CYBER CRIME DURING COVID-19 AND IT IMPACT ON ADOLESCENTS IN INDIA

***Vartika Saxena*[1]**
Research Scholar, Amity Law School, Amity University Madhya Pradesh, Gwalior
8103032177
***Prof (Dr) Rakhi Singh Chouhan*[2]**
Deputy Director, Amity Law School, Amity University Madhya Pradesh

Abstract:
The internet has evolved into a new form of life as a result of the development of new technology and communication methods. Nowadays, information technology is a critical tool utilized by practically every kind of firm. Cybercrime is rising quickly as a result of COVID-19. A cybercriminal can quickly compromise, delete, or disseminate malware from any website or gateway. The coronavirus-causing illness known as Covid-19 is afflicted. Because businesses, governments, and people all depend on it. These days, everything that needs to be done is done digitally. Our online lives are also impacted. Crimes in the modern day go beyond simple physical assault and mental torment. The internet has evolved into a new form of life as a result of the development of new technology and communication methods. Nowadays, information technology is a critical tool utilized by practically every kind of firm. Cybercrime is rising quickly as a result of COVID-19. A cybercriminal can quickly compromise, delete, or disseminate malware from any website or gateway. The coronavirus-causing illness known as Covid-19 is afflicted. Because businesses, governments, and people all depend on it. These days, everything that needs to be done is done digitally. Our online lives are also impacted. Crimes in the modern day go beyond simple physical assault and mental torment. The internet has evolved into a new form of life as a result of the development of new technology and communication methods. Nowadays, information technology is a critical tool utilized by practically every kind of firm. Cybercrime is rising quickly as a result of COVID-19. A cybercriminal can quickly compromise, delete, or disseminate malware from any website or gateway. The coronavirus-causing illness known as Covid-19 is afflicted. Because businesses, governments, and people all depend on it. These days, everything that needs to be done is done digitally. Our online lives are also impacted. Crimes in the modern day go beyond simple physical assault and mental torment. The internet has evolved into a new form of life as a result of the development of new technology and communication methods. Nowadays, information technology is a critical tool utilized by practically every kind of firm. Cybercrime is rising quickly as a result of COVID-19. A cybercriminal can quickly compromise, delete, or disseminate malware from any website or gateway. The coronavirus-causing illness known as Covid-19 is afflicted. Because businesses, governments, and people all depend on it. These days, everything that needs to be done is done digitally. Our online lives are also impacted. Crimes in the modern day go beyond simple physical assault and mental torment. This paper discuss about the repercussion of the excessive use of internet during COVID-19 by the adolescents and unprecedented cybercrimes faced by them in India.

Keywords:
Cybercrime, COVID-19, Internet, Adolescents at risk, lockdown

Introduction

The year 2020 brought unprecedented challenges to the world due to the COVID-19 pandemic. While the virus wreaked havoc on public health, it also had far-reaching effects on various aspects of society, including crime. One notable area that witnessed significant changes was cybercrime. In India, as elsewhere, cybercriminals exploited the pandemic to their advantage, resulting in a surge in digital offenses.

The COVID-19 pandemic fundamentally altered the way we live, work, and interact. Lockdowns and social distancing measures propelled societies towards a more digital existence. This shift was particularly pronounced in India, a nation with a rapidly growing internet user base, especially among adolescents. While online platforms facilitated education, communication, and entertainment during the

pandemic, they also created a breeding ground for cybercrime. This research paper examines the surge in cybercrime in India during COVID-19 and its concerning impact on adolescents.

The Numbers Speak: A Drastic Increase

Data from the National Crime Records Bureau (NCRB) paints a worrying picture, India recorded 50,035 cases of cybercrime in 2020, representing an 11.8% surge compared to the previous year1.

Cybercrime incidents in India witnessed a staggering rise during the pandemic. Compared to 2019, cybercrime rates per lakh population jumped by over 12% in 2020, translating to a significant increase in the number of reported cases. Fraud emerged as the most prevalent category, followed by sexual exploitation and extortion.

Cybercriminals exploited the heightened online presence and anxieties surrounding COVID-19. Phishing scams thrived, often disguised as legitimate government or healthcare advisories. These scams tricked individuals into revealing personal information or clicking on malicious links that compromised their devices.

This increase is particularly alarming, considering the challenges posed by the pandemic. Let's delve into the key factors contributing to this rise:

Vulnerabilities Amid Lockdowns

As the country implemented lockdowns and people shifted to remote work and online activities, cybercriminals found new opportunities. The sudden transition to digital platforms exposed vulnerabilities in systems, networks, and individual behavior. With more people relying on the internet for work, education, and entertainment, cybercriminals exploited these vulnerabilities to launch attacks.

New Threats and Techniques

The pandemic gave rise to novel cyber threats. For instance:

Ransomware Attacks: A new ransomware strain called "CovidLock" emerged, disguised as a coronavirus tracking app. Unsuspecting users downloaded it, only to find their devices held hostage by cybercriminals.

Phishing Scams: Cybercriminals sent phishing emails and messages related to COVID-19, preying on people's fears and curiosity. These scams aimed to steal personal information or spread malware.

Dark web marketplaces: The dark web witnessed a surge in activity, with the sale of stolen data, malware, and tools for cyberattacks.

Increased Internet Usage: With physical movement restricted, people turned to the internet for work, communication, and entertainment. Unfortunately, this also meant more opportunities for cybercriminals. As the number of online users surged, so did the chances of falling victim to cyberattacks.

Targeting Individuals and Organizations

Cybercriminals targeted both individuals and organizations during the pandemic:

Individuals: Phishing attacks, identity theft, and financial fraud increased. People received fraudulent emails claiming to offer COVID-19 relief or updates.

Organizations: Companies faced challenges securing remote work environments. Cybercriminals exploited weak points in home networks and unpatched software to breach corporate systems.

The Role of Disinformation

Misinformation and disinformation about COVID-19 circulated widely. Cybercriminals capitalized on this by spreading fake news, creating malicious websites, and launching attacks related to pandemic-related topics.

Adolescents as a high-risk group: Adolescents are indeed a high-risk group for cybercrime during the COVID-19 pandemic in India.

Increased Internet Usage: Adolescents are more connected to digital platforms, especially social media, due to remote learning, entertainment, and social interactions. With schools closed and limited physical activities, they spend more time online, making them susceptible to cyber threats[2]

[1]https://timesofindia.indiatimes.com/india/murders-rapes-cyber-crime-how-covid-affected-the-crime-graph-in-2020/articleshow/86233885.cms

[2] https://link.springer.com/article/10.1007/s10639-022-11168-4

Lack of Face-to-Face Interaction: The pandemic disrupted face-to-face interactions with friends and peers. Adolescents seek social connections online, which can lead to risky behavior, including sharing personal information or engaging in cyberbullying[3].
Digital Literacy Gap: While adolescents are tech-savvy, they may lack critical digital literacy skills. Cybercriminals exploit this gap by tricking them into revealing sensitive information or falling for scams4.
Emotional Vulnerability: Adolescents experience emotional stress during the pandemic – anxiety, loneliness, and uncertainty. Cyberbullies prey on these vulnerabilities, causing emotional distress through online harassment.
Peer Pressure and Trends: Adolescents often follow trends and peer behavior. Cybercrimes like sextortion, cyberstalking, and sharing inappropriate content can spread among peer groups.
Easy Accessibility to Gadgets and Internet: With gadgets readily available at home, adolescents have unrestricted access to the internet. This accessibility increases exposure to cyber threats.
Parental Monitoring Challenges: Parents may struggle to monitor their children's online activities effectively.
Adolescents explore the digital world independently, sometimes encountering risks[5].
Increased Time Online: The pandemic led to unstructured time online. Adolescents may encounter harmful content, cyberbullying, or even engage in risky behavior themselves. Strategies for a Safer Digital Future: Protecting Adolescents Against Cybercrime in India

Effects of Cybercrime on the adolescents

The COVID-19 pandemic significantly altered daily life across the globe, with a notable shift towards increased reliance on technology. In India, this trend was particularly evident as educational institutions and social interactions moved online. While this digital transformation offered numerous benefits, it also created fertile ground for cybercriminals to exploit vulnerabilities. This paper examines the rise of cybercrime during COVID-19 in India and its concerning impact on adolescents.
The usage of educational applications, the growing popularity of social media, and the recent transition to online learning and schooling are some of the reasons why internet hazards are hanging large over young people. Children are now much more susceptible to online abuse and bullying as well as other digital threats. Media sources state that in April 2020, the National Commission for Women (NCW) wrote to Gujarat's Director General of Police after someone broke into a university's online course and started acting strangely on screen.
In a another instance, a cyberbully threatening to post her private photos on the school group chat blackmailed a schoolgirl in Delhi into paying a ransom. These crimes are becoming more commonplace and require immediate attention from the government. They are no longer isolated instances. While social media's ascent is well recognized worldwide and has dominated recent advances in cyber safety, particularly for youth, there are other factors that actually present a significant threat to online safety.

Surge in Cybercrime: Data from the National Crime Records Bureau (NCRB) paints a clear picture. Cybercrime incidents in India witnessed a sharp rise during the pandemic. Compared to 2019, cybercrime rates per lakh population jumped by over 12% in 2020. This translates to a significant increase in the number of cases, with fraud being the most prevalent category, followed by sexual exploitation and extortion.
Cybercriminals capitalized on the heightened online presence and anxieties surrounding COVID-19. Phishing scams thrived, often disguised as legitimate government or healthcare advisories, tricking individuals into revealing personal information or clicking on malicious links that could compromise their devices. Adolescents, with their increased screen time and potentially lower awareness of cyber threats, became particularly vulnerable targets.

Impact on Adolescents

[3] https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic
[4] https://link.springer.com/article/10.1007/s10639-022-11168-4
[5] https://journals.sagepub.com/doi/pdf/10.1177/0973134220200312

The rise in cybercrime has had a multifaceted impact on adolescents in India. Here are some key areas of concern: Increased Exposure to Online Threats: Adolescents are more likely to engage in online activities like gaming, social media, and communication platforms. This can lead to inadvertent exposure to cyberbullying, harassment, and inappropriate content.
Financial Exploitation: Cybercriminals often target adolescents with online scams promising quick money or access to exclusive content. Their lack of financial literacy and experience can make them more susceptible to falling victim to these tactics.
Privacy Violations: Adolescents may be less cautious about sharing personal information online, making them vulnerable to identity theft, stalking, and the spread of compromising photographs or videos.
Mental Health Issues: Experiencing cybercrime can be traumatic for adolescents. It can lead to feelings of anxiety, depression, and social isolation.
A 2020 study by CRY highlighted a rise in cyberbullying cases in India during the pandemic. This online harassment can have a significant negative impact on a teenager's self-esteem and mental well-being.
Unencrypted transactions and illicit activities, such as stealing money from clients' accounts, are two of the most hazardous consequences of cybercrime. Poverty and other social and economic losses therefore rise. The bank accounts of Indian youngsters have all had their balances wiped out as a result of this disaster, as some of them have been frozen since they haven't paid back the banks' instalments on time. Despite this, the absence of expected transactions and money transfers through financial institutions is the reason why the Indian banking sector is not growing all that well. The primary cause of these fees is the low self-esteem of Indian youth, which deters them from sending money. Cybercrime may have dangerous implications, with unencrypted transactions and other illicit operations like stealing money from customers' accounts being among them.
Consequently, there is a rise in social and economic losses as well as poverty. Due to this disaster, all of the bank balances in the accounts owned by Indian youngsters have been depleted, and some of these accounts have even been frozen since the bank has not yet received the required payments from them. Nevertheless, the absence of planned transactions and money transfers via financial institutions is impeding the growth of India's banking industry. The primary reason for these fines is the lack of confidence among Indian children and teens, which makes them reluctant to part with money. Furthermore, 42 million Indians were reportedly the victims of cyberattacks in 2011, according to the Norton Cybercrimes Report's highlighted part, which determined that the victimization of Indian youth by cybercrime had reached a peak.
In addition to domestic cybercrimes, India has also been the subject of well-publicized cyberattacks, the majority of which have targeted foreign cybersecurity agencies. This is an additional concern that must be taken into account. For example, the Stuxnet virus, which was intended to damage Iran's centrifuges at the nuclear site in Natanz, also compromised the communication system of the Indian computer system. Therefore, a lack of modern cybersecurity technologies and approaches contributes to the exploitation of young people in India.

Mitigating the Risks

Addressing this growing concern requires a multi-pronged approach:
Cybersecurity Awareness Programs: Educational institutions and government bodies need to implement age-appropriate cybersecurity awareness programs for adolescents. These programs should educate teenagers on identifying online threats, protecting their privacy, and practicing safe online behavior.
Parental Guidance: Open communication between parents and adolescents is crucial. Parents should be aware of their children's online activities and guide them on safe online practices.
Law Enforcement Measures: Law enforcement agencies need to be equipped to tackle cybercrime effectively. This includes investing in cyber forensics capabilities and strengthening collaboration with international organizations to track down cybercriminals.
Advocate Krishna Mohan K Menon says:
“The Cyber Laws in India has paved the way for electronic commerce and electronic governance in the country by ensuring maximum connectivity and minimum cybersecurity risks. Also, enhancing the scope and expanding the use of digital mediums. In India, cyber laws are stated under Information

Technology Act 2000, and the aim of this law/act is to provide the electronic commerce a legal platform, and giving them an advantage of having a safeguard for their online businesses or transaction."
Maintaining cyber security requires three key resource pillars: people, process, and technology. Every business must update its cyber security plan in order to maximize the three resource pillars and sustain a strong cyber security posture. A cyber security policy and a cyber crisis management strategy should be included in the cyber security plan. Prior to the COVID-19 pandemic outbreak, "office premise"-centric resources were the key pillars of cyber security, and many firms did not have plans in place to handle situations like "work from home." Businesses that once operated out of a single, central site or a limited number of locations are now dispersed over several places. Because of this, "Remote Access Domain" security is crucial. One of the seven domains of a typical IT architecture is called the "Remote Access Domain," and it is made up of the authorized users who have remote access to the organization's resources. Access frequently happens over unprotected networks, such the internet, whether "working from home" or traveling. Data privacy is the main security problem with remote access. This implies that the material should only be seen or altered by authorized individuals.
The most popular safeguard to preserve data privacy in an untrusted environment is encryption. Application data encryption, application connection encryption, and system connection encryption are possible components of the approach.

Conclusion

During the height of the COVID-19 pandemic, there was a discernible and substantial surge in cyberattacks and cybercrimes, according to assessment. Because of government prohibitions and the tendency to stay indoors, more people are using the Internet, which has allowed hackers to leverage this to further their activities. Phishing increased as a result of scammers taking advantage of the pandemic and increasing their direct and indirect COVID-19-related campaigns, such as emails indicating order delays because of curfews or messages urging donations for COVID-19 patients. Attacks on the health, government, and economic sectors are intensifying, which is causing a notable spike in DDoS. Even though there was a noticeable decline in the number of ransomware assaults that were reported, losses increased as a result of increased ransom demands, and the expense of cleanup is rising. Furthermore, a notable surge in the dissemination of false information and fake news discovered a favorable habitat in social media. In addition, the globe saw the largest cyber assaults and, consequently, the largest and most hazardous hacking operation discovered near the end of 2020. Sunburst Trojans were released under the guise of the upgraded program. The study's findings clearly show that during COVID-19, there was a rise in cybercrimes involving adolescents as a result of a lack of user knowledge and distinct low-level security measures. Governments and organization leaders should therefore take deliberate steps to enhance cyber security during any abnormal conditions. Developing more advanced proactive cyber-attack detection software and turning on robust ICT monitoring during any unprecedented or emergency conditions are also essential.

Suggestions

Boost public knowledge of cyber security issues by launching extensive efforts to inform citizens, companies, and governmental organizations about cyber risks, safe online conduct, and the value of system updates.
Boost technical proficiency: To provide judges, prosecutors, and law enforcement agencies with the technical know-how required for successful cybercrime investigations and prosecutions, engage in training programs and capacity building.
Revisit and update cyber legislation often to stay up to current with new and emerging cyberthreats. Make sure that laws are strong, unambiguous, and give authorities the resources they need to successfully combat cybercrime. International cooperation: To find and apprehend cybercriminals who operate across boundaries, strengthen international cooperation through bilateral agreements, treaties granting mutual legal aid, and alliances with law enforcement organizations from other nations.
In order to exchange threat intelligence, resources, and knowledge and to respond to cyber threats in a more coordinated and efficient manner, it is recommended that public-private partnerships be strengthened between the government, corporate sector, and academia.

Planning for incident response: To guarantee a prompt and well-coordinated response to cyber events, businesses and governmental entities should create and execute extensive incident response plans. Data protection measures: Reduce the risk of identity theft and data breaches by enforcing data protection laws effectively and making sure that personal data is handled responsibly and maintained securely.

Bibliography:

1. DSL Reports (2011), Network Sabotage - http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-
2. IMDb (2012), Unauthorized Attacks - http://www.imdb.com/title/tt0373414/
3. Virus Glossary (2006), Virus Dissemination, http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml
4. Legal Info (2009), Crime Overview aiding and abetting or Accessory, http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html
5. Shantosh Rout (2008), Network Interferences - http://www.santoshraut.com/forensic/cybercrime.htm
6. Hundley and Anderson 1995, Schwartau 1994
7. J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit". The Oxford Handbook of Cyberpsychology. OUP, 2019.
8. S. O. Ciardhu ´ ain, "An extended model of cybercrime investigations," International Journal of Digital Evidence, vol. 3, no. 1, pp. 1–22, 2004.
9. J. L. Cebula and L. R. Young, "A taxonomy of operational cyber security risks," Carnegie Mellon University, Software Engineering Institute, Tech. Rep., 2010.
10. A. Nicholson, T. Watson, P. Norris, A. Duffy, and R. Is- 18 bell, "A taxonomy of technical attribution techniques for cyber-attacks". European Conference on Information Warfare and Security. Academic Conferences International Limited, 2012, pp. 188.
11. CPS, "Cybercrime - prosecution guidance," The Crown Prosecution Service (CPS), Tech. Rep., 2019. Available: https://www.cps.gov.uk/ legal-guidance /cybercrimeprosecution-guidance.
12. Pavan Duggal. Cyber Crimes: A Legal and Practical Approach to Cyber Crimes and Electronic Evidence (LexisNexis, 2015).
13. Debarati Halder, K Jaishankar. Cybercrime: An Indian Perspective (Universal Law Publishing, 2010)
14. The Information Technology Act, 2000
15. The Indian Penal Code, 1860
16. The Code of Criminal Procedure, 1973