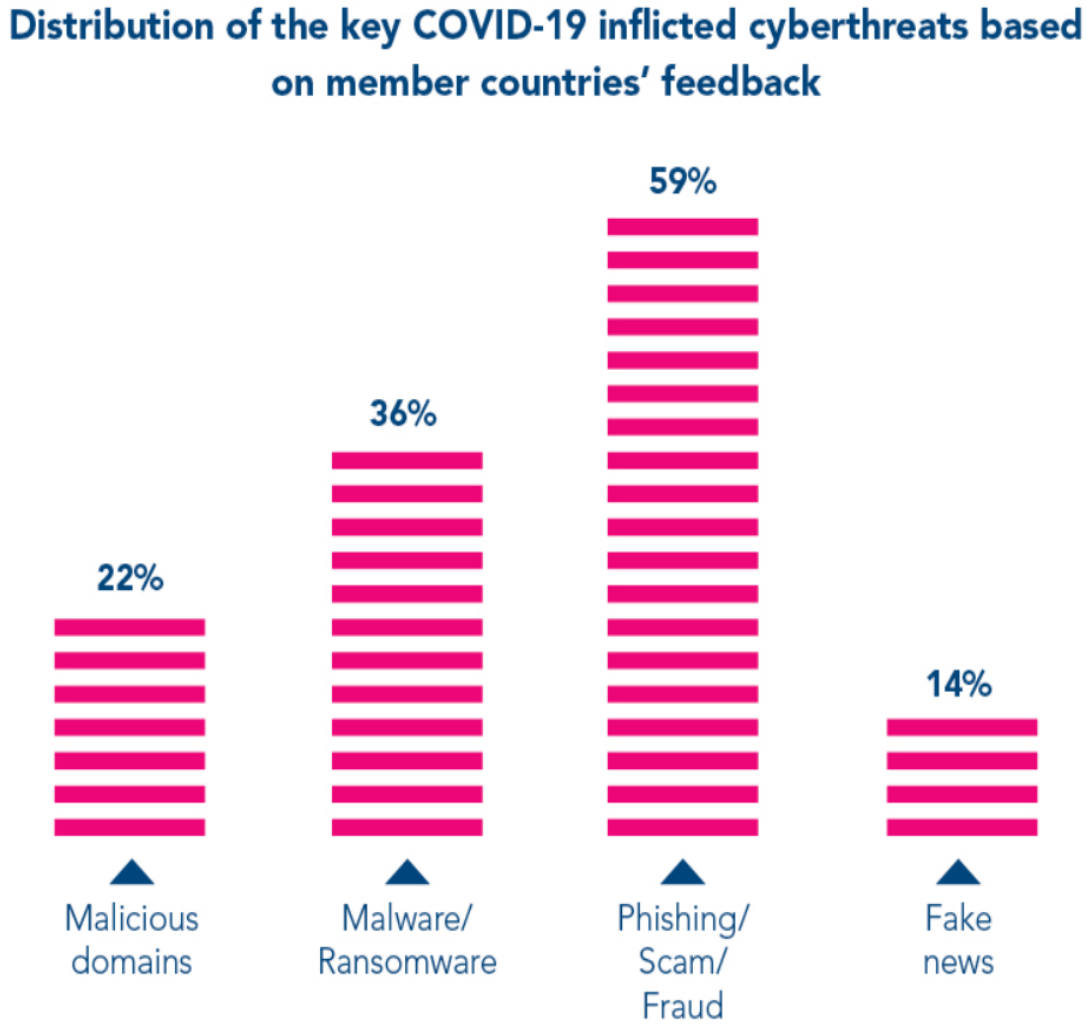

Figure 1

source: interpol report showing alarming rate of cyberattacks during covid-19

[4] Shiv Sunny, Cyber crime cases went up during lockdown, shows Delhi police data, Hindustan Times, New Delhi ,(Mar.8,2022,9:30 A.M)

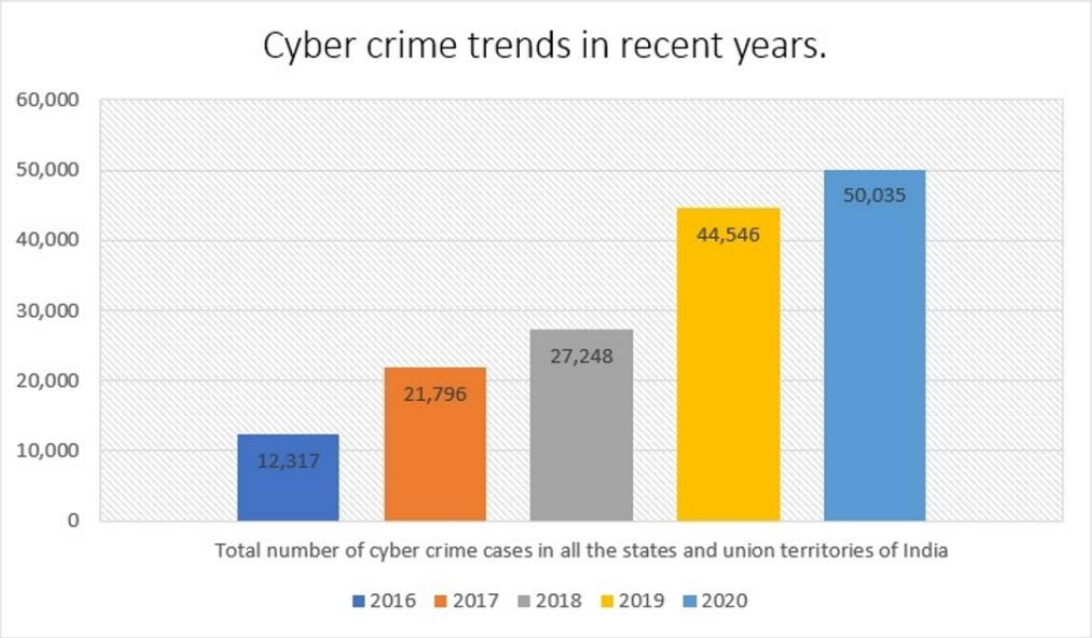

Figure 2: Showing last five years total number of cybercrime cases reported in India

Source: Crimes in India (National Crime Records Bureau) Volume II of years 2016, 2017, 2018,2019 and 2020.

Total number of cases reported for different cybercrimes in India	**2017**	**2018**	**2019**	**2020**
OTP FRAUDS	390	319	549	1093
ONLINE BANKING FRAUDS	804	968	2093	4047
CYBER BULLYING/ CYBER STALKING	542	739	777	872
RANSOMEWARE ATTACKS	300	1218	1023	727

Table 1

Source: Crimes in India (National Crime Records Bureau) Volume II of years 2017, 2018,2019 and 2020.

From Figure 1 it is clear that malicious domains, phishing scams, malware attacks during Covid 19 pandemic have increased. In figure 2 it is seen that cybercrimes have increased every year in India. The maximum rise is seen in the year 2019 and then in 2020.As data about 2021 is not available now so the analysis is done by comparing the figure of 2020 with other years. As this study is concerned with the recent trends in cybercrimes especially during pandemic so the reasons behind the rise in cyber attacks in 2020 is discussed herein. We have taken four main issues in cyberspace during pandemic i.e., One Time Password (OTP) fraud, online banking fraud, cyber bullying/ cyber stalking and ransom ware attacks. It is found that in 2020 OTP frauds, online banking frauds and cyber bulling/ cyber stalking have risen however according to NCRB data only ransom ware attacks have decreased in 2020. Cyber fraudsters have mainly resorted to OTP frauds and Online banking frauds during the pandemic.

As human viruses are communicable likewise computer viruses are communicable. Once a computer virus like Trojan horse (a malicious software) enters into another computer system it disrupt, damage, steal and inflict harmful action on the data or network of another computer. COVID-19 is used as a lure to deceive employees and customers. More infected personal computers and phones are likely to result from this. Those who download applications relating to

corona virus are also fooled into downloading ransom ware appearing as legitimate apps. The main motive behind Covid-19-related cyber crimes, is to commit cyber theft of personal details, compel the installation of malevolent software, commit fraud, or pursue illegitimate benefits[5].

It is interesting to note that pandemic has also increased the susceptibility of cyber bullying. Cyber bullying refers to any behavior which shows hatred and denigration by making use of ICT so as to cause trouble and disgust to someone.As social life has been halted by the pandemic the use of social media increased manifold to interact with friends, relatives and strangers online. As people have been isolated during the pandemic, it made them more vulnerable to cyber bullying. Apart from that, for most of the people social media is the only mode of communication in the present scenario so people have been constantly sharing new achievements they accomplished during the pandemic and expressing various viewpoints more than ever. Naturally when people become open to more and more online content and carry most of their formal and informal interactions through social media platforms, it is critical to regulate their behavior because they are more prone to hateful comments and acts. Both the perpetrator and the victim is unaware of the dangers and consequences of their online actions. Cyber bullying is a consequence of rising tension of individuals and malice of cyber attackers. Cyber bullying is increasingly affecting the teenagers and young adults which is leading to suicidal ideation. This pandemic has also increased incidents of cyber stalking which disturbs the victims mentally. Cyber stalking is one of the most common form of cyber bullying which is usually followed by posting of denigrating comments, leaking of obscene pictures and videos of victims and harassing the victims[6]. Cyber stalking is the use of internet for the purpose of stalking and harassing individuals and organizations. The hike in using social platforms by adults and teenagers during the pandemic has subsequently increased cyber crimes. The young people are mostly targeted.Women are found to be more prone to become victims of cyber stalking in comparison to men.[7]Thus, in short Covid-19 has widened the scope and diversity of many forms of cybercrimes and has made education on cyber security essential for everyone.

Legislative provisions to deal with cybercrime in India

The Information Technology (Amendment) Act, 2008 deals with cybercrimes in India. Some of the Sections of the IT Act dealing with cybercrimes are: -

Section 66B of this Act penalizes dishonest receipt of stolen computer resource or communication device with imprisonment for a term of three years or with fine of one lakh rupees or with both. Section 66C penalizes for identity theft that includes elements of both fraud and theft. As such one accused of committing such offense is not only penalized by the aforementioned provision of the IT Act, but also as per the provisions of forgery under the Indian Penal Code. Section 66 D provides punishment for cheating by impersonation through computer resources.The penal provision for cyber terrorism is provided under section 66F of the Act and Section 67 provides punishment for publishing or circulating obscene material in electronic form[8]. Section 354 D of the IPC provides for the punishment of stalking. There are other sections of IT Act and IPC which provides protection against cybercrimes.

In a case, the accused by making a false Face book profile of a minor girl aged 15 years uploaded some scandalous pictures besides her name & also posted certain offensive remarks against her. This caused severe mental stress to the minor resulting serious degradation in her academic progress. The trial court did not allow the application moved by the accused for bail & on appeal the Gauhati High Court too took stringent view in the line of the trial court rejecting the bail application[9].

Prakhar Sharma v. State of Madhya Pradesh is another such case where the accused by making a false account of the victim in the Face book posted some obscene messages along with the photographs of the victim displaying as if itwere made from the victim's original account.[10]The accused was prosecuted under sections66(c), 67, and 67(a) of the IT Act and the Madhya Pradesh High Court denied the grant of bail to the accused.

Cyber cells were established with a view to offer remedy to the victims of cyber crimes. If there is no cyber cell near the place of residence of the victim then FIR can be filed by the victim in a local police station. Other redressal

[5] Adv Purva Saini, Cyber Crime during COVID-19,International Journal of Science and Research (IJSR)ISSN: 2319-7064,(Mar.8,2022, 06:00 P.M)

[6]Ojasvi Jain et.al,Has the COVID-19 pandemic affected the susceptibility to cyber bullying in India?, Computers in Human Behavior Reports 2 (2020)100029,(Mar.9,2022, 04:00 P.M)

[7] Amrita Prasad, Beware! Cyber stalking is on the rise during the pandemic,(Mar.9,2022, 04:30 P.M),

[8] The Information Technology (Amendment) Act, 2008.

[9]Sazzadur Rehman v. State of Assam, Criminal Petition No. 654 of 2019

[10] Prakhar Sharma v. State of Madhya Pradesh, MCRC No. 377 of 2018.

mechanisms are online grievance redressal and report to the website. Women who hesitate to file a complaint at the police station can lodge a complaint against cybercrime at the National Commission for Women. The Information Technology Amendment Act of 2008, has designated the Computer Emergency Response Team (CERT-IN) as the nodal entity at national level to address computer security related issues.In spite of all these laws cyber crime cannot be tackled amid this pandemic. Delhi Police has issued guidelines on cybercrime threat during pandemic. People must be careful and cross check before login into any website as majority of the websites are malicious and engaged in phishing. The Delhi Police has recommended people to think rationally before opening a link which seems to be from the World Health Organization (WHO) or a tempting website containing information on the cure ofCovid-19.[11] Advisories of Delhi Police which have been issued in view of rising online frauds ask not to share one's password with anyone as under no circumstances there will be a need to know such personal information. Public must not assume that WHO or any other agency holds lotteries or sends out prizes, grants, or certificates via emaill.[12]

Suggestions

1. The cyber security policy of organizations must be updated so as to include remote working within its ambit. The policy must be adequate to provide safe working environment to people who are working from home. Remote-working access control, the use of personal computers, and updated data protection considerations for workers accessing vital documents and other company information are some of the necessary measures to ensure cyber security. Using VPN solution with encrypted network connection can be useful in providing safer access to internet resources to the employees.
2. Additional security to the applications by enabling multi-factor authentication can be helpful.
3. Remote workers can keep their home computers, printers, phones, and other gadgets secured by updating their operating systems and downloading the new anti-spam, anti-spyware, and anti-virus software. IT divisions should take the initiative to install anti-malware and anti-phishing software on their employees' personal computers to protect them from malicious emails and payloads.
4. Employees and general public must be made aware of the modus operandi of the cybercrime so that they become conscious about any eminent danger to their device and avoid opening those links. Employees must work carefully at home so that nonfamily member or visitors get to know important details of the company.
5. It is necessary to spread awareness by Government authorities, parents and psychologists, about the effects of cyber bullying and cyber stalking so that the number of such cases can be lessened. The victims should be supported and encouraged to report these cases to proper authorities without delay. Public awareness programme on precautions that should be taken to avoid cyber fraud is also need of the hour. Sometimes little carelessness costs a lot.
6. Local democratic cyber policing can help in curtailing cyber crimes. As the public become more vulnerable to cybercrime threats due to the pandemic, it is important to provide clarification about the role of police in reacting to and preventing cybercrime. The pandemic provides an incentive for local police departments to think outside the box when it comes to cybercrime prevention.
7. India must by appropriate mechanism publish home working guide for employees for organizations introducing home working and shall also provide for tips for identifying phishing emails as published by UK government's National Cyber Security Centre.

Conclusion

It is inferred from the available data that cybercrimes have increased indeed during the pandemic. OTP frauds and online banking frauds are the main causes behind so much economic losses during pandemic. The Covid-19pandemic creates a suitable climate for economic crimes by cyber criminals. Appropriate authorities have also emphasized the importance of bringing these crimes to the attention of financial institutions and the general public, so as to activate knowledge sharing between the public and private sectors both within and outside the country. As people ought to adhere to some health guidelines in order to defeatCovid-19 likewise people must be well aware of the hazards in cyberspace and must take adequate measures to keep their devices and bank accounts safe and secure. A more secured virtual environment will help us to efficiently handle the challenges that we are facing during the pandemic, as well as

[11] Prof. (Dr.) Tabrez Ahmad, Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cyber security, SSRN Electronic Journal,(Mar.10,2022, 02:30 P.M),DOI:10.2139/ssrn.3568830

[12] Priya Adlakha and Kiratraj Sadana,India: Cyber Crime During Corona virus Pandemic,mondaq,(Mar.10,2022,4:45 P.M),https://www.mondaq.com/india/operational-impacts-and-strategy/921026/cyber-crime-during-corona virus-pandemic

new challenges that we will face in the post-pandemic age. This article leaves scope for further research. Further the reasons sudden leap in the rate of cybercrimes in the year 2019 also need to be explored so that after knowing the reasons effective control measures can be undertaken.