International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Study on Awareness about Cyber Crime in India

Pallavi Verma

Under the guidance of Ms . Smyle

SCHOOL OF FINANCE AND COMMERCE
BACHELOR IN COMMERCE HONOURS
GALGOTIAS UNIVERSITY

INTRODUCTION

Internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education and many more. With
The advent and increasing use of the Internet, companies have crossed the barriers of local markets and are reaching customers located in all parts of the World. Computers are widely used in business not only as a tool to process information, but also to gain strategic and competitive advantage. Computers
Can be used for both constructive and destructive reasons.
The abuse of the Internet has given rise to new age crimes that are addressed in the Information Technology Act of 2000. As information around the World becomes more accessible, it also becomes more vulnerable to misuse. India is on the radar of cybercriminals with increasing cyber attacks against Indian establishments. India ranks third as a source of malicious activity on the Internet after the US and China, second as a source of malicious code, And fourth and eighth as a source or origin of web attacks and network attacks.
According to the Computer Emergency Response Team of India (CERT-In), 27,482 cases of cybercrime were reported between January and June (2017).
These include phishing, virus or malicious code, defacement, scanning or probing, site intrusion, ransomware, and denial of service attacks.

It has been shown that in the first six months of 2017, at least one cybercrime was reported every 10 minutes in India, which is higher as compared to Every 12 minutes in 2016. India has seen a total of 1.71 lakh crimes. Cyber crimes in the last 3.5 years and the number of crimes so far this year has been 27,482, indicating that the total number is likely to exceed 50,000 in December. Analysis of data from 2013 to 2016 shows that 6.7% of all cases accounted

For network scanning and probing, while viruses or malware accounted for 17.2%.
According to the latest report from the National Crime Records Bureau (NCRB), a total of 11,592 cases were registered under cybercrimes (including Cases under the Information Technology Act, crimes under related sections of IPC and crimes under the Special and Local Laws (SLL)) compared to 9,622 cases registered during the previous year (2014) which shows an increase of 20.5% compared to the previous year. Uttar Pradesh has reported the Highest number of such crimes, followed by Maharashtra and Karnataka.

The increasing rate of Internet usage has created a problem for people who spend long hours browsing the cyber world. In 2017, the number of mobile Internet users grew by 12.49 percent compared to the previous year and 23.93 percent of the population accessed the internet from their mobile phone.

This figure is expected to grow to 34.85% in 2022. (statista.com, 2017). Therefore, the increased use of the Internet has opened the door for cybercrime To flood. Lack of awareness on these issues will lead to emotional, moral or ethical financial damage.

Under such an alarming scenario, apart from tackling cybercrime, another issue that needs to be targeted at higher priority is raising awareness of "cybercrime and security" among internet users. Therefore, the current study focuses on finding the answers to alarming questions, that is, "Are people Really aware that they are vulnerable to various cybercrimes?" "If they are aware, to what extent?", and "If they are not aware, then what steps can be Taken to make them more aware and up-to-date? Cybercrime refers to any crime involving a computer or network. It is an illegal act in which the computer is a tool, a target, or both. These are criminal Activities committed through the use of electronic means of communication. It's taking something from the computer over the internet.

The term Cyber Crime has not been defined either in the Indian Parliament or in the Information Technology (IT) Act 2000. In India, the IT Act 2000 Deals with offenses related to cyber crime. Cyber crime registration in India is carried out under the three general headings which are IT Act, Indian Penal Code (IPC) and Other State Level Legislation (SLL). Several Cyber Cells have been established to exclusively handle the cases that are registered under

Cyber crimes in India.

It is a fast growing crime area. Cyber criminals are exploiting the Internet to commit a wide range of criminal activities. In the past, cybercrime was Mainly committed by individuals or small groups, but now cybercriminals constitute various groups/categories, such as professional hackers, organized Hackers, children and adolescents between the age group of 6-18, scammers, phishers. , insiders, malware authors, spammers, etc.

OBJECTIVES OF THE STUDY

- To find out the levels of awareness among internet Users regarding cyber crimes.

- To design a framework to uphold the awareness Programmes among internet users to curb the Cyber crimes and cyber security.

Chapter 2.

LITERATURE REVIEW

1. Anupreet Kaur Mokha

Research Journal of Humanities and Social Sciences 8 (4), 459-464, 2017

Usage of internet has become a daily routine for majority of people for day-to-day transactions. The number of internet users has grown tremendously and so does cyber-crimes. Cyber-crime is the crime that is done using computer and network. The threat of cyber-crime is an ever present and increasing reality in both the private and professional sectors. With the advent of internet, old crimes have taken on a new appearance. The purpose of this research is to make awareness regarding cyber-crimes which are happening in today's world and also to create awareness of increased cyber security. This paper attempts to analyze the awareness of cyber-crime among internet users with different age groups and educational qualifications. Linear Regression Model has been applied for analyzing both the objectives. This paper finds that there is a relationship exists between the age groups and educational qualification of the respondents. So, it is the duty of one and all internet users to be aware of cyber-crime and security and also help others by creating awareness among them.

1. Priyanka Datta, Surya Narayan Panda, Sarvesh Tanwar, Rajesh Kumar Kaushal

2020 International conference on emerging smart computing and informatics (ESCI), 269-275, 2020

In modern society the role of Internet and computer system is well recognized. People are greatly benefited with the development of networking and cyber space but some people are using this development in unethical way to have some illegal benefits. Recently different types of Social-networking attacks are witnessed by social networking sites user. Internal Revenue Service (IRS) impersonation scams, along with technical support scams are the most common type of tricks used by the attackers on unsuspecting victims in order to achieve financial benefits. The ratio of cyber-crime in India is constantly rising due to various reasons. Cyber-crlminals are very difficult to trace and this advantage is fully utilize by scammers. In this paper an intensive review has been done on cyber-crime in India. The studies shows that fraud cases are increasing and the victims are mostly in the age group of 20 – 29 years. Mostly children and women are affected. Thus, awareness programs are required for preventing or avoiding cyber-crime in India.

3.Aastha Verma, Charu Shri

Vision, 09722629221074760, 2022

The proliferation of the Internet's interconnections has led to a substantial increase in cyberattack incidents, often with devastating and grave consequences for the organizations and their associated clientele. The pandemic of COVID-19 has pushed most organizations towards digital transformation. The higher dependence of a firm on digital infrastructure makes it more vulnerable to cyber-crimes. The existing

literature suggests that the most notable and frequently chosen weapons of attackers are Internet of things (IoT) attacks, phishing attack, malware attack, distributed denial of service (DDoS) attack and structured query language (SQL) injection attack. In this study, an attempt has been made to generate a protection framework from these cyberattacks. In doing so, the present research has adopted a systematic stepwise process of investigation. The research method consists of four components. First, through bibliometric analysis in VOSviewer, authors identified the scope for searching the related literature published worldwide and generated visualization for comprehension. This step led to the selection of 60 research articles for further analysis. After that, each security threat's MAXQDA software word tree was developed, representing its linkages with possible security solutions and control measures. Lastly, they adopted expert elicitation protocol through semi-structured interviews with six corporate IT experts and five academic experts. The synthesis of information gathered leads to the development of a suggestive protection framework for the organizations.

II. RELATED WORK

Literature survey had been done explicitly to distinguish

What had been done and what had not been done by other

Researchers on cyber-crimes topic. It helps us to figure out

How others have identified and measured key concepts of

Cyber-crimes

WHY IS CYBER CRIMES AWARENESS IN INDIA IS IMPORTANT?

CYBER CRIME AWARENESS IN INDIA IS IMPORTANT AS:-

1. To Reduce Financial Loss.:

Cybercrime has resulted in substantial financial losses for individuals, businesses, and the Indian economy as a whole. Financial frauds, online scams, and identity thefts have become rampant, causing individuals to lose their hard-earned money and businesses to suffer significant financial setbacks.

2. To overcome data bridges and privacy concern.

Data breaches have become a recurring nightmare for Indian organizations, leading to the compromise of sensitive personal and financial information of millions of individuals. Such breaches erode public trust and raise concerns about privacy and data protection.

3. To reduce the destruction of critical infrastructure:

Cyberattacks targeting critical infrastructure, such as power grids, transportation systems, and government networks, pose a severe threat to national security. These attacks can disrupt essential services, cause economic instability, and even compromise public safety.

4. To reduce social and psychological impact:

Cybercrime not only affects individuals and organizations financially but also has a profound social and psychological impact. Victims of cyberbullying, online harassment, and cyberstalking often suffer from emotional distress, anxiety, and depression. The psychological toll of cybercrime can be long-lasting and devastating.

How to file a Cybercrime complaint online in India?

A cybercrime complaint can be filed using the National Crime Reporting Portal of India.

Website link is – https://cybercrime.gov.in/

National Cyber Crime Reporting Portal of India
This portal is an initiative of the Government of India to facilitate victims/ complainants to report cybercrime complaints online.

This portal caters for all types of cybercrime complaints including complaints pertaining to

•Online Child Pornography (CP),
•Child Sexual Abuse Material (CSAM),
•Sexually explicit content such as Rape/Gang Rape (CP/RGR) content and
•Other cybercrimes such as mobile crimes, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking.
The portal also provides an option of reporting an anonymous complaint about reporting online Child Pornography (CP) or sexually explicit content such as Rape/Gang Rape (RGR) content.

CYBERCRIME HELPLINE NUMBER
The Cyber Crime Helpline Number is 155260.

CHAPTER 3.

RESEARCH METHODOLOGY

Research methods are the techniques and tools by which you research a subject or a Topic. Research methodology involves the learning of various techniques to conduct Research and acquiring knowledge to perform tests, experiments, surveys, and Critical analysis. Research methodology simply refers to the practical "how" of any Given piece of research. It's about how a researcher systematically designs a study to Ensure valid and reliable results that address the research aims and objectives.
Research papers, dissertations, thesis, academic journal articles, or any other piece of. Formal research will contain a section (or chapter) on research methodology.

Under this section of resource mythology it is understood that why cyber crime awareness is important in India and for which government has to conduct surveys , camps and many other ways so that people may get knowledge and information regarding cyber crime happening in India and to which not only educated but also uneducated people also get the knowledge or information from the awareness of cyber crime so that less crimes are conducted and people are more are there and active about cyber crime.

RESEARCH DESIGN

A research design is the arrangement of conditions for collection and analysis of

Data in a manner that aims to combine relevance to the research purpose with

Economy in procedure. This Research design applied for the study is 'Descriptive

Research.

3.2 SOURCE OF DATA

Sources of Data begins with figuring out what sort of data is needed, followed by

The collection of a sample from a certain section of the population. Next, you have

To utilize a certain tool to gather the data from the chosen sample. The two types

Ofsources of data are:

PRIMARY DATA

Information obtained from the original source by research is called primary data. They offer much

Greater accuracy and reliability. The data was collected from the respondents through the questionnaire.

QUESTIONNAIRE MADE:-
SECONDARY DATA

SURVEY

NAME:

Q1) Have you found someone using your photo, profile, bank detail (In social network) or duplicating your personal details?

a) YES b) NO
c) DON'T KNOW

Q2) If you have found someone using your photo, profile, bank detail, did you report to admin website?

a) YES b) NO
c) DON'T KNOW

Q3) Have you ever been hacked through email, social net or blogs?

a) EMAIL b) SOCIAL NET
c) BLOGS

Q4) on a scale from 1-10 (1 is being unaware 10 is completely knowledgeable) about cybercrime?

Q5) Have you ever heard of someone being a victim of cybercrime?

a) YES b) NO
c) DON'T KNOW

Q6) Have you seen anything on the news about people being harassed online?

a) YES b) NO
c) DON'T KNOW e) INDIFFERENT TO THE QUESTION

Q7) Are you satisfied with the way your complaint was handle?

a) YES b) NO
c) DON'T KNOW e) INDIFFERENT TO THE QUESTION

Q8) Do you use strong, unique and diversified passwords?

a) YES b) NO
c) DON'T KNOW e) INDIFFERENT TO THE QUESTION

Q9) Do you allow others (Friends, relatives) to use your personal ID?

a) YES b) NO

It means that data are already available. It refers to the data that are collected And analyzed by someone else. The data was collected from the websites and journals.

HYPOTHESES:

On the basis of mentioned objectives, the present study aims at test the following hypothesis (null hypothesis):

1. H01: There is a relationship exists between the Educational level of the respondent and the awareness of cyber-crimes among them.

2. H02: There is a relationship exists between the various age groups of the respondent and the awareness of cyber-crimes among them.

CHAPTER- 4

4.1 DATA ANALYSIS AND INTERPRETATION
Tools of analysis;
The following tools are used in the study

• Percentage analysis
• Chart

E reported cyber crimes in India have been

Grouped into three categories namely, IT Act Cases,

IPC (involving Computer as Medium/Target)

Cases and Special Acts & Local Laws (SLL)

(involving Computer as Medium/Target) Cases.

Number of reported cyber crime cases under each Of these categories and motives behind the cyber
Crimes for a period of five years from 2017 to 2021 As given in NCRB Crime in India Reports (2017- 2021) has been presented in Tables 1-4.
The variation of number of cyber crime cases Across a period of five years i.e. from 2017 to 2021 For different type of offences and motives have Been shown in figures 1-4.

SLL Cases

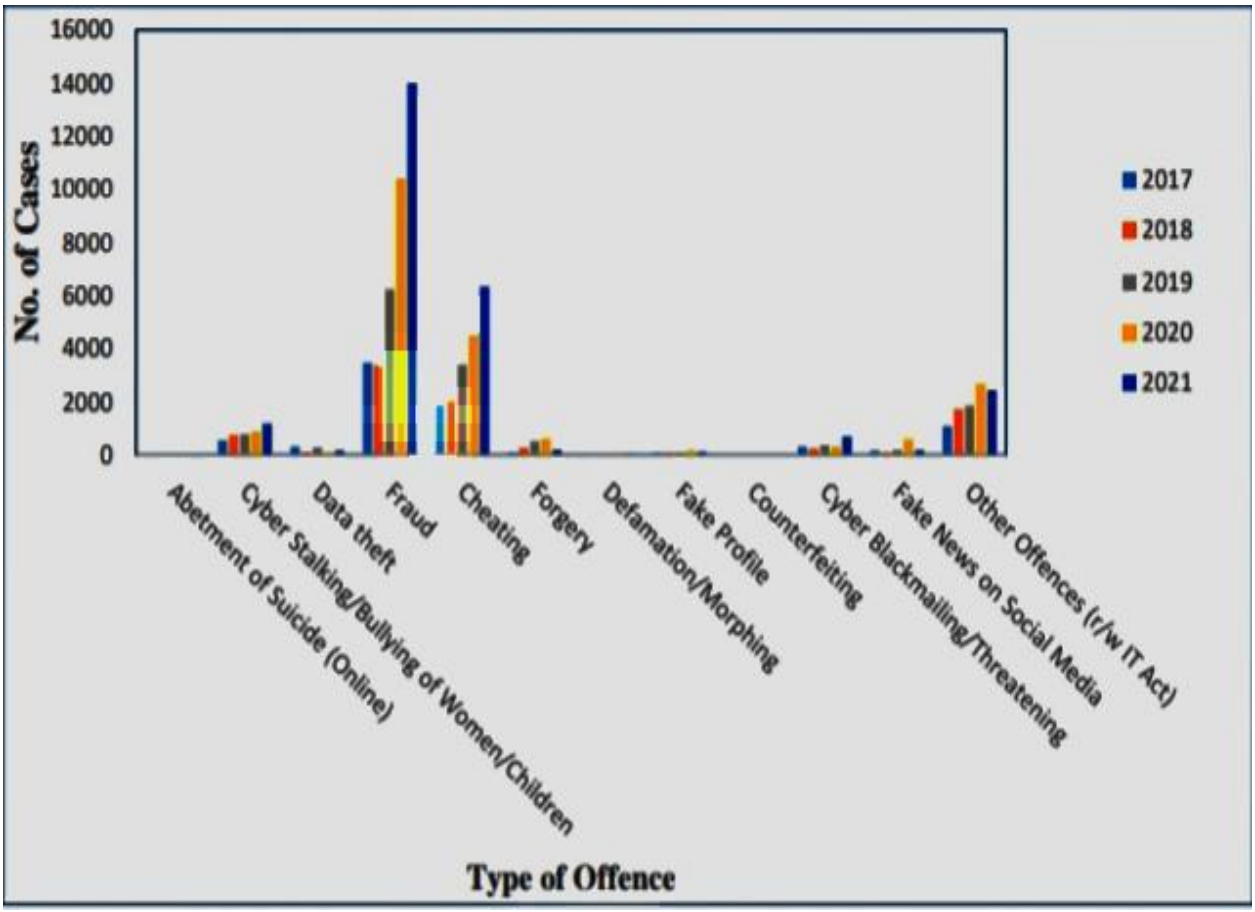


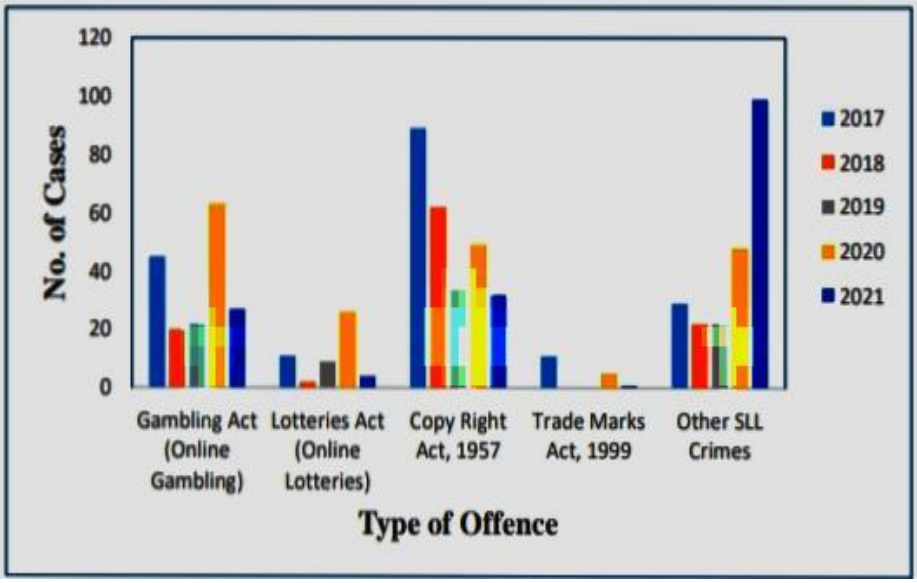
Table 3 indicates that cyber crimes under the Special and Local Laws (SLL) category are Significantly lower in number compared to the Other two categories. In the years 2017, 2018, 2019, 2020, and 2021, they accounted for only 0.85%, 0.39%, 0.20%, 0.38%, and 0.31%, respectively, of The total reported cyber crimes. On the other hand,

Fig. 3 suggests that there is no discernible trend in

CHAPTER 5

Table 3. Cyber Crimes - Offences under Special Acts & Local Laws (SLL) (Involving Communication Devices as Medium/ Target)

Sr. No.	Type of Offence	Total No. of Cases				
		2017	2018	2019	2020	2021
1	Gambling Act (Online Gambling)	45	20	22	63	27
2	Lotteries Act (Online Lotteries)	11	2	9	26	4
3	Copy Right Act, 1957	89	62	34	49	32
4	Trade Marks Act, 1999	11	0	0	5	1
5	Other SLL Crimes	29	22	22	48	99
	Total Cyber Crimes under SLL	185	106	87	191	163



FINDINGS, SUGGESTION AND CONCLUSION

The findings of cyber crime trends under the IT Act From 2017 to 2021 indicates that computer-related Offences, including identity theft, cheating by Personation, ransomware, violation of privacy, and Dishonesty receiving stolen computer resource or Communication device, constitute 23%-27% of all Cybercrimes under the Act, Additionally, the cases of publication/transmission Of obscene/sexually explicit acts in electronic form Are also increasing with time. Which shows a significant 66% increase in cyber Crimes under the IT Act in 2019 compared to 2018.
This rise can be attributed to the increasing number Of individuals in India with access to internet, Which increased from 462.1 million in 2018 to 560 Million in 2019.

CONCLUSION

The study conducted an analysis of cybercrime data In India from 2017 to 2021 and observed that the Majority of cybercrimes were related to computer- Related offenses, fraud, and publication or Transmission of obscene/sexually explicit acts in Electronic form. The primary motives behind these Crimes were fraud, sexual exploitation, extortion, Anger, and revenge. The study also found that cyber crimes in India are Increasing every year, with the most significant Increase of 63.5 percent observed in 2019. Despite Government efforts, the trend of cyber crimes is on The rise, which calls for joint efforts of both the Government and individuals. To reduce cyber

crimes in India, the study Recommends that the government needs to bridge The gap between policy making and its Implementation. Meanwhile, individuals should Use the cyber space cautiously and follow the Guidelines issued by various government agencies.

In conclusion, the study emphasizes the importance Of increased awareness and collaboration among all Stakeholders to ensure the safety and security of the Digital world in India.

REFERENCES:

1. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 5, Issue 8.

2. Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. International Journal of Enterprise Computing and Business Systems, January, Vol 2, Issue 1.

3. Archana Chanuvai Narahari and Vrajesh Shah (2016).Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand.International Journal of Advance Research and Innovative Ideas in Education.Vol-2 Issue-6.

4. Avais, M. Abdullah et.al. (2014), Awareness regarding cyber victimization among students of University of Sindh, Jamsharo. International Journal of Asian Social Science, Vol. 4(5): 632-641

5. Hasan et al., (2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404

6. The Times of India(July 22, 2017), http://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms.