ORIGINAL ARTICLE

# A Study to Find the Encounter and Awareness of Cybercrimes among People During Lockdown in Gurgaon Region of Haryana

**Kumari R,[1] Narwal S.[2]**

Research Scholar,[1] Student.[2]
1,2. GD Goenka University, Gurugram.

## Abstract:

With the COVID-19 and subsequent lockdowns, the dependency of people on the internet increased a lot for all needs. The cyber criminals perceived this opportunity to benefit themselves. People during lockdown came across the cyber-attacks in the form of phishing, cyberbullying, email frauds, fake medicine or related websites, zoom bombing, fake information etc. This survey was conducted in the regions of Gurgaon, Haryana to find the awareness of people and the encounter of cyber activities during the lockdown. It was found that people did come across cyber activities and some became victims too. Though most people do have some awareness of cyber-crimes but still most of them have incomplete awareness or unaware of the same. Most people did not report cyber-crimes to the police. It is important that the government must take steps to find the vulnerability of cybercrimes among people and spread relevant awareness among them.

**Keywords:** Cybercrime; COVID-19; Lockdown; Awareness; Phishing; Frauds.

## Introduction:

From 24 March, 2020, the govt. of India announced a complete lockdown throughout the country in order to contain the spread of Coronavirus in the country. Only the essential services were allowed to operate, causing other activities to a standstill, which hardly affected the nation's economy. In India, the areas in a district were divided into various zones of red, orange and green depending upon the cases and hence the restrictions decreasing respectively. The lockdown forced people to be contained inside their houses and people got more engaged with mobile and internet for each and every utility. This long period of lockdown had though might have reduced the number of street crimes but had paved the way to increased various other crimes like domestic violence and threat to cyber-crimes. The motivation of crime depends upon the benefits and costs of committing[1] and the imposition of lockdown has impacted the motivation of criminals leading to change in the course of crime type and commission. The cyber space in such a period became one of the easiest platforms for the criminals to explore various forms of crimes online. It is important to understand the nature of crime and its location while analyzing the implications of lockdown on crime.[2] The lockdown had increased the opportunities for cyber criminals to exploit the fear and anxiety of people to make money using various cyber- attacks such as malware, spyware, ransomware, counterfeited medical equipment and drugs sponsored through emails, fake crowd funding mails and even fake investments opportunities. The concern of pornography, drug trafficking etc. are also important to vulnerable group like children/students who were shifted to internet for online education, games etc.[3] Hence, the majority of cyber-crimes has been classified as-fake agencies/websites for supplying medicinal equipment like PPE kits, face masks, medicine, oxygen cylinders etc., Phishing (getting hold of the account details), creating fake social accounts or influential people, pornography etc. Cyber-crime does not spare influential people also. As per The Indian Express, a merchant navy officer of Indore received a mail regarding refund of his custody duty but he was asked to pay 62 lakhs rupees as the processing fee. He paid the sum also but did not get the refund. Such financial frauds became common during lockdown. Various officers from Bihar had reported the case to police. It has been reported that the use of e-wallets for various digital transactions increased by 44% and hence the cyber-attacks increased by 86% between March and April, 2020.[4] The increased dependency of internet during lockdown for each and every need from purchase to education to entertainment had paved the way for various cyber-crime activities like the use of spyware and ransomware by the crime opportunist to steal and take control of the vital information of the people.[5] Figure 1 shows increase in cyber-attack during 2019-2020 period. Almost everything went online i.e. even the court, govt. offices, medical consultations, United Nations meetings etc. The immediate shift to digital platforms had paved a difficult way to people who were unaware of these technologies and this could also cause vulnerability for these people to get into the cyber trap. Also, due to lack of awareness among people about cyber- crime, how to deal with these crimes, data theft, misuse of digital platforms etc. the cyber-crime boomed during lockdown. Various common types of cyber-crimes encountered during lockdown are phishing, zoom bombing or online abuse, ransomware etc. In a phishing cyber-attack, the attacker contacts a person through a mail, mobile or SMS posing itself as a legitimate source and thereby takes away sensitive and private data from the victim. As per K7 computing's report, Kerala posed the highest number of phishing attacks during the pandemic

**Corresponding Author**
**Dr. Ruby Kumari**
Email- rubyraut18@gmail.com
Mobile No.: +91 8447824956

**Article History**
DOR : 14.07.2022 DOA : 29.03.2023

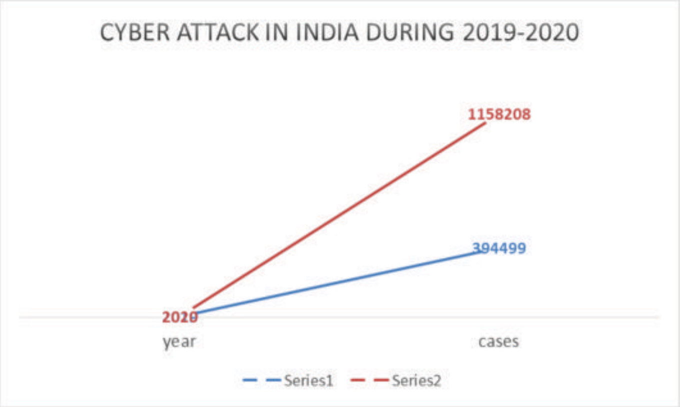
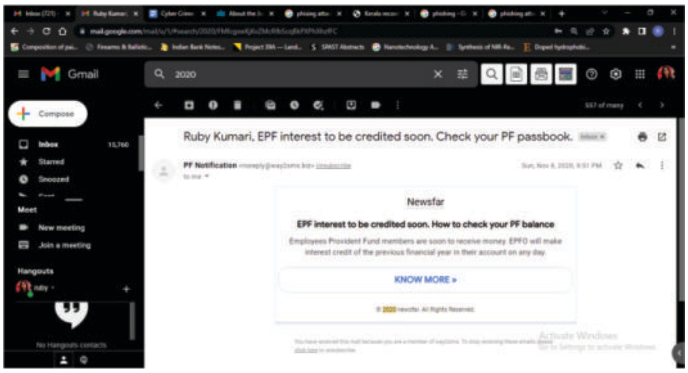


**Figure 1. Increase in Cyber-attacks in India during 2019-20. Source : Ubaid. S, 2020, Cybercrime in India: A Review.**



Ruby Kumari, EPF interest to be credited soon. Check your PF passbook.

PF Notification

Newsfar

EPF interest to be credited soon. How to check your PF balance

Employees Provident Fund members are soon to receive money. EPFO will make interest credit of the previous financial year in their account on any day.

KNOW MORE »

© 2020 newsfar. All Rights Reserved.

**Figure 2. EPF (Employee Provident Fund) mail luring the person to get into a phishing attack.**

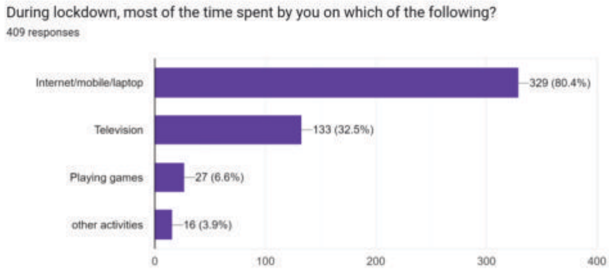


**Figure 3. Time spent by people in various activities during lockdown.**

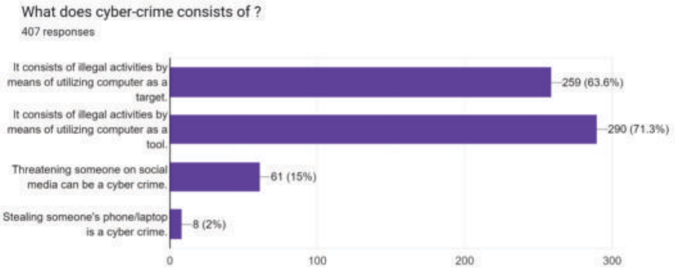


**Figure 4. Understanding of people about the definition of cybercrime.**

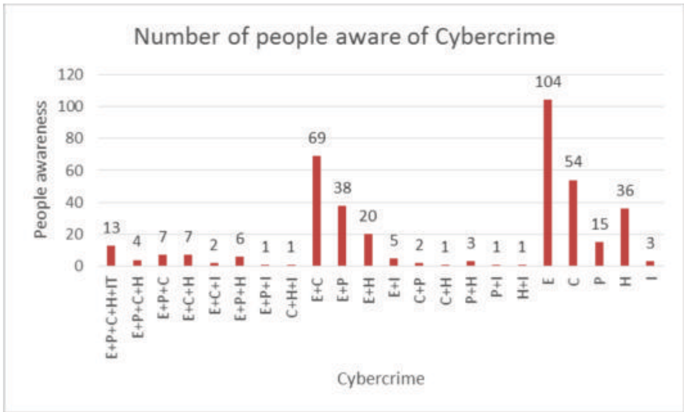


**Figure 5. Showing awareness of various types of cybercrimes among people.**

| | |
|---|---|
| E+P+C+H+IT | Email fraud+Phishing+cyberbullying+hacking+Identity theft |
| E+P+C+H | Email fraud+Phishing+cyberbullying+hacking |
| E+P+C | Email fraud+Phishing+cyberbullying |
| E+C+H | Email fraud+Cyberbullying+hacking |
| E+C+I | Email fraud+cyberbullying+Identity theft |
| E+P+H | Email fraud+Phishing+hacking |
| E+P+I | Email fraud+Phishing+Identity theft |
| C+H+I | Cyberbullying+Hacking+Identity theft |
| E+C | Email Frauds+Cyberbullying |
| E+P | Email Frauds+Phishing |
| E+H | Email Frauds+Hacking |
| E+I | Email Frauds+Identity Theft |
| C+P | Cyberbullying+Phishing |
| C+H | Cyberbullying+Hacking |
| P+H | Phishing+Hacking |
| P+I | Phishing+Identity Theft |
| H+I | Hacking+Identity Theft |
| E | Email Frauds |
| C | Cyberbullying |
| P | Phishing |
| H | Hacking |
| I | Identity Theft |

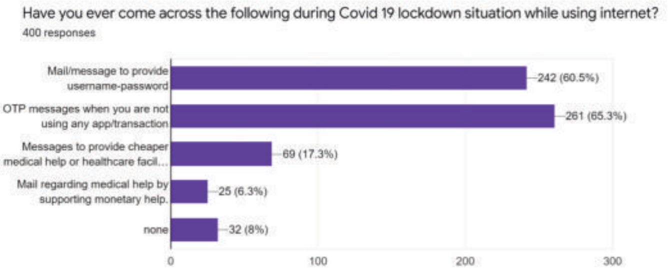


**Figure 6. Cyber activities faced by people during lockdown.**

period from Feb-April 2020 followed by Punjab and Tamil Nadu with 207 and 184 cases respectively.[6] During this period, these attacks were in the guise of famous organizations such as the World Health Organization, Center of Disease Control & Prevention etc. Figure 2 shows a screenshot of the author's Gmail. Mail seems to be from a legitimate source EPF and given the link to know more. It might be possible such links can get away useful information from the user if one clicks it. Another important surge was in zoom bombing/online abuse. There has been incidents of zoom bombing during pandemic where the cyber attackers entered the online classrooms/meeting and disturbed/abuse people in the form of verbal abuse or display/acting of indecent images/acts.[7,8] There was a case of the same by the CEO of 'The Information' Jessica Lessin who shared the zoom bombing experience, which is shown depicted in the picture taken from twitter, which shows how someone intruded into a video call and started sharing objectionable content like pornography.[9] Ransomware is a malicious software, which takes the control of a computer system/server denying the access to the user and demanding ransom in place of the restoration of data. IT companies like cognizant got infected by maze ransomware. Some firms had to pay huge ransom for clicking some malicious link, which could download the ransomware. World Health Organization even gave warning to stay away from the fraudsters imitating their employees to prevent such cyber-attacks.[10] The pandemic/lockdown has also affected the susceptibility of cyberbullying.[11] The case of Bois Locker room in Gurugram where a 17-year-old boy committed suicide because of the allegations by a girl after sharing the images of instagram group of bois locker room.[12] Apart from these cyber activities, fraud portals related to COVID 19 related information were launched by the cyber attackers. For example, websites related to the PM CARES fund. Around 4000 fraud portals were created by cybercriminals. In context to the increasing rise of cyber-crimes during COVID-19 lockdown, this paper elaborates the result of a survey conducted from the people of Gurgaon, Haryana in order to understand whether the people became victims of any cyber activities/crime, awareness about the same and any legal conscience related to cyber-crime. This study would help to understand the people's awareness about cybercrime as everything shifts towards online/digital platforms. Because it is very important to be aware of the cons of using the internet or one must be careful enough to safely use the internet. If people are not well aware about the cyber-crime, then the government/various organizations must step up to arrange the awareness camp or introduce compulsory academic courses for the students because nowadays every person from a small labor to high profile is a click away from being the victim of cyber-crimes.

## Material and methods:

This study is a survey-based analysis of encounter/information of cyber-crimes faced by people during the pandemic period. For this study, the Gurgaon (India) city was selected to collect the responses. The participants belonged to the age of 18 years or above. For the survey, questionnaire was prepared on certain parameters related to cyber-crimes and pandemic using google forms and was circulated among the people. Around 410 responses were collected. After assessing the responses, the result was presented through charts and graphs.

## Results:

The aim of this study was to understand the vulnerability of cyber-crimes during lockdown in Gurgaon region as well as the awareness of the cyber-crimes in people if they are caught with any type of cyber-crimes. From the survey responses, it was observed that most of the participants were from the age group of 18 to 39 years. As explained earlier that during the lockdown period, people were spending much of their time online in different activities. It was observed from the survey that most of the people, around 80% of the responses were involved in internet related activities followed by watching television and other activities as shown in figure 3. Although, most of the people were aware of the cyber-crime but, as per responses none of them were entirely aware of the same. Though, most of the people know that it consists of illegal activities by means of utilizing computers as target as well as computer as tool but rarely they know that stealing someone's phone/laptop or threatening someone on social media are also under the purview of cyber-crimes as shown in figure 4. Figure 5 shows various types of cyber-crimes and their awareness in people. People are mostly aware of Email frauds. It was observed that people also faced cyber activities during lockdown. The activities where people were communicated through mail to provide username or password and OTP verification were very common as shown in figure 6. One important thing observed was that most of the people did not report any type of cyber- crime to the police. In context to safe browsing of the internet, people were mostly neutral about the safety issues.

## Discussion:

The majority of the people were young in the survey, which indicates the relevance of this study as most of the people in this age group use various digital platforms for their use. The increase in the online activities during the lockdown period were also due to the shift towards digital lifestyle such as work from home and online classes for the working and students respectively combined with the social media activities, the result also affirms the same. IT Act 2000 encompasses various provisions for such offenses and their penalties too. During COVID period around 39% of the participants became the victim of cybercrime. Some people are not aware if they faced the cyber-crime or not. People not reporting the incident of cyber- crime to the police may be due to lack of awareness about the legal aspects of cyber-crime among people. People were also not much worried about the safe browsing of internet, which might be due to unawareness of the nuances of cyber threats while using the internet. Hence, it is important that people should be provided awareness about the crimes and their cyber modifications for the safe and fear free use of the internet.

**Conclusion and Limitations:** Cybercrime is one of the most dynamic crimes, which are beyond any physical boundaries or any circumference. Mere computer/mobile, target, internet and intention are the prerequisites for commission of crime. People during the lockdown were scared, nervous and totally became dependent on the internet for all sorts of requirements from entertainment to business and transactions. These opportunities were completely utilized by cyber criminals to deceive and earn money or other kinds of satisfaction. Such crimes are initially difficult to understand and victims rarely know that it could be reported to law enforcement agencies regarding the crime. People did come across various cyber activities and various reports show they became victims of the cyber-crime. Hence, it is important that basic understanding or awareness of such crimes must be taught to people. The government must step up in this regard and the academic institutions must introduce basic courses of cyber-crime or security to the curriculum. This survey though has some limitations as the number of respondents could be increased and some more aspects of cybercrimes, their legal implications, measures etc. could be extended in the questionnaire. Such surveys could also be focused on a particular cohorts like doctors, teachers, and businessmen etc. to understand more vulnerabilities of cyber-crime.

**Ethical Clearance:** NA (No Human samples were involved)

**Conflict of Interest:** None

**Source of funding:** None

**References:**

1. Becker GS. Crime and Punishment: An Economic Approach. Journal of Political Economy [Internet]. 2021 Mar [cited 2022 Mar 24];76(2):169–217. Available from: https://www.nber.org/system/files/chapters/c3625/c3625.pdf
2. Poblete-Cazenave R. The Impact of Lockdowns on Crime and Violence against Women – Evidence from India. SSRN Electronic Journal [Internet]. 2020 Jun 8 [cited 2022 Jun 20]; Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3623331
3. Radoini A. Cyber-crime during the COVID-19 Pandemic. Freedom from Fear [Internet]. 2020 Oct 14 [cited 2022 May 14];2020(16):6–10. Available from: https://www.un-ilibrary.org/content/journals/25190709/2020/16/2
4. Undale S, Kulkarni A, Patil H. Perceived eWallet security: impact of COVID-19 pandemic. Vilakshan - XIMB Journal of Management [Internet]. 2020 Nov 30 [cited 2022 May 25];18(1):89–104. Available from: https://www.emerald.com/insight/content/doi/10.1108/XJM-07-2020-0022/full/html
5. Kumar S, Manhas A. Cyber Crimes In India: Trends And Prevention. Galaxy International Interdisciplinary Research Journal (Giirj) [Internet]. [Cited 2022 Apr 29];9 (5):363–70. Available from: https://www.researchgate.net/publication/351902133_CYBER_CRIMES_IN_INDIA_TRENDS_AND_PREVENTION
6. Bureau O. Kerala records highest number of cyber crimes in lockdown time: K7 Computing's Cyber Threat Report □ [Internet]. https://www.thehindubusinessline.com/info-tech/kerala-records-highest-number-of-cyber-crimes-in-lockdown-time-k7-computings-cyber-threat-report/article31639411.ece. The Hindu; 2021 [cited 2022 Apr 20]. Available from: https://www.thehindubusinessline.com/info-tech/kerala-records-highest-number-of-cyber-crimes-in-lockdown-time-k7-computings-cyber-threat-report/article31639411.ece
7. Upadhyay NK, Rathee M. Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. Medicine, Law & Society [Internet]. 2022 Apr 26 [cited 2022 Jun 30];15(1):89–106. Available from: https://journals.um.si/index.php/medicine/article/view/1885
8. Som S, Bhattacharya S, Roy P. Crime and Pandemic Hidden face of COVID 19. Food and Scientific Reports [Internet]. 2020 Oct 8 [cited 2022 Apr 26];1(10):31–6. Available from: https://www.researchgate.net/publication/344534136_Crime_and_Pandemic_Hidden_face_of_COVID_19
9. Lessin J. Our video call was just attacked by someone who kept sharing pornography + switching between different user accounts so we could not block them. Stay tuned for next steps. And I am sorry to everyone who experienced. We shut down as soon as we could. [Internet]. 2020 [cited 2022 Mar 22]. Available from: https://twitter.com/Jessicalessin/status/1241087064134660096?ref_src=twsrc%5Etfw%7Ctwcam%20p%5Etweetembed%7Ctwterm%5E1241087064134660096%7Ctwgr%5E%7Ctwcon%5Es1_&ref%20_url=https%3A%2F%2Fembedly.forbes.com%2Fwidgets%2Fmedia.html%3Ftype%3Dtext2Fht%20mlkey%3D3ce26dc7e3454db5820ba084d28b4935schema%3Dtwitterurl%3Dhttps3A%2F%2Ft%20witter.com%2Fjessicalessin%2Fstatus%2F1241087064134660096image%3Dhttps3A%2F%2Fi.%20embed.ly%2F1%2Fimage3Furl3Dhttps253A.
10. Bhagtani H, Roj S, Raj K. Criminal Psychology and Impact of Recent Global Pandemic: Analysis of Criminal Mind with a Sudden Surge in Crime Rate. Palarch's Journal of Archaeology of Egypt/Egyptology [Internet]. 2020 [cited 2022 May 22];17(7):10801–28. Available from: https://archives.palarch.nl/index.php/jae/article/view/2759
11. Jain O, Gupta M, Satam S, Panda S. Has the COVID-19 pandemic affected the susceptibility to cyberbullying in India? Computers in Human Behavior Reports [Internet]. 2020 Aug [cited 2022 May 16];2:100029. Available from: https://www.sciencedirect.com/science/article/pii/S2451958820300294
12. Khan N. Bois Locker Room probe: Minor Girl Created Fake Profile to Test boy's character, Say Delhi Police. mirrornownewscom [Internet]. 2020 May 11 [cited 2022 Jun 20]; Available from: https://www.timesnownews.com/mirror-now/crime/article/new-twist-in-bois-locker-room-case-juvenile-girl-created-fake-profile-to-test-boys-say-delhi-police/589894
13. Ubaid S. Increasing Cybercrime in Rural India Syed. 2022 May [cited 2022 Jun 11]; Available from: https://www.researchgate.net/publication/360223028_Increasing_Cybercrime_in_Rural_India