IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Awareness And Perception On Cyber Law And Cyber Crime In India

[1]Prof. Darshan C, [2]Mr. Raju. J, [3]Mr. Anil Kumar S K, [4]Ms. Sangeetha. S, [5]Ms. Sanjana. V

[1]Professor, [2]Student, [3] Student, [4]Student, [5]Student

[1]Department of Commerce and Management,

[1]Mangalore Institute of Management and Science, Bengaluru, India.

Abstract: Cybercrime and Cyber law have emerged as critical concerns in the contemporary digital age. With rapid advancement of technology and widespread internet usage, the global cyberspace has become a breeding ground for various forms of criminal's activities. This study highlights the interplay between cybercrime encompassing activities such as hacking, data breaches, online fraud, cyberbullying and the evolving cyber law frameworks designed to combat and regulate these illicit activities. It explores the challenges posed by the borderless nature of the internet and the level of awareness regarding cybercrime and cyber law is a critical aspect in today's digital society.

Index Terms – Cybercrime, Cyber laws, Awareness & Perceptions.

I. INTRODUCTION

The first cyber-attack happened in France well before the internet was even invented, in 1834. Attackers stole financial market information by accessing the French telegraph system. From that moment on, cybercrime has grown exponentially, marked by an intriguing evolution of tactics, techniques, and procedures — all implemented for malicious gain. Still, cybercrime didn't really find its footing until the mid-point of the 20th century. Spurred on by the digital revolution, cybercriminals became early adopters of technology, using their head start and their smarts to engineer new, devious ways to part people and organizations from their data and dollars. If there was a Cybercrime Hall of Infamy, its halls would be lined with the names and faces of these noted attackers whose "groundbreaking" work caught both the eye of federal investigators and the envy of fellow hackers.

In 1962 The modern history of cybercrime began when Allen Scherr launched a cyber-attack against the MIT computer networks, stealing passwords from their database via punch card. In 1971the first computer virus was created for research purposes by Bob Thomas at BBN technologies. Referred to as the Creeper Virus, the self-replicating program was detected on the ARPANET in 1971 and foretold the potential of future viruses to cause significant damage to computer systems. The resolution of the General Assembly of United Nations

dated 30th January 1997 gave birth to the Information Technology Act which leads to the adoption of Modern Law on Electronic Commerce on International Trade Law. The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 when the new IT Ministry was formed. However, it underwent some alteration with the commerce industry due to some suggestions related to e-commerce and matters about the World Trade Organization (WTO) obligations. After the bill was introduced in the Parliament, the bill was referred to the 42-member Parliamentary Standing Committee following demands and suggestions from the Members. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cybercrime and to facilitate speedy locating of a cyber-criminal.

"cyber-crime" is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. "cyber-law" it exists to protect people from online frauds. They exist for preventing online crimes that include credit card theft and identity theft. A person who commits such thefts stands to face federal and state criminal's charges. The main goal of this article is to provide some basic knowledge and awareness of cyber-crime and cyber-law to the people.

India is the second largest online market in the world with over 560 million internet users, Ranked only behind China. And it is estimated that by 2023, there would be over 650 million internet users in the country. According to the latest national crime records bureau NCRB data, a total of 27, 248 cases of cybercrime where registered in India in 2018.In Telangana, 1205 cyber-crime cases where registered in the same year. According to FBIs report, India stands third among top 20 cybercrime victim. The national cyber-crime reporting portal (cybercrime.gov.in) which was started last year by the central government received 33,152 complaints till now resulting in lodging of 790 FIRs. In fact, according to a 2017 report, Indian consumers had lost over 18 billion US dollars due to cyber-crimes. In 2018, there were over 27,000 cases of cyber-crimes recorded in the country, marking an increase of over 121% compare to the number of the cases as two years back. Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views. The first cyber-law act was "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber-crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997".

II. REVIEW OF LITERATURE

- **(sarmah, 2017)**This article focusses on providing information on cyber-crime and cyber-laws. The objectives are to spread knowledge about cybercrime that take place through online, laws imposed against those crimes and focus on safety in cyberspace. This article found that the evolution of cybercrime, classification of cybercrime which include cybercrime against individuals, cybercrime against property, cybercrime against organization, cybercrime against society and it cover some sections of cyberlaw also few safety measures from protection against hackers. It concluded that the rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent year. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The study collected data through online website and online articles.
- **(Koranteng, 2019)**The article focusing on the cybercrime issue across many e-commerce which are increasing at a fast rate. The objective is the cybercrime on E-commerce, consumer behaviour, perceived risk and much more. Here can check the theoretical frameworks such Theory of planned behavior, Conceptual model, Hypothesis formulation and its classification. This article concluded the recent rise of cybecrime incidents threatens the use of e-commerce technologies for transactional operations. The development of appropriate e-commerce frameworks is need to identify and punish offenders. This will reduce the negative perceptions associated with e-commerce. Data is collected through several organisation and management of different counrties and statistical tools such as graphs and tabular format.
- **(broadhurst, 2006)** This article show's the rapid expansion of computer connectivity has provided opportunities for criminals to exploit security vulnerabilities in the online environment and the objective is that to prevent that, computer related crime and transnational crimes. The information knows about the challenges, criminality and computer crime, policing computer-related crime in the global village. Data is collected from university of Hong Kong and New York.
- **(brahme, 2013)**The objectives of the articles are providing information about the cybercrime, cyberlaw and cyber legislation. This article found that the complete information of cybercrime which include nature and scope of cybercrime, who commit cybercrime, classification of cybercrime and cyberlaw which include cyber legislation worldwide, cyber legislation in India. This concluded cybercrime is one of the deadliest and most dangerous crimes of the world. Even though cyber law is constantly being evolved.
- **(zhang, 2011)** Cybercrime are generally referred as criminal activities that use computers or network. The objectives that focus on identifying the cybercrime tools, target and place and we have the information of tools like copyright, spamming and target like denial of service, malwares, hacker and traditional non-cybercrime facilitated by computer and network technology. The conclusion of this paper explain cybercrime into several different classes and the main purpose is to help people realize the threats and potential and Statistical tool used like pie chart.

- **(ppnp, 2014)** This article focusses on the cybercrime and prevention of it. This article found that the history of cybercrime, types of cybercrime which include hacking, theft, cyber stalking, etc. types of hackers, effects of cybercrime on society, cyberlaw. The conclusion is in today's era the computer system and internet are increasing worldwide, thus making it easy for the cyber criminals to access any information by using their expertise. So cyberlaw knowledge must be known among the people working on the computer system. Data is collected through Wikipedia.
- **(saini, 2012)** The objective of cybercrimes and their Impacts is to provide the understanding of cybercrimes and their impacts over society with the future trends of cybercrimes. It has found out that one in five online consumers in the US has been victims of cybercrime in last 2 years. The research methodology of data collection is done via crime desk of certain countries. The samples were collected from journal articles.
- **(natah, 2015)** The objective is to educate consumer to balance between preserving information security of companies and confidentiality of customer's data. The findings include E-commerce transaction achieves the legal recognition by the electronic transactions act which deals with legal significance of complying with security assessments. The research area includes secure business application logic for e-commerce systems and bar graph is used. The data is collected via journal articles.

III. SCOPE OF THE STUDY

The scope of the study on awareness of cybercrime and cyber law is to assess the level of awareness among individuals, organizations, and government entities regarding cybercrime and cyber law. It aims to identify common cybercrime threats and their impact, as well as evaluate the effectiveness of existing cyber law policies and regulations. The study will suggest measures to enhance awareness and promote compliance with cyber law, with a focus on raising awareness among different stakeholders through educational initiatives and collaborative efforts.

IV. OBJECTIVES OF THE STUDY

- To know the Level of awareness about cyber-crime and cyber-law in society
- To understand the Perception of people related to cyber-crime and cyber-law
- To explore an overview of cyber law and cybercrime in India

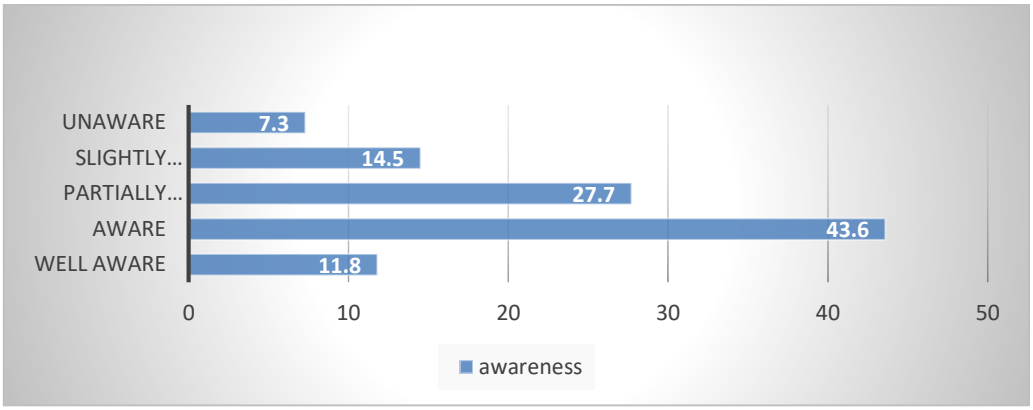
V. RESEARCH METHODOLOGY

This study uses descriptive research method to describe the situation. The data is collected from both primary and secondary source. Primary data is collected from survey and questionnaire technique. The secondary data is collected from articles, journals, website, etc. The questionnaire was collected from 110 respondents belongs to Bangalore city. The sample was selected from convenience sampling technique. Statistical tools like frequency and percentage analysis also some charts.

VI. RESULTS AND DISCUSSION

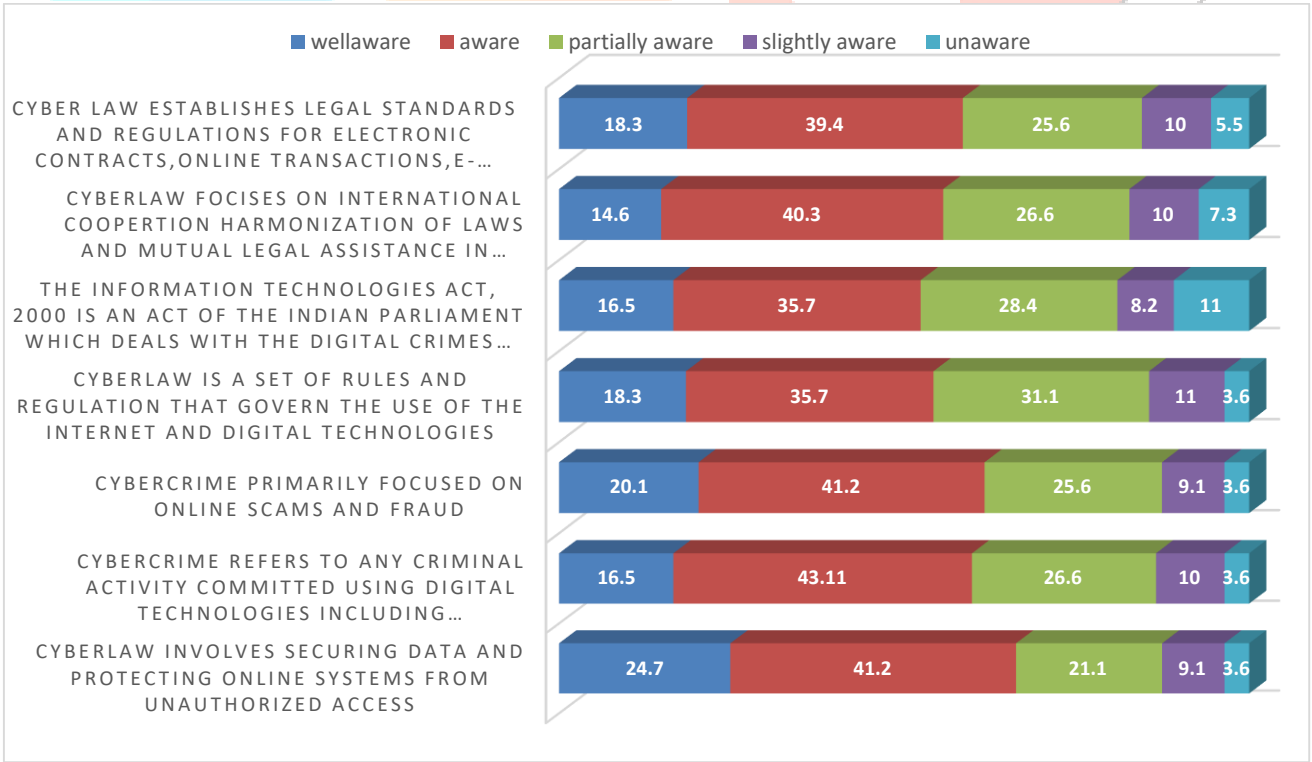
The data collected from various respondent have to analysis for the drawing conclusion. The data collected is presented in the form of charts and tables. A brief description of analysis and interpretation are given below:

Figure 6.1: Level of Awareness on cybercrime and cyberlaw.



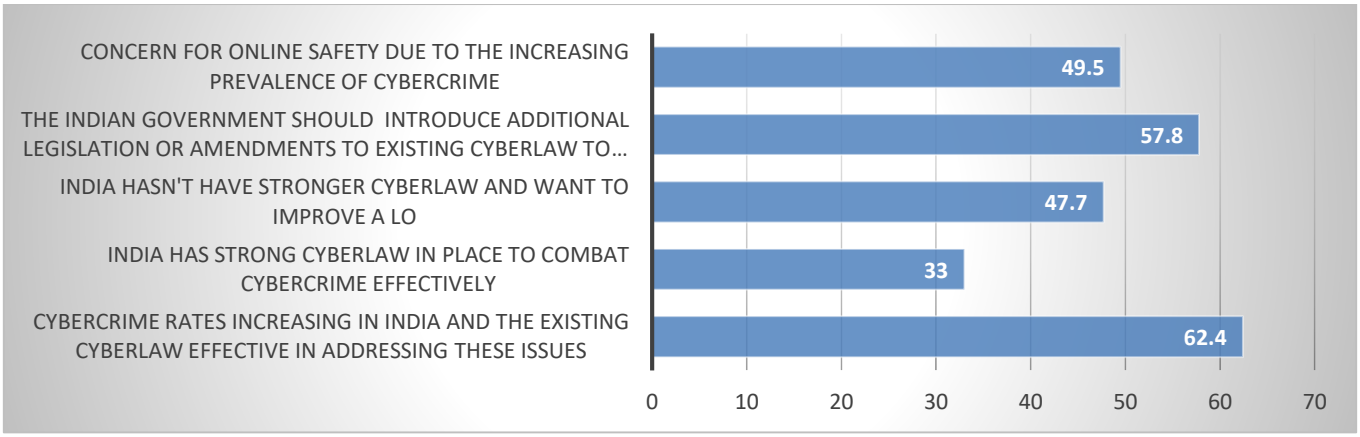
Interpretation: As per the survey above chart depicted that 11.8% responses are well aware about the "cybercrime and cyberlaw", 43.6% responses are aware about the "cybercrime and cyberlaw", 27.7% responses are partially aware about the "cybercrime and cyberlaw",14.5% responses are slightly aware about the "cybercrime and cyberlaw" and 7.3% responses are unaware about the "cybercrime and cyberlaw".

Figure 6.2: Awareness Level on the rule and regulation, criminal activities over internet.



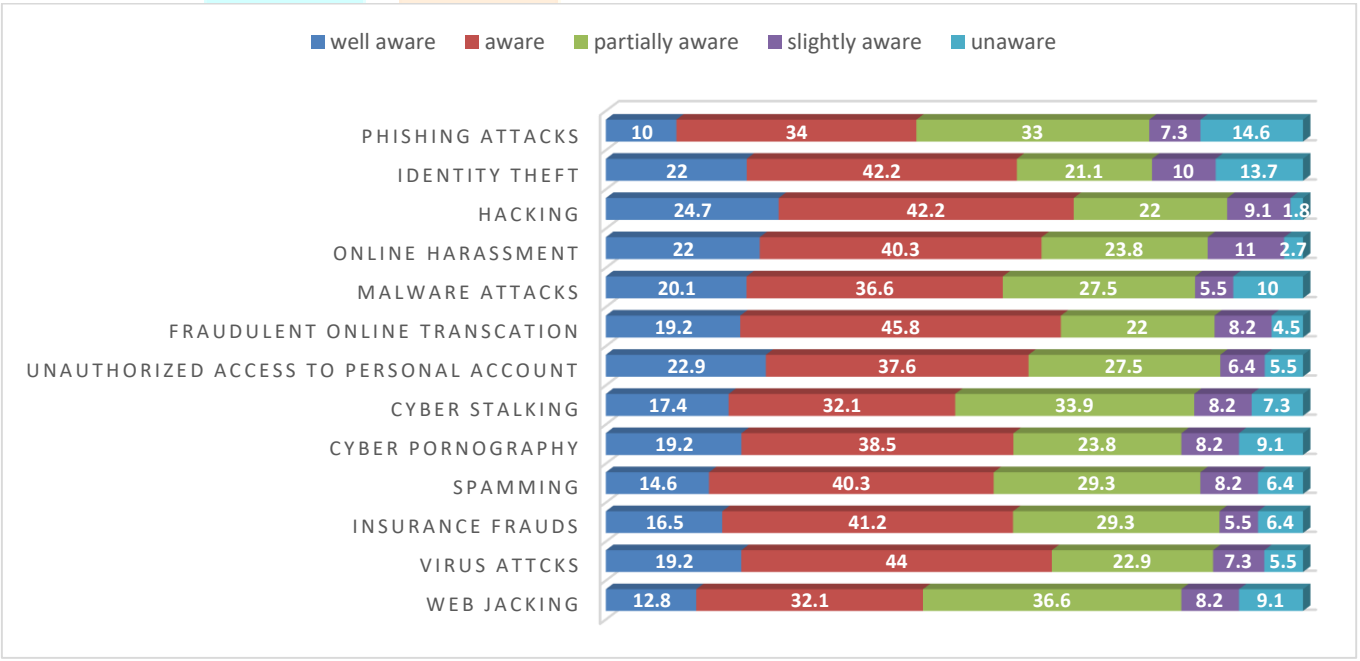
Interpretation: As per the survey the above chart indicates the awareness of respondent regarding the rule and regulation, criminal activities over internet.

Figure 6.3: Perception on Indian Cyber Law and Cybercrimes.



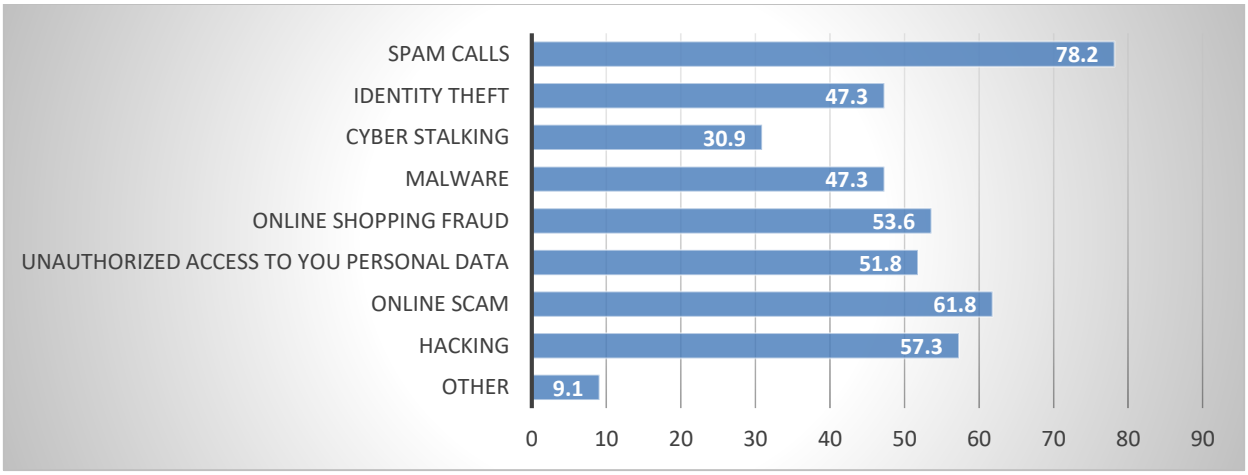
Interpretation: As per the survey the above chart depicted that the respondent perception about the cybercrime and cyber law also how strong Indian government provide security or safety from cyber-attacks.

Figure 6.4: Awareness level on different types of cybercrimes in India.



Interpretation: As per the survey the above chart depicted that awareness level of the respondent on different types of cybercrimes happening in technical world.

Figure 6.5: Different online scam or cyber-attacks which undergone by respondents.



Interpretation: As per the survey the above chart depicted that the different online scam or cyberattacks which undergone by respondents.

VII. FINDINGS OF THE STUDY

From the above data analysis and interpretation, following are the findings of the study:

- Majority of the respondents on awareness of cybercrime and cyberlaw are from female (53.6%) category compare male (46.4%) respondents.
- Most of respondents on "awareness of cybercrime and cyberlaw are from age group of below 25 years around 78.2% response.
- The most of respondents are received from under graduates (67.3%) and majority response from student.
- As per the received response most of the respondents are aware (43.6%) about the cybercrimes and cyberlaw.
- Majority of the respondent believes that cybercrime rates are increasing in India and the existing cyberlaw effective in addressing the issue.
- Also, the request is that the Indian government should introduce additional legislation or amendments to existing cyberlaw to address emerging cyberthreats more effectively.
- As per the received response majority of the respondents are overcome the challenges of spam calls, hacking, online scam and online shopping fraud.

VIII. Conclusion

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent year. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. Cyber law plays a crucial role in governing online activities, setting ethical standards, and prosecuting offenders. As technology continues to advance, it is essential to stay updated with the evolving cyber threats and adapt our legal measures accordingly. Building awareness about cybercrime and cyber law is equally important to empower individuals with the knowledge needed to navigate the digital landscape responsibly. By collaborating across borders, enforcing strict regulations, and promoting cybersecurity education, we can work towards a safer and more secure cyberspace for everyone.

References

- brahme, p. d. (2013). cyber crime and cyber law in India. *research*, 106-109.
- broadhurst, r. (2006). development in the global law enforcement of cyber-crime. *research*, 408-433.
- Koranteng, A. a. (2019). impact of cybercrime and trust on the use of E-commerce technologies. *an application of the theroy of planned behavior*, 228-250.
- natah. (2015). e-commerce security and the purview of cyber law factors. *research*, 1-14.
- ppnp. (2014). review on cyber crime and security. *research*, 48-51.
- saini, r. a. (2012). cyber-crime and their impact. *research*, 202-209.
- sarmah, a. a. (2017). a brief study on cybercrime and cyberlaw's of India. *research*, 1633-1641.
- zhang, y. (2011). a survey of cyber crime. *research*, 422-437.
- https://arcticwolf.com/resources/blog/
- https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
- https://arcticwolf.com/resources/blog/decade-of-cybercrime/