"A CRITICAL STUDY ON CYBER CRIME AND SECURITY WITH SPECIAL REFERENCE TO ACCESS TO JUSTICE FOR NETIZENS IN COVID-19"

- Dr.WINSTON DUNN

ABSTRACT

From 21stMarch 2020, our respected Prime Minister announced lockdown in the whole country to safe the citizens from corona virus which was considered as pandemic of the century. Due to this pandemic many people lost their jobs and those who had, were shifted to work from home. Because of this pandemic, technologies served us in every aspect of life, whether it is in the field of healthcare, transportation, communication, or education. But with every development in information and technology, there is always something bad rather evil has aroused. The researcher will not be wrong to say that next world war will be for the data not for the land or wealth. In the past several months, many stories of copyright theft, hacking, and cracking, as well as other viruses and hoaxes, have accumulated. More and more internet-related crimes are on the rise, like mushrooms. Now citizens has been converted to 'Nitiziens' but have been disappointed by the lawmakers' failure to provide them access to justice when they encounter any cybercrime or breach in cyber security. In this research paper, the researcher will discuss the impact of cybercrimes and breach in security in Covid era and lack of access to justice for the nitizens. The paper also discusses the comprehensive idea of cyber security and the effort launched by the Government of India to combat cybercrime. Finally, the article offers suggestions for coping with the problems of cyber security.

Keywords: - Covid-19, Cybercrime, Nitizens, Cyber Security, Access to Justice.

INTRODUCTION

> *"The world is no longer controlled by guns, energy, or money; it is run by ones and zeroes—small pieces of data. It's all about electrons. There is a war that is not a global war. It is not a competition to see who has the most BULLETS. It all comes down to who has control over the information. It is all about information, what we see and hear, how we work, and what we see."*

[1] Deepak Singh, LL.B.(D.U.), LL.M.(D.U.), PhD Scholar, Faculty of Law, University of Delhi.

Every human being in today's interconnected society is influenced by the Information Technology[2] (IT) revolution in some way. We are greatly transformed because of these two technological marvels, i.e. the computer and the network. The widespread adoption of IT has deeply affected nearly every element of our life. It is composed of various sectors, including manufacturing, marketing, and services. Glimpse of areas severely touched by advances in IT.

Computer

Computer[3] is very remarkable machine. Most of our daily activities do not include the use of computers these days. Computers are employed both deliberately and unknowingly in our everyday activities. Computer is essential to a variety of everyday tasks, whether it's withdrawing money from an ATM, producing a newsletter, driving a motorbike, designing a building, or even buying new clothes.Precisely, "Computer is an electronic device for performing arithmetic and logical operations", or "computer is a device or flexible machine to process data and converts it into information."[4]Today's computers are more powerful, smaller, cheaper, and more user friendly. The increased use of computers has been mainly due to the advent of the Internet.[5]

Internet

The most recent, and perhaps biggest, advancement in the history of information technology has resulted from the rapid growth of the internet and cyberspace.[6] The internet has altered the world in many ways. The Internet has also transformed the globe into a virtual sleepless global marketplace. These technologies have spawned many new companies and, more significantly, have altered the way most organizations operate. The new companies and new methods of conducting them, generally known as "Internet commerce" or "e-commerce," are on the rise. The

[2]Information technology is helping companies establish and secure communication networks for their organizations, protect data and information, create and maintain databases, and support workers as they solve issues with their computers or mobile devices, *available at: https://www.snhu.edu/about-us/newsroom/2018/07/what-is-information-technology*(last visited on July 13, 2021).
[3]Section 2(1) (i) of IT (Amendment) Act, 2008, *available at: https://indiankanoon.org/doc/1752240/* (last visited on July 13, 2021).
[4]Vaishali Sharma, *IT Encyclopedia com-Fundamental of Information Technology* 2 (Dhanpat Rai Publishing House, Delhi, Vol.II, 2002).
[5]Gopinath Amita and Israel Rachael, *Evidentiary Issues In Cyber Crime* 19 (Apex Court Expressions, 5th edn., 2004).
[6]Mustafa Faizan, "Challenge of Internet, Cybersex & Muslim Youth: Need for An Islamic Solution"95Aligharh Law Journal, Vol. 12, (1997).

Internet has eliminated time and location constraints for doing business and commercial operations. Without a question, computers and information technology have provided unparalleled advantages to people, companies, and society as a whole.[7]

Cyber Space

Until 1984, the world had never heard of the term 'Cyber Space.'[8] The term "cyber space" (from "*cybernetics* and *space*") was created by science fiction writer and pioneering cyberpunk[9] author William Gibson in his 1982 tale "*Burning Chrome*"[10] and popularizedin his 1984 book "Neuromancer."[11] 'Cyber space,' according to Gibson, is the virtual environment produced by computers when they interact. The Shorter Oxford English Dictionary explain the expression 'cyber space' as notional environment within which electronic communication occurs, especially when represented as the inside of a computer system; space perceived as such by an observer but generated by a computer system and having no real existence; the space of virtual reality.[12]

There are probably few, if any, words trendier than the two terms "cyber" and ".com" these days.[13] Rapid technological advancement has allowed new kinds of international crimes known as 'cybercrimes' to evolve. Cybercrimes impact every nation across the globe. The risk of cybercrime is likely to increase in the future and thus represents a great challenge for law enforcement.

---

[7]Colonel R.S. Prasad, *Cyber Crime - An Introduction,*28(The ICFAI University Press, Hyderabad, 2004).

[8]*Available at: https://whatis.techtarget.com/definition/cyberspace*(last visited on July 13, 2021).

[9]Cyberpunk was limited in the early 1980's to a movement in science-fiction literature. The words 'cyber' and 'punk' emphasize the two basic aspects of cyberpunk technology and individualism. The meaning of the word 'cyberpunk' could be something like 'anarchy via machines' or 'machine/computer rebel movements', *available at: http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.Pattammond.COEConvention.Cybercrime,pdf.*(last visited on July 13, 2021).

[10]"Burning Chrome" is a science fiction short story by Canadian-American writer William Gibson, first published in Omni in July 1982, *available at https://www.google.com/search?q=burning+chrome&oq=Burning+Chrome&aqs=chrome.0.0i355i512j46i512j0i512l8.840j0j7&sourceid=chrome&ie=UTF-8*(last visited on July 13, 2021).

[11]Neuromancer is a 1984 science fiction novel by American-Canadian writer William Gibson. Considered one of the earliest and best-known works in the cyberpunk genre, available at:- *https://www.google.com/search?q=Neuromancer&ei=euYGYdOwMePaz7sPp6yVqAk&oq=Neuromancer&gs_lcp=Cgdnd3Mtd2l6EAMyDQguELEDEIMBEEMQkwIyBQgAEIAEMgUIABCABDIFCAAQgAQyBQguEIAEMgUILhCABDIFCC4QgAQyBQgAEIAEMgUIABCABDIFCAAQgAQ6BwgAEEcQsAM6BwgAELADEEM6DQguELADEMgDEEMQkwI6CgguELADEMgDEENKBQg4EgExSgQIQRgAUMXwCVjF8AlgkPcJaAFwAngAgAGuBIgB1QWSAQcwLjEuNS0xmAEAoAECoAEByAEPwAEB&sclient=gwswiz&ved=0ahUKEwjT1d3SuJDyAhVj7XMBHSdWBZUQ4dUDCA4&uact=5* (last visited on July 13, 2021).

[12]*The Shorter Oxford English Dictionary* 588(Oxford University Press, New York, 5thEd. 2002).

[13]S. Sundari Nanda, *A Practical Overview of Cyber Crime Trends* 16(CBI Bulletin, New Delhi. Vol. 8,2000).

Cybercrime

According to the Merriam-Webster Dictionary,[14] the word “cybercrime” may be defined as either criminal behavior in which a computer is either the target of the crime (hacking, phishing, spamming) or a tool for committing the offence (child pornography, hate crimes). Technological tools may be used by cybercriminals to get access to personal data, trade secrets, or for illicit or harmful objectives over the Internet. In addition to communication and data storage, criminals may also utilize computers for document and data storage. Those that engage in unlawful acts in the pursuit of profit are called hackers. The terms "cybercrime" and "computer crime" are synonymous. “Cybercrime is a crime that involves hacking, phishing, or spamming a computer as the goal of the crime or as a tool to conduct the offence (child pornography, hate crimes). With computers and the Internet, thieves may now steal personal information, company trade secrets, or carry out harmful activities. Because of their usage in the criminal underworld, computers are also often used for communication and storing of documents and data. Many hackers refer to those who engage in criminal acts as hackers. A synonym for "computer crime" is "cybercrime."[15]

Many cybercrimes are not violent, but instead motivated by money, pride, or the opportunity to play on another person's character flaw. With the Net as it is, it is quite difficult to trace the perpetrator since the Internet can be a place of manipulation and be accessible from any part of the world. Cybercrimes are regarded as white-collar crimes for these reasons. Two and three In order to fully comprehend the implications of cybercrime, it is essential to realize that it is one of several political, social, and economic processes presently under way throughout the globe.[16]

Netizens

Netizens are people who live in cyberspace and are connected with computers, information technology, and the Internet. Thus, a netizen is someone who becomes a part of and participates

[14]*Available at: -https://www.merriam-webster.com/dictionary/cybercrime*(last visited on July 13, 2021).
[15]*Available at: -https://www.techopedia.com/*(last visited on July 13, 2021).
[16]B.Jyoti Kiran and Shiladitya Goswam, ″The Menace of Cyber Crime", Legal Services India,*available at:-http://www.legalserviceindia.com/articles/article+2 302682a.htm*(last visited on July 13, 2021).

in the broader online culture, which has few borders save language. The name ‘netizen' is derived from the terms ‘Internet' and ‘citizen.' [17]

Around the globe, there are about 4.6 billion people who use the internet in January 2021. That accounts for about 59.5% of the global population. For the total, 92.6% (4.32 billion) of those surveyed, who accessed the internet, did so through mobile devices.[18]Furthermore, there are approximately 30 million websites on the internet.

Cyber Security

Cyber Security, which has traditionally occupied a supporting role to national security, has grown in prominence to the point that it has become a basic component of national security. In other words, it's the capacity of a state to defend itself and its institutions against various cyber-attacks, such as espionage, sabotage, crime, and fraud, as well as identity theft. At this moment, there are no precedents to rely on, so the most we can do is identify the pressures and track the capabilities, with an eye toward classifying their comparative behaviors over time. Regulated, restricted, or otherwise policed messages are disseminated in most countries with internet access. It is common for the numerator to be larger than the denominator.[19]

However, "cyber security" has no established meaning among the population. Cyber-attacks including identity theft, hacking, and intellectual property infringement as well as state-sponsored activities, such as acts of war, are all considered dangers to the internet. This captures the essence of the task at hand: it's intended to defend the public against dangers that may affect end users, administrators, ISPs, utility corporations, financial institutions, defensecontractors, and the government.[20]

The dangers countering cyber-security are made up of three different things:

2 **Cyber-crime -**Systems-based crime, such as individuals or organizations conducting "cyber-attacks" on targets for financial gain or damage is known as cybercrime.

3 **Cyber-attack -**Politically motivated information collecting frequently occurs in a cyber-

[17]*Available at: -https://www.easytechjunkie.com/what-is-a-netizen.htm*(last visited on July 16, 2021).
[18]*Available at: -https://www.statista.com/statistics/617136/digital-population-worldwide/*(last visited on July 16, 2021).
[19]*Available at: -https://shodhganga.inflibnet.ac.in/bitstream/10603/150766/7/07_chapter%201.pdf*(last visited on July 16, 2021).
[20]*Ibid.*

attack.

4 **Cyber-terrorism -** An effort is made to sabotage electronic systems to produce fear or panic.

Challenges of Cyber Security

Cyber security has been considered as one of the most urgent national security problems.A report says, in a speech during his presidential campaign, President Obama promised to "make cyber security the top priority that it should be in the 21st century . . . and appoint a National Cyber Advisor who will report directly" to thePresident.

To protect an organization's cyber security, cyber professionals must keep in mind not only deliberate attacks, such as those by disgruntled employees, industrial espionage, and terrorists, but also unintentional compromises of the information infrastructure due to errors in the usage of systems and equipment, as well as incidents due to natural disasters. There is a risk that security vulnerabilities may let an attacker enter a network, get access to the control software, and disrupt network load circumstances in a manner that is difficult to anticipate. Defending cyberspace necessarily requires building effective partnerships between organizations charged with securing cyberspace and those who utilize the space by countless other organizations, such as government organizations, financial institutions, transportation providers, manufacturing facilities, and service providers. Cyberspace's defense has a distinctive characteristic. Defending the national territory or space is firmly defined, since all areas that are protected by land, sea, and air troops have well defined boundaries. Outer space and cyberspace are distinct because of the various aspects. Even from the viewpoint of national interest, they are worldwide.

ACCESS TO JUSTICE

Concept of Justice

Justice has ever been the highest ideal of mankind. It has been a dominant urge behind all social upheavals and revolutions. Justice, under various names governs the world-nature and humanity, science and conscience, logic and morals, political economy, politics, history, literature and art.[21] Whatever name may be given to 'Justice' it is the most primitive in the human soul, most

[21] *Available at: https://www.un.org/esa/socdev/documents/ifsd/SocialJustice.pdf*(last visited on July 16, 2021).

fundamental in society and most sacred among ideas. It is the essence of religions and the sum total of reason, the secret object of faith, and, of knowledge. Justice can be imagined more universal, stronger and more complete than justice. Justice is founded on what the majority of right thinking people regard as fair.[22] Justice, according to Aristotle[23], requires that things of this universe be equitably distributed among all the members of the community *or* state and this just distribution shall be maintained by law as against any violation.

Aristotle distinguishes between natural and conventional Justice. By Natural Justice he means that justice which has the same force everywhere and does not exist by people's thinking this or that. Natural rules are the same everywherewhether we accept it or not. By conventional justice he means thatpart of justice which is laid down by law. A rule of conventionaljustice has settled one way or the other indifferently and onceit is settled it no longer remains indifferent, and is to befollowed by society. The things are 'just' by virtue of conventionor expediency. The things which are 'just' not by nature but byhuman enactment are not everywhere the same.[24]

Rawls says that primary object of Justice is the basic structure of society, or more exactly the way in which the major social institutions distribute fundamental rights and duties and determine the division of advantages from social cooperation.[25]

Equality of Access to Justice

Equality before law is the fundamental principle of our legal system and its logical corollary is the equality of opportunity to get justice. It is not sufficient that law treats all persons equally.[26] The emphasis is that everyone should have equal access to the courts that doors of the courts be opened to all alike and that law should not only be applied to all impartially but should be equally accessible to all. 'Access to Justice' is a powerful expression of a social need which is imperative, urgent and more widespread than is generally acknowledged.[27]

[22]John Rawls, *A Theory of Justice*, *available at: - https://www.jstor.org/stable/191342*(last visited on July 18, 2021).
[23]*Available at: https://is.cuni.cz/studium/predmety/index.php?do=download&did=104852&kod=JPM327*(last visited on July 16, 2021).
[24]*Supra* note 22.
[25]*Ibid.*
[26]Law Commission of India (Report No. 213), November 2008, *available at: -https://lawcommissionofindia.nic.in /reports/report213.pdf*(last visited on July 18, 2021).
[27]*Ibid.*

Equality of access here means effective access and not the theoretical access. The idea of "Access to Justice" represents social order, in which justice is provided to all people, regardless of their position in society. Administration of civil justice should be made accessible to all citizens without regard to financial or social status. On the other hand, a key premise of the idea is that justice should be provided to all people in an evenhanded and effective manner, and on the flip side, no one should face oppression because of his or her inability to pay or the fear of going to court.[28] In other words, it means that problems and complaints occurring in society be dealt with in an orderly and lawful manner. The main goal is to help ensure social harmony and prevent social disharmony.

Traditional concept of "access to justice" as understood by man in the street, is the access to, the courts of law. For a common man the courts represent the very essence of justice. For him, the court system is an ideal and practical forum for the administration of justice, both civil and criminal, where legal rights and duties are determined and enforced. The ordinary courts are *seen* as part of the machinery of government, in which the judges exercise judicial power and authority with dignity, integrity and impartiality. Access to courts is considered as the basic mode for the adjudication of legal disputes and conflicts.

The two primary objectives of the legal system are stated in the phrase "access to justice." The words 'access to Justice' focus on two basic purposes of the legal system.

(1) The system must be equally accessible to all and,

(2) It must lead to results that are individually and socially just.[29]

Now, after discussing the concepts of cybercrime, cybersecurity, and access to justice etc. the researcher will discuss whether the netizens have access to justice in this covid-19 period with in the background of cybercrime and security.

Cyber Threat and Cybersecurity after the onset of COVID-19

Criminologists often state, "A crime occurs only when the chance presents itself." Before the age of information and technology, only conventional crimes such as murder, rape, theft, extortion, robbery, dacoity, and banditry were in our awareness but due to advancement of science and

[28] Andrew Higgins, *"*Legal Aid and Access to Justice in England and India*", available at: https://www.jstor.org/stable/44283780*(last visited on July 18, 2021).
[29] *Ibid.*

technology criminals have developed and improved online crimes like data theft, online fraud etc. The internet has given many more individuals access to an online virtual paradise where they may freely connect with a wealth of different cultures, ethnicities, and geographies. While the advantages of the internet may be used in both good and bad ways, if the internet is misused or abused by filthy minds and evil individuals, it becomes a virtual hell.

In this day and age when the usage of computers and the internet-connected systems have grown widespread, cyber security issues have emerged. When one is prepared to defend against dangerous individuals and software on the internet, it is essential to consider information security. The majority of attacks on computer networks are deliberate, having been designed by malevolent individuals.

As a result of the epidemic, the World Health Organization has designated COVID-19 a pandemic, having significant effect on the lives, families, and communities of people. This has drastically affected organizations, with everything from new working styles to new cyber security threats following suit.

Due to the fast developing worldwide response, we know that organizations face major difficulties that they must deal with promptly. Due to the increased operational and financial pressures, many organizations and workers are beginning to question current methods of working. This may raise the danger of cyber assaults to an unimaginable degree if not well thought out.

Organizations today are more reliant on technology than they have ever been, which puts cyber security good practices at risk. As attackers exploit uncertainty, unexpected circumstances, and fast IT and organizational development, we are starting to see the nature of the threat shift. The Coronavirus (COVID-19) pandemic has led to the largest number of workers worldwide who are required to be connected, regardless of where they are located. In order to deal with employees working from home, you need to make sure they are aware of the kinds of phishing schemes that are currently playing on concerns about the Coronavirus. All employees, regardless of the size of their company, are currently under resourced when it comes to cyber resources.

An organization must make sure that all devices that its employees use are protected. 42% of endpoints are unsecured at any one moment according to the Absolute 2019 Global Endpoint Security Trend Report. Due to this, individuals who work from home should learn about their online privacy and cybersecurity vulnerabilities, since this may cost twice as much in worldwide criminal damage by the end of 2018.

With the beginning of COVID-19, it became more apparent that the nation's existing cybersecurity policy was vulnerable. More work-from-home access created more security issues. A study that quizzed workers at various Indian companies discovered that 66% of them experienced at least one data leak. Over the last several months, security experts have seen a 500% increase in the number of cyber assaults and security breaches, and about 3 to 4 times as many phishing attempts.

The Data Security Council of India claims there has been an increase in the number of financial transactions that has led to an increase in the number of fraudulent assaults. During this growth, there was also an increase in healthcare with fraudulent activity resulting in detection of theft, as well as other problems. At least 1,000 assaults on educational facilities were recorded, as well.[30]

COVID-19 has brought out the greatest amount of workers around the globe who are compelled to operate remotely. When employees work from home, it is essential that they have knowledge and awareness of phishing schemes, one of the fastest-growing forms of cybercrime, which is currently taking advantage of people's concerns about the Coronavirus. Businesses of all sizes and kinds are dealing with very little cybersecurity resources compared to what they had before to this.[31]

Organizations must take steps to make sure every user endpoint is completely secure. While the Absolute 2019 Global Endpoint Security Trend Report found that 42% of endpoints are unsecured at any one moment, this indicates that the rest of the systems on the network are fully protected. People working from home should quickly get cyber security knowledge to prevent their personal information from falling prey to worldwide cybercrime harm that may cost them double this year. It is no coincidence that as the home-working becomes the new normal, crooks

[30]*Available at: -https://analyticsindiamag.com/what-is-the-current-cybersecurity-policy-in-india-how-it-has-been-impacted-by-covid/*(last visited on July 18, 2021).
[31]*Ibid.*

are exploiting the general fear by capitalizing on it. Fears, vulnerability, and disruption are among the techniques new coronavirus-themed phishing schemes are using.[32]

Cybercrime is the world's largest menace, and it is one of the most dangerous issues affecting humanity. A regular occurrence in the cybercrime sphere is the appearance of the yearly official cybercrime report from Cybersecurity Ventures. The most successful phishing attempts take use of people's emotions and worries, together with their heightened interest in news about the coronavirus, and as a result these communications are difficult to ignore.A new study predicts that the global economic cost of cybercrime will rise to $6 trillion per year by 2021, from $3 trillion in 2015. The importance of this deal cannot be overstated: this represents the greatest transfer of economic wealth in history, and is risky because it jeopardizes incentives for innovation and investment. Finally, it will yield a return much greater than the combined global market value of all major illegal drugs.[33]

Cyber-crime often occurs because of a variety of factors that lend itself to that kind of behavior:-

1. Higher transaction volume and digitized data. For purposes of analysis, it is simple to get transactional and customer information, as well as the outcomes of product launches, as well as market intelligence. It is a much sought-after goal to create valuable intellectual property online.

2. Comparatively it is to be anticipated that it will be more transparent since corporations and businesses are operating their offices from home itself. The majority of individuals want to use mobile devices to access company networks for day-to-day operations. New and improved smart technology gadgets allows for more connection, but they also bring out new kinds of security risks. A simple way into business networks for hackers is to compromise these securities.

[32]Prof. (Dr.) Tabrez Ahmad, "Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity", *available at: -https://www.coursehero.com/file/68276925/SSRN-id3568830pdf/*(last visited on July 18, 2021).

[33]*Ibid.*

3. MaliciousSoftware i.e. viruses and spyware are able to gain partial control of key programmers, this software is both invasive and powerful.

4. Companies use networks to improve their company profitability by linking customers and suppliers.

5. The technology used by sophisticated hackers and professional cybercrime organizations is more advanced than previously thought. This could occur, for example, when a hacker is paid to install malware on the device of an end user. Today's malware threats are tougher to detect because they steal personal data for monetary benefit. Some believe that they earn more money if they become hackers, rather than if they pursue careers in cyber security.

Let's discuss some stats:-

THE BEST AND THE WORST CYBERSECURE COUNTRIES

ThePrint

RANK 2019	RANK 2020	COUNTRY	SCORE 2019	SCORE 2020	PERCENTAGE OF MOBILES INFECTED WITH MALWARE	PERCENTAGE OF COMPUTERS INFECTED WITH MALWARE	BEST PREPARED FOR CYBERATTACKS
1	1	ALGERIA	55.75	48.99	26.47	19.75	0.262
15	18	INDIA	39.30	33.82	28.75	11.74	0.719
13	23	CHINA	40.80	28.90	4.73	9.65	0.828
57	76	DENMARK	12.04	6.72	2.57	3.15	0.852

Source: -The Print

In the above table, we can see that India was on 15 position in 2019 before COVID-19 hit the world but in 2020 we fall 3 positions down and got 18th position in the list of the best and the worst cyber secure countries. This shows how we are lacking to secure our country.

Cyber Crime Cases Registered Under Information Technology Act, 2000:[34]

According to the Information Technology Act, almost 8,600 cases were filled. Identifying thefts, cheating through impersonating by using a computer, and violating privacy are all

[34] *Available at: -https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/*(last visited on July 20, 2021).

part of the act.

Breakup of cases registered cases under IT Act are as follows:

TYPE	TOTAL NUMBER OF CASES UNDER IT ACT	PERCENTAGE OF OVERALL
Tempering computer source documents	**206**	**0.91**
Computer related crimes	**6818**	**79.16**
Cyber terrorism	**12**	**0.14**
Publication of obscene/sexually explicit content	**957**	**11.11**
Breach of confidentiality/privacy	**35**	**0.41**
Other cyber-crimes under IT Act	**713**	**8.28**
Total number of cyber-crimes under IT Act	**8613**	**100**

Source: - TOI

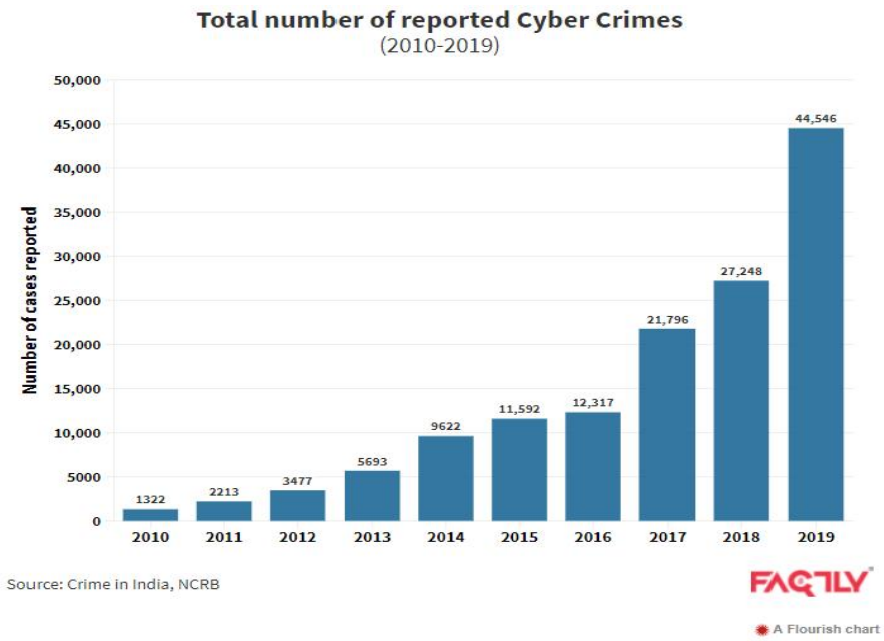
There has been an increase in the number of cases filed under the Information Technology Act, 2000, and the Indian Penal Code (IPC). From 2011 to 2020, the number of cases reported under the IT Act increased by more than 350 percent. The number of cybercrimes reported under the IT Act has increased by almost 70% from 2019 to 2020. Over the next seven years, IPC offences will see a rise of more than sevenfold. The number of people arrested for perpetrating cybercrime also experiences a similar pattern.

A recent surge in cybercrimes has also been acknowledged by the government, which also points to the growth in the use of technology, gadgets, and applications such as smartphones and sophisticated software.

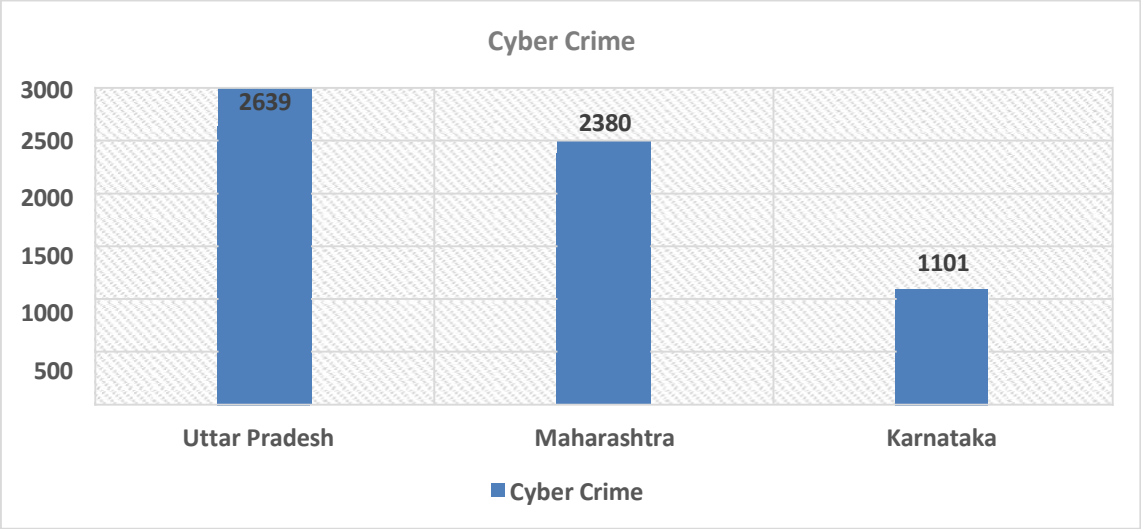
Cybercrimes have also increased as internet access has become more widespread. To combat cybercrime, it is essential that Cyber Security be implemented immediately. Cyber security is safeguarding your personal information from being stolen, detected, and handled appropriately in the case of a cyber-attack.

Total Number of Reported Cyber Crimes (2010-2019)[35]

Over the years, many updates have been made to this part of the NCRB report due to the recent emergence of cybercrimes as a new entry. It was under the cause-wise list until recently, and so information was added and removed when new causes emerged. Between 2018 and 2019, the NCRB recorded highest growth in cybercrimes in one year. This has made the motivation of cyber-investigation crime's much more difficult. Fraud cases have grown substantially. Fraud charges alone accounted for almost 60% of cybercrime in 2019. With regard to extortion, prank, sexual exploitation, vengeance, and instances of disgrace, the numbers have steadily increased over the years. There is a possibility that the rise in cyber-crime reporting is due to an increased awareness of the general population.



[35]Available at: -https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/(last visited on July 20, 2021).



State & City Wise Cyber-Crime Record in Year2020:

Source: "Crime in India 2020- Statistics", National Crime Records Bureau Report, 2020[36]

Cybercrimes were 11,592 in 2020, according to the National Crime Records Bureau (NCRB). Cyber-crime is expected to rise by a total of 9.3% by the year 2021(13,317) more than the total for 2020(11,592). Between that year and now, Uttar Pradesh has reported the highest number of cybercrimes, with 2639 incidents, which accounts for 21.4% of all recorded cybercrimes. Maharashtra comes in second with 2380 instances representing 19.3% of all reported cases. This is followed by Karnataka, with 1101 cases which account for 8.9% of all reported cases. The bulk of cyber-crime instances have been recorded in these states: Uttar Pradesh, Karnataka, and Maharashtra.

Cybercrime shoots up in lockdown, over 2000 cases reported till April[37]

[36] *Available at: -http://ncrb.nic.in/*(last visited on July 20, 2021).
[37] *Available at: -https://www.newindianexpress.com/states/karnataka/2020/jun/11/cyber-crime-shoots-up-in-lock down-over-2k-cases-reported-till-april-2155009.html*(last visited on July 20, 2021).

Cybercrime occurred at a higher rate during March and April than any other time in 2018, according to data from the City Crime Records Bureau. It shows that during that period, there were 1,308 cybercrime cases, of which an increase in bank fraud and scams occurred in which people impersonating government officials trick people into transferring money for welfare schemes or a government-run relief fund.

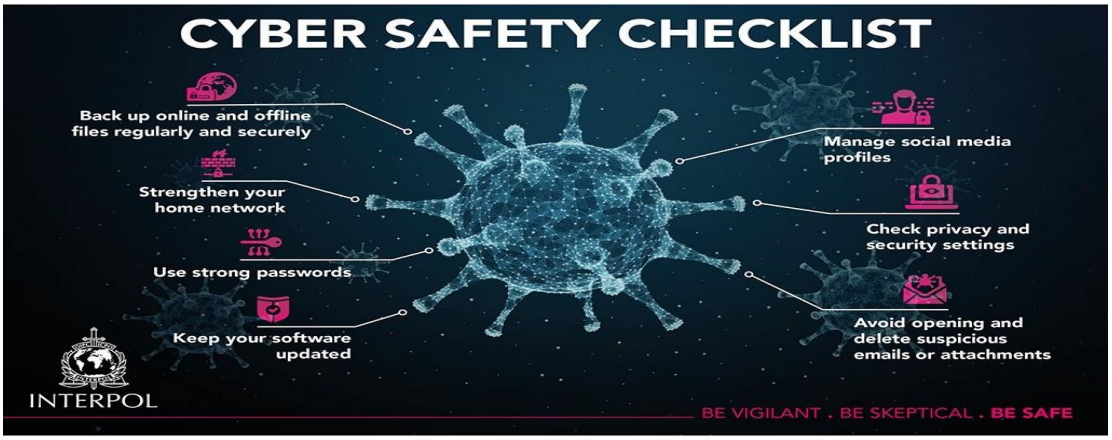
COMMON METHODS OF TARGETTING

Major types of crimes	Jan	Feb	March	April
Debit/credit card frauds (vishing)	87	141	347	202
Job fraud	8	27	41	9
Card skimming	47	56	83	19
Gifts and loan offers	49	102	209	38
Social media cases	23	35	57	52
Other advance fee scams	10	8	12	7
Business opportunity fraud	3	15	11	4
Total	305	490	878	430

Source: -City Crime Records Bureau.[38]

Cyber safety tips - protect yourself againstcyber-attacks[39]

Here are t



[38]*Ibid.*

[39]Ajit Singh, "An Introduction to Experimental and Exploratory Research", *available at: - https://ssrn.com/abstract=3789360*(last visited on July 20, 2021).

op cyber safety tips from Interpol:

Source: - Interpol.int

1. The software and operating system should be regularly updated.
2. For the best protection, use antivirus software such as Kaspersky Total Security, Norton, or Quick Heal.
3. Create strong passwords; don't use easy-to-guess passwords.
4. When email arrives from an unknown source, please do not open the attachment. These may be contaminated with malware.
5. Don't click on links in emails that are sent to you from people you don't know or sites you're not acquainted with. Malicious software may be distributed in this manner very often.
6. To avoid man-in-the-middle attacks, avoid utilizing insecure Wi-Fi networks in public areas.

Some suggestions: - how corporations and workers may protect their cyber security

1. **Virus/malware protection-** Antivirus and malware software should be made available to employees as a means of protecting their personal computers. Although this does not provide complete protection, it has the effect of drastically reducing many lower-level assaults.

2. **Cyber security awareness-** In order to appropriately and consistently apply rules and processes for the transmission of emails or other material to private email addresses and/or cloud storage, it is essential for staff to be aware of the best practicesand procedures already in place.

3. **Users' awareness of phishing-** When receiving emails, employees should verify the sender's address.

4. **VPN is required-** Another layer of security is added when using virtual private networks (VPNs). In order to maintain their ability to defend against cyberattacks, they must be accompanied by other cyber security measures. In many ways, companies have the same fundamental cybersecurity measures available to them.

5. **Identify gaps in performance-** Every IT system has vulnerabilities. Companies should always do tests on their software to detect vulnerabilities and deal with the most serious issues as soon as feasible. Either vulnerability scanning or penetration testing activities may be used. All components in the technological infrastructure should be made more difficult to disrupt.

6. **Received many reviews-** To assess if current controls are adequate, companies should analyses their risk exposure and identify what measures are needed. Cyberattack tactics that have lately emerged should be included in the evaluations.

7. **Consider implementing new technologies and tools-** Ensuring the security of remote working may be further enhanced by the use of sophisticated technologies, such as host checking (a tool to verify the security posture of an endpoint before allowing access to corporate information systems).

8. **Indirect methods of investigation-** To assist businesses in better monitoring cyber threats, organizations should promote proactive usage of cyber threat information, which would provide attack indications (IOC) and attack solutions.

9. **Preventing business risk-** To enhance the security of an organization, businesses may use governance, risk, and compliance (GRC) solutions. a comprehensive risk exposure and linkage of risk disciplines is provided by GRC solutions (e.g. cybersecurity, operational risks, business continuity)

10. **Defend yourself against assaults**- According to industry experts, businesses should be prepared to respond to a cyberattack by carrying out regular cyber crisis simulations.

Nitizens work from home should follow these Cybersecurity Tips to protect themselves.

1. Using multi-factor authentication whenever feasible, with an additional layer of protection that will be provided by third-party applications. Additional safeguards include using a password manager to help keep hazardous behaviors like storing or sharing credentials under control.

2. Home and remote working should be included into all organizations' cybersecurity

policies. It is essential that your organization's policies be up to date when you add employees outside of the office. All remote working functions, as well as the usage of personal devices, and updated data privacy requirements must be considered.

3. Employees should use the IT equipment provided by employers to communicate with colleagues regarding official matters. Many software installations, known as app stores, sit quietly in the background of the company's IT, protecting employees. An business and its employees might be at risk if a security issue occurred on an employee's personal device

4. Personal devices used to access corporate networks that are not equipped with the appropriate security make companies susceptible to hackers. Any leaked or compromised information on a personal device exposes the business to liability.

Let those who work from home and those who are worried about cybersecurity understand the current cybersecurity landscape so that they can get the correct results in an increasingly challenging life, business, and global economic climate.

CONCLUSION

The idea of cyber security is extremely complex, as understanding it necessitates a thorough understanding of several different fields, including computer science and international relations, information technology, economics, organizationalbehavior, psychology, political science, sociology, decision sciences, engineering, and law.

In Covid-19 pandemic, due to work from home scenario, everything has changed drastically. Now, people are preferring more UPI or online payments rather than cash transactions, people working from home or even from Delhi Wi-Fi__33 networks to save themselves form pandemic. India has seen rise in cybercrimes against online users and even companies are not using cyber security software to save their funding and without proper security, protection, rules, laws etc. citizens cannot have access to justice.

Without a shared vision, cybersecurity and cybercrimes will persist. Cyber security must be a higher priority in India's fight against terrorism. The cyber landscape has changed drastically

since 2013, and the government has acknowledged the necessity for a more comprehensive framework for the operationalization of the vision of cyber security policy as articulated in India's national strategy. Thus, India's cyber security policy must be updated because to provide ‘access to justice’ the Nitizens has to be fully protected against the present and upcoming cyber threats.

According to a recent survey conducted by the news magazine TOI, which announced that India will require 20 lakh cyber security professionals by 2025 to support its fast-growing internet economy. The Union ministry of information technology estimates that the country will require 20 lakh cyber security professionals by 2025. Telecoms, utility sectors, power, oil & gas, airlines, government (law & order and e-governance) will account for the rest of the new positions predicted to be created in the financial industry.

An academic background and work experience help determine whether someone is qualified to hold responsibilities such as network security administrators, network defense analysts, web security administrators, application security testers, and security analysts. The employment position would be to design and conduct IT product and service development and quality assurance for firms, and ensure their security is as good as feasible. This area involves specialties around secure programming, permitted hacking, and network security surveillance.