

# AN ANALYTICAL STUDY ON THE AWARENESS OF PARENTS ABOUT CYBERCRIMES AGAINST CHILDREN

RITU DUBEY TIWARI \*

## INTRODUCTION

The internet in India is growing rapidly. It has given rise to new opportunity in every field like entertainment, business, sports, education etc. The internet has both advantage and disadvantage and one of the most disadvantage is cybercrime. We can say, cybercrime is any illegal activity, which is committed using a computer network especially the internet. At least one cybercrime was reported every 10 minutes in India in the first six months of 2017. That is higher than a crime every 12 minutes in 2016. According to the Indian Computer Emergency Response Team (CERT-In). In India educated person commits most of cybercrime cases. Therefore, it is required the deep knowledge and awareness about the cybercrime. In addition, in India most of the cases found where crimes are committed due to lack of knowledge or by ignorance.

According to the Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported from January to June 2017. These include phishing, scanning or probing, site intrusions, defacements, virus or malicious code, ransomware and denial-of-service attacks. With more Indians going online, cyber experts said putting in place critical infrastructure to predict and prevent cybercrimes was crucial. India has seen a total of 1.71 lakh cybercrimes in the past three and a half years and the number of crimes in the last year (27,482) indicate that the total number is likely to cross

50,000 by December, just as in 2016. (Kumar C. , 2017)

Cybercrime is emerging as a very serious threat in today's world. It has been ranked as a top tier threat and has become a priority for governments and corporations worldwide. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Today, everybody is using the computers that is from white-collar employees to terrorists and from teenagers to adults. All the conventional crimes like forgery, extortion, kidnapping are being done with the help of computers. New generation is growing up with computers and most important is that all the monetary transactions are moving on to the internet.

## RESEARCH BACKGROUND

Children have always been vulnerable to victimization. Their trusting natures and lack of experience make them perfect targets for culprits, both people they know and those they do not. As children grow into adolescents, they remain vulnerable to victimization. Children are often curious and eager to try new things. Many children struggle with issues of rebellion and independence and seek attention and affection from people outside the home, often by using computers, tablets, and mobiles.

---

\*Principal, NISCORT Media College-Ghaziabad. **Correspondence E-mail Id:** editor@eurekajournals.com

The Internet is a new, effective, and more anonymous way to seek out and groom children for criminal purposes such as producing and distributing child pornography, contacting and stalking children for the purpose of engaging in sexual acts, and exploiting children for sexual tourism for personal and commercial purposes.

Cybercrime prevention can be achieved quickly and in a cost-effective manner. It is mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their attack surface and moderate the risks. (Kumar S. , 2015)

With this in mind, the researcher has taken the topic, which is very relevant of the time, "An Analytical Study on the Awareness of the Parents about Cybercrimes against Children". This study will differently throw light on the realities and actual happenings that one can see in and around their surroundings. This study will also give necessary tips for the parents to prevent cybercrimes in which children are prone to be the victims.

## **RESEARCH PROBLEM**

The purpose of this thesis is to study the awareness level of parents about the cybercrimes that affecting their children. Almost every school-going child has access to social media these days, but shockingly hardly any of them know about the privacy settings on their profiles. With details of their personal lives going public, they make themselves vulnerable to all sorts of cyber harassment. Children have always been vulnerable to victimization. Their trusting natures and lack of experience make them perfect targets for culprits, both people they know and those they don't. As children grow into adolescents, they remain vulnerable to victimization. In

addition, this analytical study on cybercrimes creates awareness on parents about the cybercrimes against children.

## **RESEARCH OBJECTIVES**

The research objectives are the points of finding information from certain types of research. Research objectives are found by deciding what type of research needs to be done and what types of information is hoping to obtain from the research. After decided the purpose of the research, the objectives of the research can be decided by figuring out which subjects need to be covered. This study aims to create the awareness of parents about cybercrimes against children.

The objective of research is to find the answers to certain questions through the application of scientific procedure. The general objective of a study states that what researchers expect to achieve by the study in general terms. It is possible to break down a general objective into smaller, logically connected parts. These are normally referred to as specific objectives. Specific objectives should systematically address the various research questions. The purpose of our research is first to study and analysis of different classification and types of cybercrimes and illegal activities which is done through the internet. In the current era Internet is a very hazardous weapon of hackers so, many types of cybercrimes occurs in current scenario like cyber bullying, cyber hacking and identity theft. There are so many modes of criminal activity on the internet that the traditional policing methods and the laws that bind criminals at times lose jurisdiction in cybercrime cases. This is why there are so many crimes being committed online.

A cyber law is the law governing cyber space. Cyber space is a very broad term and it includes all things which are related with cybercrimes and laws such as Computers, networks, hardware, software, data storage devices, internet, E-mails and all intelligent devices. The growth of

Electronic commerce has impelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of electronic commerce. All these regulatory mechanisms and legal infrastructure come within the domain of cyber law.

### **THE MAIN OBJECTIVES OF THE PRESENT STUDY ARE AS FOLLOWS**

#### **TO CREATE**

The first objective of this research is to create awareness about cybercrime to the parents.

#### **TO EXPLORE**

The second objective of this research is to explore about cybercrime against children in India.

#### **TO GAIN**

The third objective of this research is to gain more knowledge and to eradicate about cybercrime.

#### **SIGNIFICANCE OF THE STUDY**

In today's world, the reality is that all individuals especially children are accessed to the internet are vulnerable to cyber-attack. The significance of this research is that the researcher wants to create awareness about cybercrime to the parents which their children are victimised.

#### **LIMITATIONS OF THE STUDY**

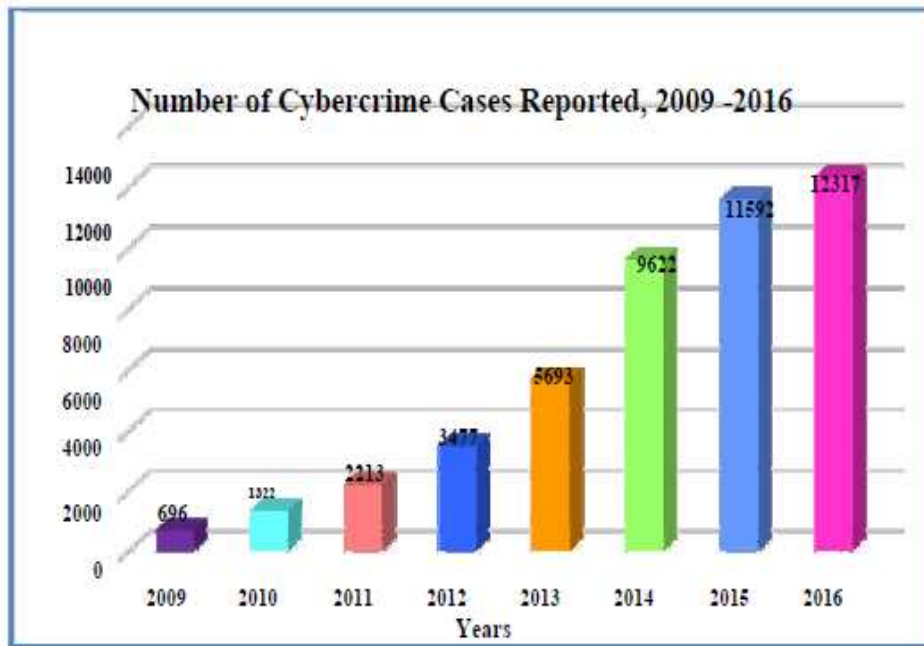
There are a various limitations in this study as follows:

1. This study was done only in English language with the help of a research tool developed for the purpose of the study.
2. An analytical study about Cybercrimes is a vast subject and many have researched on this topic. The researcher has limited on the awareness of the parents about the cybercrimes against children.
3. Survey was done only on the persons which their children are using the social media.
4. Some of the parents do not want to disclose the fact because of social pressure.
5. Children do not want to share that they face such types of incidents to their parents.
6. Parents and children do not share healthy relationship relating to Cybercrime

#### **THE GRAPHS AND STATISTIC NUMBER OF CYBERCRIME CASES REPORTED FROM 2009 TO 2016**

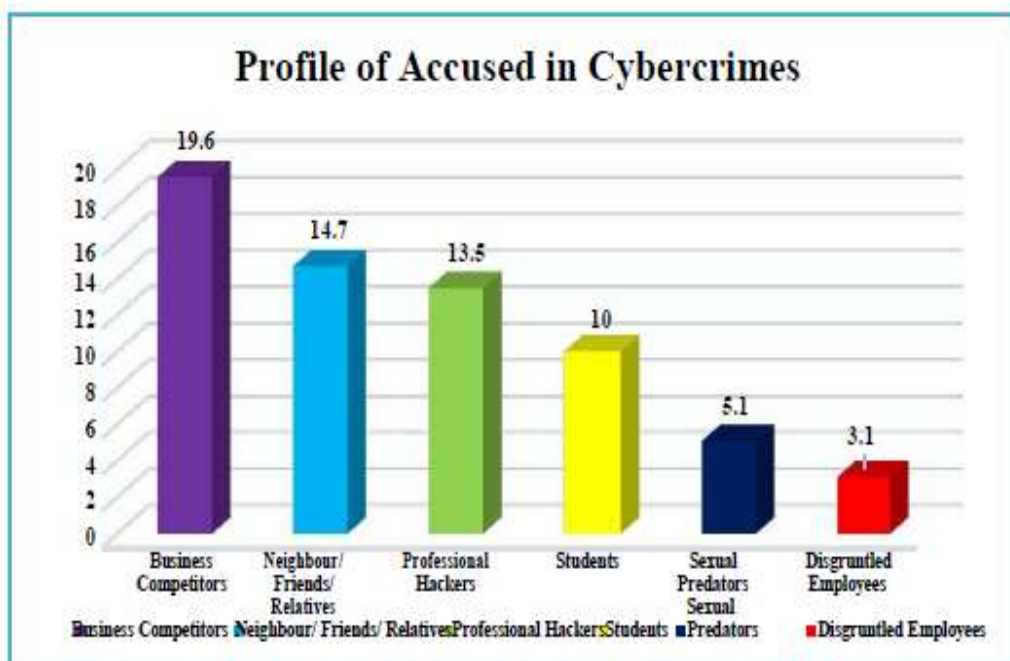
The National Crime Records Bureau (NCRB) said in its 2016 report (for 2015), 11,592 cases of cybercrimes were registered in India, leading to 8,121 arrests. While Uttar Pradesh recorded the highest number of cybercrimes at 2,208, Maharashtra followed closely with 2,195. (Das, 2017) There has been a spike in attacks after demonetisation.

The 18 weeks following demonetisation had not just led to an upward spiral in cybercrime, but also rendered ineffective India's cyber defences, with mobile and digital wallets becoming vulnerable to hacking. The reason, they said, was the absence of legal prevention.



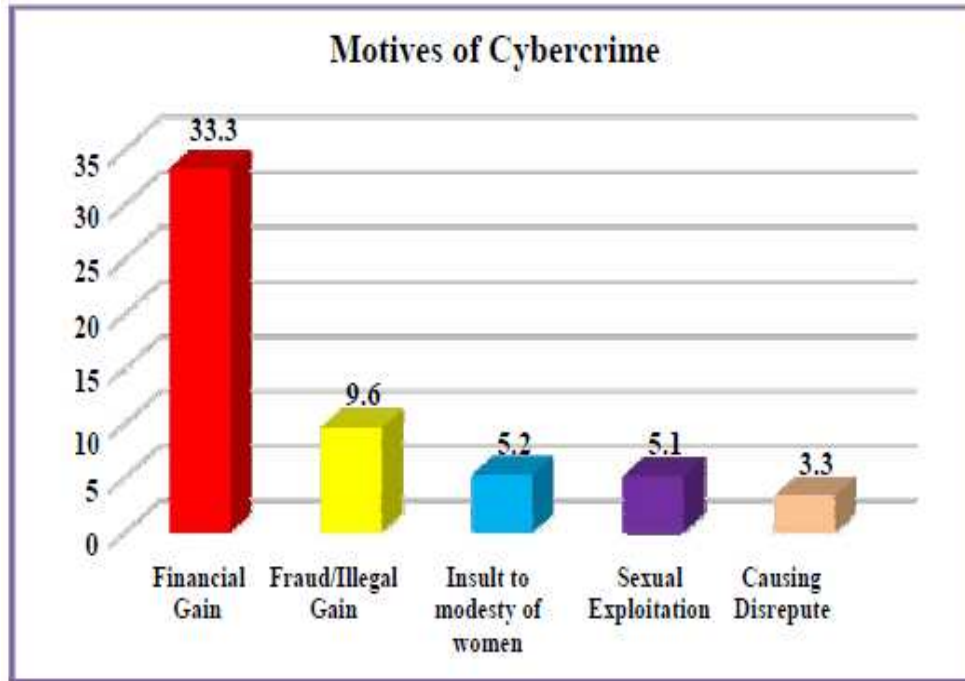
National Crime Record Bureau (NCRB) reports about the Cybercrime cases which reports from 2009 to 2016. That the Cybercrime cases are increasing year by year. The main function of the

NCRB as a source of information on crime and criminals to assist the investigators in linking crime to the culprits.



The profile of accused in Cybercrimes are mainly about the business competitors are leading which we can see in the diagram. This chart which is taken from the NCRB. The below the chart also

depicts about the motive of Cybercrimes by financial gain, illegal gain, insult to modest to women, sexual exploitation and causing disputes.



### TYPES OF CYBERCRIMES WHICH AFFECTS THE CHILDREN

Following are the few examples of cybercrimes which affects the children as well as the users.

#### CYBER TRAFFICKING

Cyber trafficking is one of the means through which the Internet is used for marketing initiatives directed at people using online search functions. It may be trafficking in weapons, drugs, human beings, which affect the large numbers of persons.

#### CYBER HACKING

Hacking among the all types of cybercrime it is the most dangerous and serious threat to the internet and e-commerce. Hacking simply refers to the breaking into the computer system and steals valuable information or data from the system without any permission. Hacking is done by hackers now the question arises who are hackers; hackers are in between client and server and able to spoof the data or information. In other words it is duplication of the IP address illegally.

### MORPHING

Morphing is a special effect in motion pictures and animations that changes one image or shape into another through a seamless transition. In other word morphing is to change smoothly from one image to another by small gradual steps using computer animation techniques. (Kumar S. , 2015)

### IDENTITY THEFT

Identify theft is a form of stealing someone's personal information and pretending to be that person in order to obtain financial resources or other benefits in that person's name without their consent. Identity theft is considered as Cyber Crime. The personal information stolen can include the person's name, social security number, birth date or credit card numbers. This stolen information is then used to obtain new credit cards, access bank accounts or obtain other benefits, such as driver's license. Identity theft can also be performed by hacking into computer networks to obtain personal data-sometimes in large amounts. (Singh B. , 2015)

## **CYBER KIDNAPING**

Cyber kidnapping is defined by the law as the unlawful restraint of a person. Cyber Kidnapping is a Cybercrime which involves unethical hacking of one's offline or online saved data, and then blackmailing the person for the leakage of same data, in exchange of ransom.

## **CYBER BULLYING**

Cyber bullying is a bullying that takes place over digital devices like cell phones, computers, and tablets. The use of information technology to harm or harass other people in a deliberate, repeated, and hostile manner.

## **CYBER EXPLOITATION**

Cyber exploitation is the science of covertly capturing e-mail traffic, text messages, other electronic communications, and other data. Cyber exploitation is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware.

## **CYBER LAWS IN INDIA**

Cyber Laws in India the information Technology Act is an outcome of the resolution dated 30 January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic 17 Commerce on International Trade Law. (Singh A. , 2017)

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

Cyber law encompasses laws relating to –

- Cyber crimes

- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

## **INFORMATION TECHNOLOGY ACT, 2000**

In India, cyber laws are contained in the Information Technology Act, 2000 it is know as IT Act. Which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government Information Technology Act, 2000 is India's mother legislation regulating these of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital or electronic signatures, cybercrimes and liability of network service providers.

## **CYBERCRIME PREVENTION FOR THE CHILDREN**

Cybercrime prevention can be achieved quickly and in a cost-effective manner, the prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It is mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their attack surface and moderate the risks. (Kumar S. , 2015)

## **CYBER CRIME CHALLENGES**

Endless discussion is there regarding the pros and cons of cybercrime. There are many challenges in front of us to fight against the cybercrime towards children. Some of them here are discussed below:

1. Lack of awareness and the culture of cyber security, at individual as well as organizational level.
2. Lack of trained and qualified human power to implement the counter measures.
3. No e-mail account policy especially for the defense forces, police and the security agency personnel.
4. Cyber attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.
5. The minimum necessary eligibility to join the police doesn't include any knowledge of computers sector so that they are almost illiterate to cyber-crime.
6. The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes.
7. Promotion of Research and Development in Information and Communication Technology (ICT) is not up to the mark.
8. Security forces and Law enforcement personnel are not equipped to address high-tech crimes.
9. Present protocols are not self-sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
10. Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes. (Poonia, 2014)

## **REVIEW OF LITERATURE**

This section reports a brief review of research literature wherein the researchers have dealt with the related topics of awareness about cybercrimes, cyberlaws. (Menon, 2003) has revealed that awareness of cybernetics in India is terribly low and thus has gained a reputation as a country where foreign investors can do business

in cybersecurity and have been investing heavily in cybersecurity.

(Pandey, 2006) concluded that lack of awareness about internet and low level of internet security is fast making Indore a heaven for cybercriminals. There has been a steady increase in the number of cybercrimes as people are not aware about the rapid developments in the cyber world. Increasing dependence of common citizens on cybernetics without proper security has made the job easy for cybercriminals.

According to (Kumar K. , 2001) one area that requires special attention is the Cyberlaws awareness in India. Very few users, practitioners and organizations are aware about disputes arising out of IT Act, 2000 and its various amendments. (Hamelink, 2000) found that cybercrime prosecution is not resorted in many instances due to lack of awareness among both the victims and the enforcement authorities about the applicability of general laws to cybercrimes. (Pandey, 2006) has concluded that proactive actions on the part of Government and enhanced participation of education system in the cybersecurity awareness approach may lead to a strongly secured nation.

(Archana Chanuvai Narahari, 2016) Criminals are taking advantage of the fast internet speed and convenience provided by the internet to perform large and different criminal activities, says (Aggarwal, 2015). In her paper, she insisted that it becomes the duty of all the internet users to be aware of the cybercrime and the cyber law made to deal with cybercrimes. She has also discussed the types of cybercrime, which can help people to identify the crime that they have been victim of.

(Parmar, 2016) concluded from their survey that most of the netizens, irrespective of being related to IT field were not able to actively keep themselves updated with the latest information related to cyberlaws and computer security. They

felt that the situation could be ever worse among the netizens who are not associated with IT field. They recommended inculcating basic ethics among netizens, while creating awareness on cyber laws in India.

A similar kind of research is conducted by (Pandey, 2006) to study the awareness about cyber laws in Indian society and found that there is a significant difference between the awareness level of male and female users of internet services and it was established that male netizens are more aware of cyber laws compare to women users.

### **THEORETICAL FRAMEWORK**

Among the Cybercrime theories there are a few, which specifically study on the awareness of parents about cybercrimes against children. Theories shows that the awareness level of the parents on cybercrimes. In studying the cybercrimes the classification and different types of cybercrimes, which will affect the children. The theories like the uses and gratifications theory, protection motivation theory, social learning theory and rational choice theories will make the framework.

### **THE USES AND GRATIFICATIONS THEORY**

The Uses and Gratifications Theory originated in the early 1940s. The theory can be traced to Harold Laswell's Limited Effects Theory and findings on why people chose specific media. Early research focused primarily on descriptions of audience's uses and purposes for choosing the media.

### **PROTECTION MOTIVATION THEORY**

Protection motivation theory play a very important role in the awareness of parents about cybercrimes. It was originally developed to explain the influence of fear invocations on attitudes and to give motivation to the children.

Protection motivation theory is organised around two cognitive processes: the process of threat assessment and the process of handling assessment.

### **SOCIAL LEARNING THEORY**

Social learning theory explains the fact that individuals learn different behaviour and it is not biologically inherent. In this theory there are four main requirements in which social learning occur; First individuals must have a close contact with those they are imitating which can be family members, close friends or teachers. Secondly, individuals must engage in imitation of their superiors. Thirdly, is that they must understand their behaviour This theory takes into account the fact that the behaviour learnt could be negative as well as positive.

### **RATIONAL CHOICE THEORY**

Rational choice theory emergence came about during the late 18th century and came directly from the choice theory. In this theory, its expectations about human behavior have been integrated into many diverse criminological theories and criminal justice arbitrations. People openly accept their behavior and are inclined to the avoidance of discomfort and the pursuit of pleasure.. The rational choice mindset has been applied to a broad spectrum of crimes, including theft, bullying, vandalism, and white-collar crime.

### **RESEARCH GAP**

Several studies have been done on cybercrimes and types of cybercrimes at different levels. The investigator could find negligible work on cybercrime awareness and attitude of parents. By undertaking this problem to study, the investigator will try his best to identify the various facts, laws, and regulations regarding cybercrimes awareness and attitude towards parents about cybercrimes against children.



## **HYPOTHESIS OF THE STUDY**

The hypothesis is a tentative solution of a problem. The research activities are planned in this study is to verify the hypothesis. Hypothesis is used in this study to create awareness among the parents about the cybercrimes against the children.

The following hypothesis are posed for the study:

- H. 1. Parents are unaware about different types of Cybercrimes against children.
- H. 2. Children unknowingly becoming prey to the different types of Cybercrimes.

## **RESEARCH DESIGN AND METHODOLOGY**

### **RESEARCH DESIGN AND METHODOLOGY**

A research design is a master plan specifying the method and procedure for analysing and collecting the need information. It provides the framework to be used as a guide in collecting and analysing data. Descriptive research is used to describe characteristics of a population or phenomenon being studied. The design of a suitable questionnaire and capturing data from different respondents test the hypothesis set for the study and results in coming out clear-cut closing after data analysis. The research design and methodology are important components of the research. Accordingly a quantitative approach is used by the researcher for this research study.

Survey using questionnaire is used in this study as a tool for the data collection. Some of the objectives of the study such as to create awareness about cybercrime to the parents and to gain more knowledge and to eradicate about cybercrime. Which are collected relevant literature from the various sources including search on the internet.

Subsequently, several articles were collected; a bibliography of most relevant documents to the study were identified and compiled. This has

facilitated to get a fairly good picture of the available literature on the topic.

### **UNIVERSE OF STUDY**

The universe consists of all survey elements that qualify for inclusion in the research study. The precise definition of the universe for a particular study is set by the research question, which specifies to create awareness about cybercrime to the parents and to gain more knowledge and to eradicate about cybercrime. In research that involves taking a sample of things for testing and review, the universe may include inanimate objects. Accordingly to the universe for this research is the parents itself which their children age group is 9 to 16 or from 7<sup>th</sup> std to 10<sup>th</sup> std respectively.

### **SAMPLE, TOOLS AND DATA COLLECTION PROCESS**

In this, let us focus on survey, samples and process data collection in elaborate way.

### **SURVEY**

The research strategy in the following research is survey. It is a systematic method of gathering information from a target population, a survey makes use of statistical techniques mainly used in quantitative research. Survey gives us the possibility of gathering enough reliable data.

### **SAMPLES**

When it comes to research, an entire population cannot be examined due to time and resource constraints. It is a representative of the entire population or universe. A small group is selected as representative of the universe by the following scientific method it is known as sampling. Sampling is based on the principle that each unit will get equal chance of selection. We select some of the units using scientific procedure and techniques. (Kishor, 2003)

The sample size of 50 parents from two different churches were selected for the purpose of conducting the survey at random. The study area is selected purposively. Purposive selection of the sample is due to the facts that no studies have been conducted in this area on this topic. 50 parents were selected from two different churches they from Vaishali sector 1 and Mayur Vihar phase 1.

## **PROCESS OF DATA COLLECTION**

The methodology followed was a questionnaire based survey among the parents of the selected areas such as Mayur Vihar phase I and Vaishali Sector I. People are more truthful while responding to the questionnaires regarding controversial issues in particular due to the fact that their responses are anonymous. However, they also have drawbacks. Majority of the parents who receive questionnaires don't return them and those who do might not be representative of the originally selected sample. (Leedy, 2001)

The questionnaire (Appendix-1) comprised of 20 structured questions on various aspects on awareness of parents about cybercrimes against children. Two questions were to collect demographic information, like their age and gender and their children's age range. The questions were classified into five types of mode such as whether their children are access to the internet. The awareness about the cybercrimes to the parents. Different types of cybercrimes, the cyber laws and the action and prevention about the

## **DATA PROCESSING AND ANALYSIS**

Data processing is concerned with editing, coding, classifying, tabulating and charting and diagramming research data. The objective of the study could be achieved by using various tabular techniques to come to a conclusion after analysing the data. The techniques employed to

computer the data are simple calculation through Microsoft excel sheets and column charts. Data will be presented in the form of pie charts and bar graphs for each question.

## **ANALYTICAL FRAMEWORK**

The data after collection has to be processed and analysed in accordance with the outline laid down for the purpose at the time of developing the research plan. This is essential for a scientific study and for ensuring that we have all relevant data for making contemplated comparisons and analysis. The term analysis refers to the computation of certain measures along with searching for patterns of relationship that exist among data-groups. Data analysis is inevitable for two reasons: (1) we test our hypothesis or

Otherwise answer our research questions; (2) we can present the result of the study to our readers in an understanding and convincing manner.

## **CONCLUSION**

The purpose of this study would be highlighting on the awareness of parents about cybercrimes against children. This chapter provides details of the research methodology and procedures used in this study and provides a justification of the research methodology. The focus of this chapter was on the development of the questionnaire and the analytical methods employed to assess the propositions and answer the research questions. This chapter also described the statistical methods employed for the data analysis. The next chapter reports the results of the data analysis.

## **RESEARCH FINDING IN RELATION TO THE HYPOTHESIS**

The research was done with Vaishali sector-1 and Mayur Vihar phase-1 migrant parents from Kerala on regarding with the hypothesis, the findings were that most of them aware about the cybercrimes against children. They do think that

awareness of the parents about cybercrimes will prevent cybercrimes to the children. The data was collected through survey. The parents were selected from two churches namely St. Mary's Church Mayur Vihar phase-1 and St. John Paul II Church Vaishali sector-1. These two churches are mainly malayali families. The survey depicts that majority of the parents are not aware about the different types of Cybercrimes against children.

### **HYPOTHESIS NO 1.PARENTS ARE UNAWARE ABOUT DIFFERENT TYPES OF CYBERCRIMES AGAINST CHILDREN**

In the Chart no. 4.3.1. show that maximum 68% parents are aware about the Cybercrimes in general. However, in the Chart no. 4.4.1.1. to 4.4.1.7. shows that they are unaware about the different types of cybercrimes against children. This shows the ignorance of the parents and the little knowledge they have about the cyber crimes. They may be knowing that there is threat called cybercrime but they do not that their children too were the victims of certain cybercrimes. Therefore the hypothesis i.e., parents are unaware about different types of cybercrimes against children, is proved to be correct from the data collected and verified.

### **HYPOTHESIS NO 2. CHILDREN UNKNOWINGLY BECOMING PREY TO THE DIFFERENT TYPES OF CYBERCRIMES**

In the Chart no. 4.2.1. Shows that 98% children are accessing the internet. It shows that there is a threat always that prowls all over trying to catch, and the children are becoming prey to it without knowledge and ignorance. Some children fall prey to it out of curiosity and while others become victims unknowingly or by some influence by their peer group. The parents by and large 58% knew that their children had affected by cybercrime and many others were afraid about their children's usage of internet as there is always a threat of cybercrime.

## **RECOMMENDATIONS**

- It is suggested that parents should be educated and they can educate their children about the Cybercrimes.
- It is suggested that Government must be strict enough to give punishment to the cybercriminals.
- It is suggested that parent must aware about the different laws that are prescribed for the cyber laws.
- Parent must guide and give knowledge to their children about the different types of cybercrimes that they will be victimised.
- Our educational system should prepare its students with value education and computer education to make use of internet.

## **GENERAL CONCLUSION**

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime from the cyber space. It is quite possible to check them and to recheck them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and to prevent the cybercrimes against children.

The present study was concluded in such a way that the study on the awareness of parent about the Cybercrimes against children. Promoting a culture of cyber security awareness among parents is a key element to the prevention of cybercrime. The parent are not having much knowledge about the different types of Cybercrimes and its consequences. It helps to develop the curiosity among the parents to know and to prevent the Cybercrimes which will affect their children. No doubt, it is not possible to eliminate cybercrime in total. However, it is quite possible to check them. Legislation cannot totally succeed in eliminating crime from the globe. So, let us try to be aware of our rights and duties that is to report the crime as a collective duty towards the society and making the application of laws

stricter to check crime. The study observes that majority of the children are online daily for long period of time due to which their studies are affected negatively resulting in poor academic grades. It is also observed that children who use social networking sites on a regular basis tend to have negative effect on health, anxiety and depression.

The study reflected that the children are having on online addiction in which an individual forgets his/her real life and finds solace in virtual life. This trend makes a person avoid his real life problems and indulge in cyber space. This is having adverse effect to the personality of adolescents who have framed their dual identity one in the real world and another in the virtual world. The present study proves that the Chart no. 4.5.1. to 4.5.2. depicts that Cyber law is highly effective for the development of cybercrime awareness among children as well as parents. The present studies shows that children users belonging to 9-13 years of age group have easy access to internet in comparison with other age groups and they easily convince their parents for the same.

The overall findings indicates satisfactory awareness among all the parents. Results revealed the importance of awareness as a tool to decrease and to prevent cybercrime. Many parents do not want to disclose the fact because of social pressure. Children do not want to share that they face such types of incidents to their parents. Parents and children do not share healthy relationship relating to Cybercrimes.

According to Mr. Nandkumar Saravade experts in cyber security and risk management says that, "lack of user awareness about Internet, cyber laws and risks pose a big challenge in India. When we consider the wide strata of users, from tech-savvy to new users, as well as different socio-economic conditions, demographics, culture and age, making users aware about the risk and saving them from cyber frauds is a challenge

before law enforcement agencies as well as the government." (Money Life, 2015)

Dr. Rakesh Goyal, a PhD holder in cyber security explains, "There are several ways your data can be stolen. Therefore, the next time you put your information on the web, look at the costs versus benefits. Remember, your identity is at stake; your assets are at stake; and your existence is at stake. You should be responsible for your own security." (Money Life, 2015) Let us conclude by quoting from Rakshit Tandon a cyber-security expert "Virtual life: It's not a game, It's your life stay safe!" (Tandon)

## REFERENCES

- [1]. Aggarwal, G. (2015). *General Awareness on Cyber Crime*. Punjab: International Journal of Advanced Research in Computer Science and Software Engineering.
- [2]. Aghatise, J. (2006, June 5). Cybercrime Defination.
- [3]. Archana Chanuvai Narahari, V. S. (2016). Cyber Crime and Security-A Study on Awareness among Young Netizens of Anand (Gujarat State, India).
- [4]. Das, S. (2017, April 6). Retrieved from <http://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html>
- [5]. Desai, S. (n.d.). *Study of Online Cyber Crimes in India*. Retrieved 01 22, 2018, from <http://www.imedpub.com/articles/study-of-online-cyber-crimes-in-india.pdf>
- [6]. Hamelink, C. J. (2000). *The Ethics of Cyberspace*. New Delhi: SAGE Publications.
- [7]. Kishor. (2003). *Hand book of Communication research*. Bhopal: Makhhal Chaturvedi University Publication.
- [8]. Kumar, C. (2017, July 22). *TNN*. Retrieved from TNN: <https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms>

- [9]. Kumar, K. (2001). *Cyber Laws*. New Delhi: Dominant Publishers and Distributors.
- [10]. Kumar, S. (2015). Present scenario of cybercrime in INDIA and its preventions. *International Journal of Scientific & Engineering Research*.
- [11]. Leedy, O. (2001). *Practical Research: Planning and Desig*. Merril Prentice Hall.
- [12]. Menon, S. (2003). *Protection of Intellectual Property in Cyber Space*. Delhi: Authors Press.
- [13]. *Money Life*. (2015, July 21). Retrieved from Money Life: <https://www.moneylife.in/article/your-awareness-is-important-to-prevent-cyber-crime/42860.html>.
- [14]. Nayak, S. D. (n.d.). Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=8A7B0A9C59BB3FC044AF979DF836A168?doi=10.1.1.429.548&rep=rep1&type=pdf>.
- [15]. News, B. (2013, November 19). 'Selfie' named by Oxford Dictionaries as word of 2013. Retrieved October 15, 2016, from <http://www.bbc.com/news/uk-24992393>.
- [16]. Oldham, J. M. (1995). *The New Personality Self-Portrait: Why You Think, Work, Love and Act the Way You Do*. New York: Bantam.
- [17]. Oxford. (2013, November 19). *The Oxford Dictionaries Word of the Year 2013*. Retrieved October 15, 2016, from <http://blog.oxforddictionaries.com/press-releases/oxford-dictionaries-word-of-the-year-2013/>.
- [18]. Pandey, A. (2006). *Cyber Crimes Detention and Prevention*. New Delhi: Jain Book Agency Publishers.
- [19]. Parmar, P. K. (2016). *Critical Study and Analysis of Cyber Law Awareness Among*
- [20]. *Netizens. Conference: International Conference on ICT for Sustainable Development*. Retrieved from [http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2\\_32](http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32).
- [21]. Poonia, A. S. (2014). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 119-121.
- [22]. Saroj Mehta, V. S. (2013, January 1). A STUDY OF AWARENESS ABOUT CYBERLAWS IN THE. *International Journal of Computing and Business Research (IJCBR)*.
- [23]. Singh, A. (2017). Studies Report on Cyber Law in India &. *International Journal of Innovative Research in Computer*.
- [24]. Singh, B. (2015). A study of cyber crime awareness and attitude towards internet of college students of haryana state.
- [25]. Sorokowski, P. (2015, May 15). *Selfie posting behaviors are associated with narcissism among men*. Retrieved October 18, 2016, from <http://www.sciencedirect.com>.
- [26]. Tandon, R.(n.d.).Retrieved from rakshit tendon Web site: <http://www.rakshittandon.com/index.html>.
- [27]. Theresa M. Senft, N. K. (2015). What Does the Selfie Say? Investigating a Global Phenomenon. *International Journal of Communication*, 1588–1606.
- [28]. Tisnadibrata, I. L. (2014, June 16). *Small-screen Addiction*. Retrieved October 16, 2016, from <http://www.bangkokpost.com>.
- [29]. [http://www.bangkokpost.com/print/415628/Yougal Joshi, A. S. \(n.d.\). A Study on Cyber Crime and Security Scenario in INDIA](http://www.bangkokpost.com/print/415628/Yougal%20Joshi,%20A.%20S.%20(n.d.).%20A%20Study%20on%20Cyber%20Crime%20and%20Security%20Scenario%20in%20INDIA).
- [30]. Retrieved 01 22, 2018, from [http://www.ijemr.net/DOC/AStudyOnCyberCrimeAndSecurityScenarioInINDIA\(13-18\)48f66c6f-4d11-4f64-95ec-a3600f6cd9d3.pdf](http://www.ijemr.net/DOC/AStudyOnCyberCrimeAndSecurityScenarioInINDIA(13-18)48f66c6f-4d11-4f64-95ec-a3600f6cd9d3.pdf).