TECHNOLOGY MEDIATED INTERPERSONAL CRIMES AMONG HIGHER SECONDARY SCHOOL STUDENTS

SNEHA T.S.

Dissertation submitted to the
University of Calicut for the partial fulfilment
Of the requirements for the Degree of
MASTER OF EDUCATION

FARROOK TRAINING COLLEGE
UNIVERSITY OF CALICUT

2020

DECLARATION

I, **SNEHA.T.S,** do hereby declare that this dissertation entitled, **TECHNOLOGY MEDIATED INTERPERSONAL CRIMES AMONG HIGHER SECONDARY SCHOOL STUDENTS ,** has not been submitted by me for the award of any Degree, Diploma, Title or Recognition before.

Farook College

Date: **SNEHA.T.S**

Dr. T.K. UMER FAROOQUE
Assistant Professor
Farook Training College
Calicut

CERTIFICATE

I**, Dr. T.K. UMER FAROOQUE .,** do hereby certify that the dissertation entitled, TECHNOLOGY MEDIATED INTERPERSONAL CRIMES AMONG HIGHER SECONDARY SCHOOL STUDENTS **,** is a record of bonafide study and research carried out by **SNEHA.T.S** ,of M.Ed Programme (2018-20), under my supervision and guidance, and has not been submitted by her for the award of any Degree, Diploma, Title or Recognition before.

Farook College,
Date: **Dr. T.K. UMER FAROOQUE**

Acknowledgement

The investigator at the very beginning thanks God Almighty, the most merciful and generous, who helped her to complete the mission successfully.

The investigator is deeply indebted to her supervising Teacher, ***Dr. T.K. UMER FAROOQUE.,*** *Assistant Professor, Farook Training College, for his constant encouragement, generous help and valuable suggestions combined with expert criticism.*

The investigator would like to express her profound gratitude to Prof. ***Dr. C. A. Jawahar,*** *former principal, Farook Training College and* ***Dr. Mohammed Saleem .T,*** *Principal, Farook Training College, for their whole hearted co-operation in extending the facilities and encouragement to conduct this study.*

The investigator express her sincere thanks to ***Dr. Niranjana K.P.,*** *Assistant Professor, Farook Training College, for providing support and coordinating the two year M.Ed. programme effectively.*

Sincere thanks are extended to all faculty members and special thanks to the Librarian, ***Mrs.Sabira. M.****, library staff and office staff of Farook Training College, for their support and encouragement throughout the study.*

The investigator is obliged to the principals, teachers and students of various secondary school in Calicut district who extended their support to collect the data related to the study.

Finally the investigator is deeply indebted to her parents, family and friends for providing whole-hearted support and help to complete the task successfully.

Farook Training College, **SNEHA.T.S.**

CONTENTS

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

- **Need and significance of the study**
- **Statement of the problem**
- **Definition of key terms**
- **Variable of the study**
- **Objectives of the study**
- **Hypotheses of the study**
- **Methodology**
- **Scope and Limitations of the study**
- **Organization of the report**

Education provides young people with knowledge and experience by adults or by more experienced individuals. Education has existed since the time of man. Since the dawn of civilization, education is believed to have been responsible for the cultivation of civilized society. The provision of education to citizens enables the development of a responsible and thoughtful society. Without education it is difficult for both individuals and society to make any progress and prosperity.

Technology has affected almost every aspects of life today, and education is no exception. The teacher lectures on the podium in front of the room while the students sit in the rows and listen. Some of the students have books opened in front of them, and they seem to follow along. Well, a few look bored. Some of them are talking to their neighbors. Some of the students might be sleeping. Classrooms today do not really look much different; though you might find modern students looking at their laptops, tablets, or Smart phone’s instead of books (even if definitely open to Facebook). Optimists would say that technology has done nothing to change education. Technology, however, has fundamentally altered education in many respects. Technology, for example, has significantly expanded access to education. In medieval times, books were scarce and few people had access to educational opportunities. Individuals needed to fly to the study centers to get an education. Today, a large amount of material (books, audio, pictures, videos) are accessible on one's reach via the Internet, and resources for formal learning are available online worldwide through the Khan Academy, MOOCs, podcasts, formal college graduation programs, and more. Due to technology, exposure to learning opportunities today is unique in scope. Opportunities for communication and collaboration have also been expanded by technology.

We use technology everyday everywhere in order to fulfill a particular duty or our specific interest .The technology helps us in many ways from morning till evening. People from all the age groups benefit from technology until and unless they know how to access the same. But one must never forget that anything that comes to us has its own advantages and disadvantages

There are various benefits of technology. Technology has made communication much easier than ever before by the introduction of advanced and modified innovations of phones and applications. Not only in the professional world but also in the house old sphere, technology has contributed a lot. Most of the technology that we have around us gets with a lot of changes from the past inventions. In the entertainment sector, we have more techniques to provide the audience with a real time experience. There are more games, better musical instruments; better visual systems like smart TV'S .Great success has been achieved in social networking by connecting millions of people at one umbrella. In several countries around the world, the Internet, smart phone phones and information technology are now integrated in the societal systems of banking, health, education and industry.

Despite all these advantages there are some disadvantages as well, which have negatively affected the importance of technology. A study reveals that mobile devices and the internet are primarily used by youth for communication and staying connected with peers; there is a perceived social aspect to these devices. Devices today have significantly greater computing power and functionality and are continually decreasing in their physical size. However the rise of crimes increased with the increase in the devices, (Glasner ,2010). Another rising problem that has been witnessed is unemployment. Due to the over practice and much involvement of technology, the machinery has replaced human labor leading in unemployment in so many sectors. Due to the presence of social applications like whatsapp, facebook, and twitter, etc the actual social isolation has increased leading to depression and increased loneliness cases amongst the youngsters. The increased dependency of humans on technology has even affected the intelligence and creativity of children. Our nation is a developing nation in the context of technology and science. So, we must know how to make wise utilization of technology without creating hindrance in the growth of an individual, mentally as well as physically. The openness and reliability of the Internet and information technologies in promoting society institutions networks also promote the growth of technology mediated crimes and deviant subcultures.

Study reveals Social media usage in particular has increased dramatically over the last decade and continues at an incline. Research Center indicates that 71% of 13- to 17-year-olds use Facebook, 52% use Instagram, and 41% use Snapchat in 2015. Teenage girls are also using image-based social media platforms more frequently than their male counterparts; 61% of girls use Instagram versus 44% of boys. This increase in usage of social media, especially Facebook and Instagram, may negatively affect adolescent girls and young women in regard to their self-confidence and body satisfaction (Lenhart, 2015).Another study shows the risk of cyberbullying, sexual victimization, or harassment from others is real and pervasive (Federal Bureau of Investigation, 2011).

The study ‘Social Networking Sites raging craze among teens’ by Mishra (2013) points out the rapid growth and popularity of social networking sites such as Facebook and Orkut in society. As information is easily accessible on these social networking sites, students rely on these sites blindfold. It reduces the learning and research capabilities of students. The adolescents are eager to join these sites in spite of proposed age limit, otherwise they are termed as old fashioned and out dated. These sites have become a medium of fashion symbol as teens upload their latest photographs on these and expect to receive comment. Moreover, psychiatrists say that the teens who involve in many activities on social networking sites while studying, results in less attention, which eventually causes poor academic performance.

The present study is an attempt to analyze the awareness on technology mediated interpersonal crimes using technological gadgets like Smartphone, PC, notebook, tablet etc. The advancement in technology increased the usage of gadgets increased among people. The study focuses on higher secondary school students who falls under the period of stress and strain storm and strife. This may lead them to commit crime using such gadgets without proper awareness. So it is necessary to know the awareness level of higher secondary school students on Technology Mediated Interpersonal Crimes.

Need and Significance of the Study

The present study explores the awareness on Technology Mediated Interpersonal Crimes among Higher Secondary School Students. Here the interpersonal crimes means the intentional use of physical force or power against oneself, another person or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological harm, imperfect development or deprivation. So the study intends to find out the awareness on technology mediated interpersonal crimes among higher secondary school students.

A wide range of devices are in use today, including smart phones, media players, tablets, and notebook PCs. As well as the use of internet seems to be increased in the present scenario. Social media is the most recent type of media and has many features and characteristics. There are several facilities on the same platform, such as email, messaging, sharing images, audio and video sharing, fast publishing, linking with the world, direct connectivity. It's also cheapest to have quickest exposure to the internet, so it's very relevant for people of all ages. Its usage is growing on a regular basis with a high pace throughout the world. The majority of young people transition rapidly from mainstream media as TV viewers and radio listeners to social media in all age groups. As the advancement made by technology the rate of crimes committed by using such media got increased day by day.

The study intends to analyze the awareness on technology mediated interpersonal crimes among higher secondary school students. Majority of studies reveal that no particular gender is targeted in victimisation more than the other (Hinduja and Patchin, 2008, Williams and Guerra, 2007, Vajras Et Al., 2009)

.Another study reveals that the seriousness of crimes committed using such computers and mobile phones are often not understood: one third of respondents in a study believed that cyberbullying is not hurtful (Cassidy et.al., 2009). Further, evidence from Cassidy et al. (2009) suggests that girls and boys receive qualitatively different attacks, whereby the content of attacks on girls is sexual in nature.

Again regarding the Awareness of students on the Technology Mediated Interpersonal Crimes several studies have been conducted. One of the researches is on cyber crime awareness among XII students in Bathinda, Punjab. It was found out that the gender of the students does not create a difference in the level of awareness of cybercrime. The stream chosen by the students also does not play a part in the awareness level (Jagvinder Singh ,2012). Another study focuses on the awareness of cyber crime laws in India. It states that even though there exist firewalls, antivirus and many other effective measures to control cybercrime, India is still far behind in combating cybercrime. It was found out that there lies a significant difference between the awareness level of male users and female users (Saroj Mehta and Vikram Singh's, 2013).

It was found that that e-frauds and identity thefts have caused financial loss on a global level and is a challenge for the nation's infrastructure and security. Further, cyber criminals are using networks to commit traditional crimes online such as child pornography and pirated software .Legislation and effective enforcement is needed to counter attack viruses, hackers and terrorists. However, the authors have not discussed the effects of cyber crime on society. They have limited themselves on technical issues (Heuven and Botterman, 2003)

Beck (1992) labels the contemporary world as both industrial society and risk society. The indiscriminate use of technology has associated risks which are yet not traceable. Due to the complexity of society and technological advancement, new crimes especially cyber crime have grown creating new type of risk for individuals, organizations and for society

Different studies reveal that technology mediated interpersonal crime among youngsters using such media shows a hike. Some of the crimes noted are hacking, cyber defamation, cyber staking pornography, identity theft, cloning or recapping, phishing, credit card crime, happy slapping, software piracy etc.

We know that higher secondary school students are the adolescent students. It is a period of storm and stress, a period of biological growth and development, an undefined status, increased decision making, increased pressure and the search for self. With the advancement of technology adolescent also adopt themselves to accept the changes. The use of social media is increasing day by day among them. So there is an increased chance for committing crimes using social media. Therefore, it is necessary to know whether the adolescents are committing technology mediated crimes by knowing it is a crime or unknowingly getting into crime. The study intends to explore the awareness level on technology mediated interpersonal crimes among the higher secondary students.

It is important to say that a good family produces a good citizen. Good teachers create a good Student. Here lays the role played by family and teachers in the socialization of the child. Parents at a broader level can raise awareness to the community about this social phenomenon. It is high time for our people to rethink on the ways they adopt for social concerns and issues. We should make more effective efforts to make children aware about technology mediated crimes by organizing seminars, debates on illegal activities committed through the internet. By all means we can save our children from committing such crimes.

There are many studies conducted in the area of cyber crime. However there are no studies conducted in India especially in Kerala. So this study is a relevant and significant study.

Statement of the Problem

The present study is entitled as "**TECHNOLOGY MEDIATED INTERPERSONAL CRIMES AMONG HIGHER SECONDARY SCHOOL STUDENTS"**

Definition of Key Terms

Technology Mediated Interpersonal Crimes

The intentional use of physical force or power against oneself, another person or against a group or community that either results in or has a high likelihood of resulting in injury death, psychological harm, imperfect development or deprivation.

For the present study technology mediated interpersonal crimes mean that the crimes by using technological gadgets like smart phone, tablet, smart phone, laptop PC's etc. The technology mediated interpersonal crimes such as Cyber bullying, Cyber Defamation, software piracy, Hacking & Cracking, Child

Pornography, Spoofing, Credit Card Fraud, Internet Relay Chat Crime, Cyber Theft, Cyber Squatting, E-mail Spamming, Denial of Service attacks, Forgery, Investment Frauds, Data Diddling, Espionage, Sniffing Attack, Cyber Stalking, Salami Slicing Attack, Happy Slapping, Phishing, Cyber Terrorism are considered for the study.

Higher Secondary School Students

Students who are studying in plus one and plus two are called higher secondary school students.

In the present study students studying at the plus one classes were considered higher secondary school students.

Variable of the Study

Technology Mediated Interpersonal Crime is the only variable for the present study

Objectives of the Study

1. To find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students for the total sample and the relevant subsamples based on gender, locale of the students and type of management of schools.

2. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

3. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

4. To find out whether there exist any significant difference in the awareness on technology mediated interpersonal crimes for the subsample based on type of management of schools.

Hypotheses of the Study

1. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

2. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

3. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes for the sub sample based on type of management of schools.

Methodology

Method

For the present study survey method was used as the method of research

Sample

For the present study 600 higher secondary school students from various higher secondary schools in Kozhikode district were selected as sample by using stratified random sampling technique. Due weightage was given to the sub samples like gender, locale of the students and type of management of schools.

Tool Used for the Study

Awareness test on Technology Mediated Interpersonal Crimes.

An awareness test on technology mediated interpersonal crimes was developed by the investigator with the help of supervising teacher.

Statistical techniques used

In the present study the collected data were analyzed by the following techniques.

1. Descriptive statistics like mean, median, mode, standard deviation, skewness and kurtosis

2. Test of significance of difference between mean scores

Scope and Limitations of the Study

The present study is intended to investigate the extent of awareness of technology mediated interpersonal crimes among higher secondary school students in Calicut district. While selecting the sample, due emphasis was given to make the sample a true representative of the population. The prepared awareness test was administered to a sample of 600 higher secondary school students. The study helps to know the level of awareness of students on technology mediated interpersonal crimes.

Some limitations crept into the study. The limitations of the study were:

1. The study was confined to only one district of Kerala.
2. The study intends to check only the awareness level of students on technology mediated interpersonal crimes.
3. The study was conducted among students of standard XI assuming that it is the representation of the two standards of higher secondary school education viz., standard XI and XII as sub sample.
4. The investigator considered gender, locale, and type of management of schools.
5. Sub groups like subject of specialization, socio economic status were not included in the study.

Organization of the Report

The report is presented in five chapters.

Chapter I consist of a brief introduction to the problem, need and significance, statement of the problem, definition of key terms, variable, objectives, hypothesis ,methodology, sample, tool used for the study, statistical techniques, scope and limitations of the study and organization of the report

Chapter II presents the theoretical overview of the concerned variables and review of related studies.

Chapter III gives an account of the methodology in detail used for the present study. It consists of Variable, Objectives, Hypotheses, Tool Used for Data Collection, Sample, Data Collection Procedure, Scoring and Consolidation of Data and Statistical Techniques used for Data.

Chapter IV shows the analysis of collected data made my different statistical techniques required as per objectives of the study.

Chapter V presents summary, major findings of the Study, Tenability of Hypotheses, Educational Implications and Suggestions for Further Research

CHAPTER II

REVIEW OF RELATED LITERATURE

- **Theoretical Overview of the Variable.**
- **Studies related to Technology Mediated Interpersonal Crimes.**
- **Conclusion**

REVIEW OF RELATED LITERATURE

Review of related literature is an important aspect of any investigation. A proper study of related literature would enable the investigator to locate and go deep in to the problem. Review of the related literature helps the researcher to acquaint himself with current knowledge in the field or area in which he is going to conduct his research. It enables the researcher to delimit and define his problem and thus to state objectives clearly and concisely. The knowledge of related literature brings the researcher up to date on the work which others have done. Thus a thorough examination of the related literature will help a researcher to understand the significance of present study and to build a new approach to the same.

Review of related literature helps a researcher to give a deep insight to the design of the study, it helps to show whether the evidence already available solves the problem adequately without further investigation and others to avoid the risk of duplication.

Practically all human knowledge can be found in books and libraries. So an extensive use of the library and thorough investigation of related literature are essential in planning and carrying out the kind of searching involved.

The present study is an attempt to find out the awareness level of technology mediated interpersonal crimes among Higher Secondary School students. The first section deals with the theoretical overview of the variable and second section deals with the various studies carried out by the researchers by using the variable under consideration.

Theoretical Overview of the Variable.

Studies related to Technology Mediated Interpersonal Crimes.

Theoretical Overview of Technology Mediated Interpersonal Crimes

The intentional use of physical force or power against oneself, another person or against a group or community that either results in or has a high likelihood of resulting in injury death, psychological harm, imperfect development or deprivation is known as interpersonal crimes.

The technology mediated interpersonal crimes are those crimes committed by using technological gadgets like smart phone, tablet, smartphone, laptop PC's etc. The technology mediated interpersonal crimes such as Cyber bullying, Cyber Defamation, software piracy, Hacking & Cracking, Child Pornography, Spoofing, Credit Card Fraud, Internet Relay Chat Crime, Cyber Theft, Cyber Squatting, E-mail Spamming, Denial of Service attacks, Forgery, Investment Frauds, Data Diddling, Espionage, Sniffing Attack, Cyber Stalking, Salami Slicing Attack, Happy Slapping, Phishing, Cyber Terrorism are considered for the study.

Technology mediated interpersonal crimes

Cyber bullying

Cyber bullying is a form of bullying that takes place via internet connected devices like smart phones, computers, or tablets. Cyber bullying can occur via social media, email, messaging apps, text messages, forums, games, and more. Any online medium that allows for the sharing of information can become a platform for cyber bullying.

Cyber bullying is the use of technology to intimidate, harass, threaten, torment, or humiliate a target. Examples of cyber bullying including sending mean texts, posting false information about a person online, or sharing embarrassing photos or videos.

Cyber Defamation

Cyber Defamation is the intentional infringement of another person's right to his good name and tarnishing the image, respect or dignity of any person in front of right thinking members of the society through the electronic gadgets.

Software Piracy

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software. Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Hacking & Cracking

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destroy and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Crackers may steal or modify data or insert viruses or worms which damage the system. By hacking a web server taking control of another person's website is called web hijacking.

Child Pornography

Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc. There are more than 420 million individual pornographic web pages today. Child pornography is a very unfortunate reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

Spoofing

Spoofing means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained actual password. He creates a new identity by fooling the computer into thinking he is the genuine system operator. The hacker then takes control of the system. He can commit innumerable number of frauds using this false identity. In short spoofing refers to thing that appears to have been originated from one source when it was actually sent from another source.

Credit Card Fraud

Online Transaction has become a normal thing in day today life. Knowingly or unknowingly passing credit card information over the internet can land you in trouble. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

Internet Relay Chat Crime

Internet Relay Chat (IRC) is a protocol for real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message as well as chat and data transfer, including file sharing.

1. Criminals use it for meeting co-conspirators.
2. Hackers use it for discussing their exploits / sharing the techniques
3. Adult with psychiatric disorder (Pedophiles) use chat rooms to allure small children

Cyber Theft

Stealing of financial and /or personal information through the use of computers for making its fraudulent or other illegal use.

Identity Theft:- Identity theft occurs when someone appropriates another’s personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

Theft of Internet Hours:- Unauthorized use of Internet hours paid for by another person. Theft of computer system (Hardware):-This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

Logical bombs are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Cyber Squatting

The term Cyber Squatting refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names. Cyber squatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner. Both the federal government and the Internet Corporation for Assigned Names and Numbers have taken action to protect the owners of trademarks and businesses against cyber squatting abuses.

E-mail Spamming

E-mail "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter is called email spamming. Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam.

Denial of Service attacks

Flooding a computer resource with more requests than it can handle. This causes the resource to crash there by denying access of service to authorized users.

Forgery

Forgery involves a false document, signature, or other imitation of an object of value used with the intent to deceive another. Those who commit forgery are often charged with the crime of fraud.

Investment Frauds

Investment fraud is an offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing. in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatically changing the financial information for some time before processing and then restoring original information.

Software Piracy

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software. Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Espionage

Espionage or spying is the act of obtaining secret or confidential information or divulging the same without the permission of the holder of the information. Spies help agencies uncover secret information. Any individual or spy ring (a cooperating group of spies), in the service of a government, company or independent operation, can commit espionage. The practice is clandestine, as it is by definition unwelcome. In some circumstances it may be a legal tool of law enforcement and in others it may be illegal and punishable by law. Espionage is a method of gathering which includes information gathering from undisclosed sources.

Sniffing Attack

Sniffing attack or a sniffer attack, in context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.

Cyber Stalking

Stalking refers to repeated unwanted intrusive behaviors that result in the victim experiencing fear, physical or psychological harm or emotional distress .Cyber stalking refers to stalking activities conducted in ‘cyber space’ using information and communication technologies.

Salami Slicing Attack

A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size. Although salami slicing attack is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well .The attacker uses an online database to seize the information of customers that is bank/credit card details deducting very little amounts from every account over a period of time. The customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

Happy Slapping.

The practice whereby a group of people assault a stranger at random while filming the incident on a mobile device, so as to circulate the images or post them online.

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Cyber Terrorism

The concept of cyber terrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks.

Development of technology mediated interpersonal crimes

The illegal misuse of information technology and the required legal response are problems which have been addressed since the advent of technology. Over the last 50 years, numerous approaches have been introduced at national and regional level. One of the reasons why the issue remains a challenge is constant technological progress, as well as changing strategies and means of committing offences.

In the 1960s, the introduction of transistor-based computer systems that were smaller and cheaper than vacuum tube-based machines led to an increase in the use of computer technology. At this early stage, the crimes focused on physical damage to computer systems and stored data. Such incidents have been reported, for example, in Canada, where a student riot caused a fire in 1969 that destroyed computer data stored at the university. In the mid-1960s, the United States launched a debate on the creation of a central data storage authority for all ministries. Within this context, possible criminal abuse of databases and the related risks to privacy were discussed.

In the 1970s, the use of computer systems and computer data increased further. At the end of the decade, an estimated number of 100 000 mainframe computers were operating in the United States. With falling prices, computer technology has been widely used in the administration and business sectors and by the public. The 1970s were characterized by a shift from traditional property crimes against computer systems that dominated the 1960s to new forms of crime. While physical damage continues to be a relevant form of criminal abuse of computer systems, new forms of computer crime have been identified. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud. Multimillion dollar losses have already been caused by computer-related fraud at this time. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cyber crime. Interpol discussed the phenomena and possibilities for legal response.

In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and patent-related crimes. The interconnection of computer systems has led to new types of offences. Networks allowed offenders to enter a computer system without being present at the crime scene. In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the process. OECD and the Council of Europe set up study groups to analyze the phenomena and evaluate possibilities for legal response.

The introduction of the graphical interface ('WWW') in the 1990s, followed by a rapid increase in the number of Internet users, has led to new challenges. Information legally made available in one country has been made available globally – even in countries where such information has been criminalized. Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were generally local crimes, the Internet has transformed electronic crimes into transnational crimes. As a result, the international community has dealt with this issue more intensively. The UN General Assembly Resolution adopted in 1990 and the Computer Crime Prevention and Control Manual issued in 1994 are just two examples.

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. As in every previous decade , new trends in cybercrime and cybercrime have continued to emerge in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing" and "botnet attacks," and the emerging use of technology that is more difficult for law enforcement to manage and investigate, such as “voice-over-IP (VoIP) communication” and “cloud computing”. It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

Studies related to Technology Mediated Interpersonal Crimes

Joseph B. Walther (1992) through their study on Interpersonal Effects in Computer-Mediated Interaction a Relational Perspective points out that, several theories and much experimental research on relational tone in computer-mediated communication (CMC) points to the lack of nonverbal cues in this channel as a cause of impersonal and task-oriented messages. Field research in CMC often reports more positive relational behavior. This article examines the assumptions, methods, and findings of such research and suggests that negative relational effects are confined to narrow situational boundary conditions. Instead, it is proposed that communicators use cumulative CMC messages to create individual experiences of others. Users may establish relationships based on these experiences and convey multidimensional relational messages through verbal or textual indications. Predictions are suggested about these systems, and it is recommended for future work for integrates these criteria.

William F. Skinner, Anne M. Fream(1997) through their study ,A Social Learning Theory Analysis of Computer Crime among College Students portraits that computer crime is a fairly recent field of criminological and deviant science. Despite the exception of Hollinger, few studies investigated the phenomenon of illicit code activities and almost none sought to provide a theoretical explanation for the behaviour. Throughout this report, the authors include data on the prevalence of five illicit computer practices from a multistage study (N=581) of students at a southern university over the history, past year, and last month. The writers also investigate the etiology of computer crime by examining social learning theory's ability to describe these behaviours. Using multiple regression methods, they demonstrate that differential correlation steps, differential strengthening and punishment, concepts, and sources of imitation are significantly linked to computer crime. Findings from this analysis are contrasted with results from Hollinger and explored in terms of why the theory of social learning is a fitting and valuable theoretical framework for understanding why college students.

Furnell ,Steven (2002) in their book *Cybercrime: vandalizing the information society* speaks asbout multiple hacking instruments and abilities. He characterizes viruses of malware and events involving malware. Not only this, Furnell observes the effects of hacking on society, politics and business. He defines hackers as the members of a contemporary society's evolving subculture. He also identifies the causes of the hacker's negative stereotyping development. But the means and measures to control hacking have not been discussed by Furnell.

Spitzberg, B. H., & Hoobler, G.(2002) conducted a study on Cyber stalking and the technologies of interpersonal terrorism they reveals that despite widespread mainstream press reporting of the internet's dark side, no social science work has yet been conducted on the subject of cyber stalking. This study summarizes three pilot studies performed in the course of creating a satisfactorily factorial complex measure of cyber stalking victimization, and then examines the frequency of such victimization, and its interrelationships with obsessive relational intrusion. Findings suggest that a nontrivial proportion of the sample experiences cyber stalking, and that there are limited but generally stable associations between aspects of cyber stalking and spatially dependent stalking. Furthermore, the findings indicated that only interactional ways of coping were reliably associated with ways of cyber stalking.

Brian D. Ng, Peter M. Wiemer-Hastings(2005) study on Addiction to the Internet and Online Gaming states that With the use of computers and the Internet is a part of everyday life, the opportunity for overuse is added, which may lead to addiction. Internet addiction study has found people could become addicted to it. Internet addiction shares some of the negative characteristics of drug abuse which has been seen to lead to outcomes such as school failure, family loss which relationship issues.

Majid (2006) says that new crimes are appearing at a fast rate and ancient crimes are disappearing or changing form, and what counts as a crime differs across cultures. As Majid Yar points out,' academic criminology has been slow in reorienting itself to cyber-world events.' He has discussed at length the Internet's emergence and growth and the role it plays in a new range of everyday activities, the extent of cyber criminal activity, and the problems associated with measuring it. The author cites numerous examples of how cybercrime has had a adverse impact on society. Different forms of cybercrime such as hacking, pornography, piracy, and speech online hate, e-fraud, identity theft, etc. are discussed in general. One of the important points the author raises is that crime and deviance in criminal investigation cannot always be strictly segregated. The dynamics in which the borders between criminal and deviant are socially negotiated are a recurring characteristic of the web-based modern events. As an inherently de-territorialized phenomenon, cybercrime has presented fresh difficulties to police and criminal justice. In addition, fresh issues emerge due to resource constraints and inadequate knowledge. An significant issue that the author does not answer is whether information and communications technologies are enablers of crime or enhancers of crime.Not only that some of the latest high-tech offences are not included by Yar;dangers presented to critical infrastructure by people and structured organizations owing to political or religious motivations and the risks connected with the new payment system. In the technical globe, as we are increasingly moving forward, we need to tackle these future problems.

E. Kraft (2006) made a study on Cyber bullying: a worldwide trend of misusing technology to harass others . The study says Technology has led to a new form of bullying in the 21st century called cyber bullying. Cyber bullying is using the Internet or a cell phone to harass a victim with pictures and text. There have been reports in the media of youth being harassed by e-mail, postings on websites, instant messages, and mobile text messages worldwide. This study summarizes findings about the prevalence and effects of cyberbullying from studies conducted in Australia, Canada, the United Kingdom, and the United States. Results of the studies were compared to media reports of cyberbullying and traditional bullying research. Strategies to stop and prevent cyberbullying were discussed. The percentage of respondents experiencing incidents of cyberbullying in the studies ranged from 10% to 42%. The mobile phone was the predominant method of cyberbullying in Australia and the United Kingdom, whereas the Internet was the favoured method in the United States and Canada. Some victims of cyberbullying have been driven to suicide while others remain unaffected by it. The most common feelings of victims were anger, sadness, frustration, and fear. Independent studies in the United States, United Kingdom, and Canada documented that parents and children do not discuss cyberbullying. It is recommended that schools establish and post acceptable use policies for the Internet. Parents need to be educated about cyberbullying so that they can impose consequences if their child is harassing another child. Real time computerized reporting systems such Text Someone can be used to augment reporting of incidents. Showing students how mobile phone calls and e-mail messages can be traced may deter cyberbullying.

Michel L Pittaro (2007) made a study on Cyber stalking: An Analysis of Online Harassment and Intimidation. The study says culture has come to rely on the sheer scale, technical capacity, and quick speed of the Internet to scan for unparalleled information sites, discover the unseen, and interact with practically everyone across the world, wherever, and whenever. The Internet, on the other hand, has opened portals of previously inaccessible criminal incentives that not only threaten, but also overcome all physical borders, borders, and limits to track, deter, and reduce what appears to be an growing global epidemic. As such, the Internet has practically become a fertile breeding ground for a totally new and unusual form of criminal attacker known hereafter as the cyber stalker–a perpetrator who uses the Internet as a device or weapon of sorts to prey on, annoy, intimidate and create extreme terror and trepidation in his victims by advanced stalking techniques. This report provides a look into the deviant practices and strategies associated with cyber-stalking activities, regulatory response mechanisms and prevention programs explicitly designed to combat this growing global epidemic.

Peter K. Smith, Jess Mahdavi, Manuel Fontes Carvalho, Sonja Fisher, Shanette Russell, Neil Tippe T (2008) conducted a study on Cyber bullying: its nature and impact in secondary school pupils . Cyber bullying explains the use of cell phones and the Internet for bullying. Most recent research has concentrated on text message frequency and email bullying. Two studies of pupils aged 11-16 years: (1) 92 pupils from 14 schools, supplemented by focus groups; (2) 533 pupils from 5 schools, evaluating the generalizability of results from the first report, and exploring associations between cyber bullying and general use of the internet. Both studies distinguished cyber bullying inside and outside school, and 7 cyber bullying media. Both research found cyber bullying less severe, yet appreciable, than conventional bullying, and reported more outside of school than within. The bullying of phone calls and text messages was most common, with instant messaging in the second study; their effect was viewed as comparable to conventional bullying. Cell phone / video clip bullying was seen to be more negative impact. Differences in age and gender differed between the two samples. Study one showed most cyber bullying was performed by one or a couple of students, usually from the same group of years. This mostly just lasted about a week, but at times a lot longer. The second study showed that being a cyber victim, but not a cyber bully, was associated with the use of the internet; many cyber victims were typical bully victims.

Hunter, H.A. (2009) through the study conducted on Computer Crime and Identity theft portraits that the topic at hand is the enhanced amount of bugs and security risks for people participating in e-commerce, company transactions on the

World Wide Web. In 2008, 10 million Americans were affected by identity theft and each year, businesses around the world lose over $220 billion due to identity fraud. Identity fraud is an ongoing problem that must be addressed. Credit card information is what is most often stolen in a data breach case. The project evolved from various main ideas to a well researched thesis paper. Once the decision for the topic was made for the Master Thesis paper: “Computer Security and Identity Theft” and it was approved by the Regis University advisor, the first step was to begin to do a thorough research of both primary and secondary sources. The primary references used in this master thesis include interviews with co-workers and colleagues in the IT Security field. This allowed for the gathering a more subjective or personal view of the extent of the problem. The secondary resources included periodicals such as journal article, books, and websites that shed like into the subject. These resources not only served as an aid in producing a detailed literature review, but allowed for the support the argument or problem in the document. Most consumers don't pay their bills by mailing them to the retailer with their wallet, they pay for the things they purchase online, which leave them vulnerable to hacks and social manipulation assaults. It says their business websites their credit card / debit card numbers, phone number and home address and even their date of birth information. Both of these technology flaws are highly at risk of identity fraud. Identity fraud is when personal (confidential) information about an individual, such as social security or account numbers, is stolen and used against them. The work was developed by watching a business being restructured. Many ideas were also based on its employees having had identity theft. Some of the things observed at a major local university were lack of awareness, training and instruction.

Gianluca Stringhini, Christopher Krügel, Giovanni Vigna (2010) conducted a study on Detecting spammers on social networks **.**Social networking has become a common way for people to get together online and connect. Users spend a large amount of time processing and posting a variety of personal knowledge on common social network sites (such as Facebook, MySpace, or Twitter); As well as the prospect of reaching thousands of people, this information also draws the attention of cyber criminals. Cybercriminals, for example, may manipulate the users ' tacit trust relationships to attract people to malicious websites. Cyber criminals may, as another example, consider personal information useful for identity theft or to push targeted spam campaigns. In this paper they examine the degree to which spam has become part of social networks. They built a wide and varied collection of "honey-profiles" on three major social networking sites to gather the data about spamming activity, and logged the kind of connections and messages they received. Afterwards, they analyzed the data gathered and found anomalous activity of users who approached our profiles. We developed strategies to identify spammers in social networks based on the study of this activity, and we aggregated their messages in large spam campaigns. Their findings show that the accounts used by spammers can be instantly detected, and our research has been used to take-down attempts within a real-world social network. More specifically, they partnered with Twitter during this analysis, and identified and removed 15,857 spam profiles correctly.

Welsh (2011) calls the "digital natives" or the "I Generation" generation of today. A set of studies reveals the psychological and sociological effects of constant networking. Although studies reveal some of Facebook's positive aspects such as a shy kid who gets a good experience by building online relationships, negative features such as narcissism, lack of empathy, increased aggression and mental illnesses such as schizophrenia and depression are also reported as a result of excessive use of social networking sites. Online social networking is noted to distract teenagers from research. It results in bad performance in academia. Teenagers who are technologically dependent are poor in interpersonal skills. Not only this, but they are unaware that somewhere somebody might have saved it online / offline even after removing pictures or published data. Welsh warn the digital generation to use online sites with precaution. However, he did not analyze the causes behind the lack of concern on privacy issues by adolescents.

Jaishankar (2011) refers to the fact that criminal justice still lacks appropriate and up-to-date information about the contemporary reality of cybercrime. In order to comprehend cyber crime, his ' Space Transition Theory ' is essential. In virtual space, anonymity has become more criminogenic. It has caused cyberspace's Deviance and Criminal Subculture. Victimization of social networking in particular adolescent victimization was connected with the theory of routine activity and the theory of lifestyle. Because of the liberty these techniques give, teenagers explore fresh techniques, but it also makes them susceptible to internet crime. Even though cyber bullying is discussed, it is not indicated in a psychological context and its social consequences.

Holt (2011) highlights four main kinds of cybercrime, namely cyber trespass, cyber deception / theft, cyber porn, obscenity, and cyber violence. In the light of evolving trends and patterns of crime, he has discussed multiple criminological theories. He looks at hacking and its different types. In the light of latest legal developments, he also evaluated child porn. He also assesses the law dealing with cyber bullying and cyber stalking. More research is required in his opinions to create' consciousness' among the prevalent individuals that google for anything and nearly everything.

Das and Sahoo (2011) assess social networking sites and think that it is impossible to demarcate personal and public life in the era of social networking. A person becomes helpless when he or she is posted on a website to control the distribution of personal data, image or video. Although individuals set the level of privacy, it is still shared with an unidentified web administrator. Using the Facebook profile data you can readily determine a person's physical place. Social networking sites are becoming an individual's privacy danger. As individuals are immersed in a virtual world of interactions, the writers also highlight the biological effect. Another drawback of the social networking site is that individuals who have spent a lot of time interacting with colleagues and browsing profiles transform their minds away from other main job, and it becomes a practice for them to visit their profile several times a day. The writers also point out that there has emerged a fresh form of internet addiction called ' Facebook Addiction Disorder ' where individuals become internet addicts. Cyber crimes via social networking sites include posting objectionable material on the profile of users, producing fake profiles to defame a individual, and accessing someone's profile through hacking. Sites of social networking have the ability to ruin relationships and can render life miserable.

Stephanie Chant, Majeed Khader, Jansen Ang, Eunice Tan , Katharine Khoo and Jeffery Chin (2012) conducted a study on Understanding " Happy Slapping" they discuss happy slapping and undertakes an analysis of this new crime trend. The analysis is undertaken using four angles (the 'CLIP profiling approach' employed by the Behavioural Sciences Unit, Singapore) using five case studies from different parts of the world: a criminalistics and forensic science perspective, a legal perspective, an investigative and operational perspective and a psychological perspective. Each perspective provides a richer understanding of this new phenomenon. The study hopes to promote a richer understanding of this new form of technology-enhanced crime, so as to aid future effective law enforcement efforts and extend theoretical knowledge of this form of behaviour. The study concludes with recommendations for _future research on this phenomenon. Three important questions remain for future research agenda. First, is happy slapping a transient fad or can we expect more of it in the future? How do we measure the extent of the problem? Second, how is happy slapping different from other forms of cyber bullying? Third, should and how should law enforcement respond to happy slapping? These questions will pave the way for more research on happy slapping, which we believe is an emerging trend in youth and cyber crime.

June Ahn (2012) conducted study on Teenagers' Experiences With Social Network Sites: Relationships to Bridging and Bonding Social Capital. Many studies have examined the relationship between social network sites (SNSs) and the development of social capital. However, most studies to date have only considered college and adult populations. This study examines the patterns of SNS use in an urban, teenage sample in the United States.The total student population in the four high schools was approximately 8,900. Of this population universe, 852 youths returned their consent forms and participated in the study. To examine the relationship between teenagers’ experiences with SNSs and their social capital, he conducted a survey in two urban high school districts in the United States during the autumn of 2009. A Web-based survey was developed that asked several questions. The participants were asked to indicate whether they were members of Facebook and/or Myspace. The survey also collected measures of self-esteem and social capital (outlined in detail later). To recruit participants, he visited four high schools and made presentations in classrooms and distributed flyers. The teenagers also received consent forms, which their parents were required to sign before they could participate in the study. It tests the hypothesis that use of SNSs is related to higher levels of social capital. The results show that youth who use Facebook and Myspace report higher social capital in both their school and online relationships. In addition, the analysis suggests that distinct modes of SNS experiences are differentially related to bridging and bonding social capital. Time spent in SNSs is related to bridging capital, while positive or negative experiences are related to bonding capital. The study offers new insights into how youth experience SNSs and the relationship of that experience with their connection to the world.

Hemraj Saini, Yerra Shankar Rao, Tarini Charana Panda (2012). conducted a study on Cyber-Crimes and their Impact: A Review .The study says that in the modern internet computing period, as much information as possible is internet and vulnerable to cyber attacks. There are a large range of cyber threats and their activity is difficult to understand in the early stages of cyber attacks, thus difficult to control. Cyber threats may have a motive behind them, or may be unknowingly handled. The threats that are carefully handled can be known as the cyber crime that have extreme impacts on society in the form of economic destruction, psychological disturbance, national security danger, etc. Restricting cybercrime is based on careful study of its actions and awareness of its impacts across various layers of society. Therefore, for emerging cyber crime developments, the present report offers awareness of cybercrimes and their effects on society.

Debarati Halder, K. Jaishankar(2013) through their study on Revenge Porn by Teens in the United States and India: A Socio-Legal Analysis states that there is a lacuna in dealing with adolescent sexual behaviour including revenge taking mentality with the help of sexted images. This paper argues that instead of dealing the issue of revenge porn by teens in the traditional procedural ways as has been laid down in the legal provisions or by way of rusticating the children (including the perpetrators and the victim) from the school as has happened in India in several occasions, therapeutic jurisprudence approach should be taken up.

R. Sivakumar (2013) conducted a study on computer mediated interpersonal crimes a study of cyber bullying among college students in cosmopolitan cities. A total of 600 respondents were selected for the present study from five major cosmopolitan cities (New Delhi, Mumbai, Kolkata, Chennai and Bengaluru). Stratified random sampling was used to select the colleges in the above said cities. Purposive sampling method was adopted to choose the college student samples. Primary data were collected using a structured interview schedule. As sampling techniques f' and 't' tests were carried out. it was found that with numbers of reports of cyber bullying, cyber vandalism, nuisance and finally kidnapping and murder through the internet by the youth, it has become a serious problem for the colleges, parents, law and justice machinery and the society as a whole to maintain peace and inculcate good values in the youth. cyber bullying is a much neglected problem in India. There was no specific law to prevent cyber bullying activities among students, though there are laws to prevent ragging. With the advent of internet, the bullying behaviour has spread across the school and college campuses in India. Many incidents of cyber bullying happen in India and they go unreported. They are reported only when they result in crimes like murder. It was assumed that such incidents are rare and with one such reported incident the children with Indian value will never dare to do such things in the future. However, the infamous Bombay cyber bullying case proved the social thinking wrong and proved that cyber bullying is growing in India.

Sanjeev Davey ,Anuradha Davey(2014) made an Assessment of Smartphone Addiction in Indian Adolescents: A Mixed Method Study by Systematic-review and Meta-analysis Approach. The assessment of emergence of smartphone abuse in Indian adolescents was done by a mixed method approach as per preferred reporting items for systematic-review and meta-analysis (PRISMA [2009]) guidelines for systematic-review and meta-analysis done by using Med-Calc online meta-analysis software.the investigator searched for studies in any form on two key search words: “Smartphone addiction” and “Indian Adolescents” using websites of MEDLINE, EMBASE, Psyc-INFO, Global Health, PubMed, Biomed-

Central, Web of Science, Cochrane Library, World library - World-Cat, Indian libraries such as National Medical Library of India from 1 January, 1995 to March 31, 2014 first for systematic-review. A total of 45 articles were considered in systematic-review from whole world; later on 6 studies out of these 45 related to Smartphone's addiction in India were extracted to perform meta-analysis, in which total 1304 participants (range: 165-335) were enrolled. The smartphone addiction magnitude in India ranged from 39% to 44% as per fixed effects calculated ($P <$ 0.0001). Meta-analysis finding reveals that mobile phone (smartphone) usage has a significant effect in causing psychological problems, affecting classroom performance, hampering of studies, eating, stress, etc. Most of adolescents are exposed to the media applications and instant mobile broadband access involved with the evolution of Smartphone. Increase in the use of smartphones in societies, has raised concern about social and psychological effects of excessive use of smartphone's especially among Indian adolescents. Smartphone's have made mobile connectivity so accessible that today's Indian generations are abusing their Smartphone. Smartphone abuse to addiction has become more serious since adolescents can download and run numerous applications with smartphone even without Internet connection.

Urmila Goel (2014) conducted a study on Awareness among B.Ed teacher training towards Cyber-crime .The population for the study were all B.Ed. Teacher Trainees of Sonipat district. Multi-stage sampling technique and simple random sampling technique is used for the selection of sample. A sample of 120 students is taken for the study. Cyber Crime Awareness among B.Ed. Teacher Trainees was measured by Cyber Crime Awareness Scale (CCAS-RS). It was found that boys teacher trainees has more awareness towards cyber crime than girls teacher trainees. Also science girls teacher trainees has more awareness towards cyber crime than art girls teacher trainees. The science boys teacher trainees has more awareness towards cyber crime than art boys teacher trainees. It was interpreted that rural boys and girls teacher trainees have almost equal awareness towards cyber crime. It can help the teacher to know about the level of awareness towards cyber crime in students. The study suggests that the teacher can tell the students about the harmful effects of using internet without sufficient preventing measures. The teacher can tell the students about safe internet browsing and protect themselves of being victims. It can help in decreasing the involvement of students in cyber crimes who do mistakes due to the lack of awareness towards cyber crime. The students can protect themselves from hacking, phishing, spam, identity theft etc.

Deepak Raj Rao .G (2014) cyber crime and social networking websites a study on the victims and vulnerabilities of social networking university of madras. The first hand information via questionnaire would be gathered from students, employees and general public who are accessible and please to share their details, views, opinions and thoughts. Students, employees of software companies and general public as population for this research were selected and based on non-probability sampling techniques such as purposive and convenience practices the necessary information recognized in the framing of problem, its aims and objectives and hypothesis would be gathered. In this research, Cluster sampling technique was adopted for the selection of sample as the population in this research is large. it was found that users of Social Networking Sites are not related to the family social status age and education background . There is Increase in number of Social Networking Sites users is not because of purchase of more home computers . Users with less knowledge with computer operation use Social Networking Sites equivalent with that of the computer experts. Those who don't have computer at home use Social Networking Sites more offer than the users who have computer in home Victimization in Social Networking Sites cyber crime is not due to more hours spend in Social Networking Sites. Victimization in Social Networking Sites cyber crime is due the trust of the users on the safe Social Networking Sites web application. it was suggested that the users of Social Networking Sites should not pass their personal information to others. While dealing there must be proper care taken by themselves. Hence, it is must for users to watch what they post online and stay safe.

Md Shamimul Hasan, Rashidah Abdul Rahman, Sharifah Farah Hilwani Binti Tengku Abdillah and Normah Omar(2015) conducted a study on "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia" . The study examines the relationship between perception and gender, age and knowledge as well as the relationship between awareness and gender, age and knowledge towards cybercrime. A field survey is conducted among 342 students in the faculty of accountancy of Universiti Teknologi MARA (UiTM) with a structured questionnaire that covers demographic information and seven most known cybercrimes. Percentile analysis, correlation matrix, multivariate regressions are done to test the hypotheses. In addition, Post Hoc test is conducted to locate where the significant differences lies. The study finds female students are more aware and have affirmative insights than male, students in the age group of 18-23 years have lower perception and awareness than those aged 24 years and above and those with higher academic qualifications are more aware at cybercrime and perceived the issue of risk differently. The study provides empirical evidence to the top management of the higher level institutions on the needs to improve their policies and procedures to protect young generation reducing the high risk of becoming a victim.

Teen Jose, Dr. S. Sasidhar,. Y. Vijayalakshmi Dr. P. Manimegalai (2015) conducted a study on Cyber Crimes in Kerala: A study it states that with the advancement of technology, cybercrimes increases. A study of growing cybercrimes in Kerala is made. An Illustration of the share of Kerala in the country's crime statistics is done. A special mention is made on the increasing cybercrime against women. Topic wise distribution of cybercrimes in Kerala is given and is compared to that of the country as a whole. Motives of the crimes are studied. The suspects of the crimes are being mentioned. Latest statistics of cybercrimes as reported by the National Bureau of Crime Records and State Bureau of Crime Records are mentioned. The reports published by the Hi-tech crime enquiry cell of the state government and the reports of the cyber cell, Thiruvananthapuram and Thrissur are taken for analysis. A district wise analysis of the cybercrimes in Kerala is made.

Bijoy Saima (2015) conducted a study on "Cyber Crime Awareness amongst Students of Government Law College, Trivandrum- A Legal Survey". The study aims to examine the level of ethical and security awareness among law students. A questionnaire based survey method on cyber-crime was used among students of government law college, Trivandrum in the state of Kerala. The study was completed by 89 respondents from 10 classes. The sample was obtained from random selection. The questionnaire was designed in such a manner that the respondents can complete the questionnaire in an average minimum time of 4 minutes. There is no gender differentiation in this survey. The overall findings indicates satisfactory awareness all the students, only 40 percent of the students were able to exhibit a firm theoretical knowledge of the common types of cyber-crimes enlisted under section 43 of the Information Technology Act, 2000. The findings of this study could be useful for the college management to understand the mentality of the students while setting up policies and regulations to effectively reduce the instances of cyber-crime in the student community.

Archana Chanuvai Narahari & Vrajesh Shah (2016) made a study on Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India) The study is focused on a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes. The study is based on both qualitative and quantitative research analysis. In the first stage, In-depth Interviews are conducted with two ethical hackers. Purposive sampling method was selected. For interviewing structured open ended schedule was adopted. In the second stage, a survey is conducted on 100 young internet users of Anand. The age of the respondents falls between 17 to 35 years. Simple random sampling method was adopted. The study proves that internet users in Anand are not thoroughly aware of cybercrimes and cyber security that are prevailing.

Varghese (2016) performed a survey entitled ' A sociological analysis of the consciousness of cybercrime safety among adolescents ' and found that the cyber law module is extremely efficient in developing knowledge of cybercrime among high school learners. The research disclosed that for a lengthy moment, most learners were online daily because their studies are badly impacted resulting in bad grades. It was also found that learners who regularly use social networking sites tend to have adverse health effects such as stomachs, bad sleep patterns, eye strain, anxiety and depression.

Sukanya .K.P, Raju C.V (2017) conducted a study to find the Cyber Law Awareness among youth of Malappuram District cyber law awareness was checked among youth in Malappuram district. And they were characterized with an age group of 18 to 35. Study samples were chosen from a population who uses computer and internet facilities in daily life. And questionnaire was used to collect data from samples. Stratified random sampling was used for this study. It was found that most of the youth are familiar with IT Act, 2000 in India. But some are ignorant about it. It’s necessary to make them aware of this legal system because we are living in a highly sophisticated e- world. Here chances for getting trapped are very high. So it would be better if the cyber authorities conduct law awareness programs for users of cyberspace.

Dr. Ursula M.Wilder (2017) wrote an article on The Psychology of Espionage and Leaking in the Digital Age. It says Advances in technology, the

Internet, mobile platforms, social media, and computing power are driving unparalleled defining changes in the world. Communication technologies, in particular, have altered how people relate to each other individually, in social groups, in nations, and globally, and are expanding what people mean when they use the term “reality.” The new technologies have, unsurprisingly, precipitated changes in the manifestations of spying from within the world of professional intelligence, where leaking now joins espionage as a major threat to national security. Other threats from insiders include sabotage and workplace violence. The main focus of this article was on the role of the Internet (to include social media) in espionage and leaking. The three essential factors predisposing individuals to espionage or leaking classified material dysfunctions in the personality, states of crisis, and opportunity operate symbiotically. The risk of spying can be mitigated through programs designed to spot and address warning signs at each stage of an employee’s career and by providing support services to troubled employees once they have been identified or by disciplining them appropriately.

Sreehari A, K.J Abinanth, Sujith B, Unnikuttan P.S, Mrs. Jayashree (2018) made a Study of Awareness on Cyber Crime Among College Students With Special Reference To Kochi. Using random sampling, this research was carried out in Kochi with 200 respondents. The respondents are college students who are either undergraduates or postgraduates. The data was collected using online surveys which were sent to the students.The research shows that only most users are just aware about cybercrime. It states the ratio of awareness among the respondents regarding cybercrime is high for hacking when compared to other types. it shows that the most of these respondents are not properly aware of the cybercrime laws. Most of the respondents spend more than 2 hours on the internet. Also maximum respondents stated that they have no idea about the safety of their information while being online. Many respondents do not know the proper steps in ensuring that they keep their data safe. It was also found that a minority of the respondents have lost money during online transactions. Also a large percentage of the respondents rarely change their password for accounts which is also a safety threat. It is also clear that the respondents even though they are just aware about cyber crime still download various content such as movies, games etc. which falls under cybercrime. The study also found out that most of the respondents occasionally receive spam messages and spam calls but hardly anyone of these respondents failed to report it to the cybercrime police in order it to prevent it from occurring again.

D.A Prathima Mathias and Suma B(2018) conducted a Survey on Cybercrime Awareness Among Graduate and Postgraduate Students of Government Institutions In Chickmagaluru, Karnataka, India and a Subsequent Effort to Educate them through a Seminar. Survey conducted among Students of this college (both UG and PG) aged between 18-21 years were considered for the present study. Probability sampling method based on simple random sampling was adopted, taking care that 50% of them were from UG and 50% from PG. Total population of the college was 2,500 hence 250 questionnaires were distributed .Personal Information Schedule (PIS) Survey questions were framed by the authors based on various cyber security issues like virus, phishing and other attacks in the internet. It was found that majority of students are gadget literates. The major use of internet by students is for social networking. The study shows that majority of students are completely unaware of cybercrime and cyber security. study suggests that schools and colleges have to educate both students and parents on safe surfing, using workshops and seminars as medium of instruction. School children learn computer basics in their curriculum, similarly awareness of cybercrime should be a part of regular course work.

Afrozulla Khan Z Vaishnavi Rajesh Thakur and Arjun (2018) investigated Cyber Crime Awareness among MSW students ,School Of Social Work, Mangaluru. The study was conducted among 100 MSW students. The sample was selected through 'Simple Random Sampling Method'. Age of the respondents was distributed from 20-35 years. Data collected from the students using questionnaire. Respondents were asked about term cybercrime, 68% respondents stated that they are somewhat familiar with the term cyber-crime, 22% of the respondents are very familiar with the term cyber-crime, and 10% of the respondents are not familiar with the term cyber-crime.it was found that there is a significant difference between the awareness level of different age group. Results revealed the importance of awareness as a tool to decrease/ prevent cyber-crime. The overall findings indicate unsatisfactory awareness on cyber-crime among MSW students. Therefore, it is concluded that the hypothesis has not been proved to be coherent, i.e., MSW students are not aware of cyber-crimes.

Taylor Kohut, Aleksandar Stulhofer (2018) made a study titled as 'Is pornography use a risk for adolescent well-being? An examination of temporal relationships in two independent panel samples'. They examined the relationship between pornography use, subjective well-being, symptoms of depressions and anxiety, and self-esteem in two independent panel samples (*N* = 455; *N* = 858) of Croatian adolescents using cross-lagged path analysis and lagged linear mixed models. The data for this study were collected in two panel samples of Croatian adolescents from Zagreb and Rijeka that were recruited as a part of the PROBIOPS (Prospective Biopsychosocial Study of the Effects of Sexually Explicit Material on Young People's Sexual Socialization and Health) project. The samples included high-school sophomores (M_{Zagreb} = 16.1 years, SD = 0.46, range = 15–19 and M_{Rijeka} = 15.9 years, SD = 0.52, range = 15–18) who were then re-surveyed at 6-month intervals (baseline surveys were conducted in April of 2015 in Zagreb and December the same year in Rijeka). In Zagreb, students were recruited from 59 of 90 schools in the capitol city and the surrounding county. In Rijeka, the panel included students from 14 larger secondary schools, which accounted for 63% of the city's 2nd year high-school student population. They did not find consistent evidence that pornography use was associated with negative changes in subjective well-being, symptoms of depression and anxiety, or self-esteem in either gender. Such findings are at odds with some interpretations of the available evidence from cross-sectional research Despite common public concerns that surround adolescent use of sexual media , the results of this first longitudinal assessment of the relationship between pornography use and adolescents' subjective well-being provide no evidence that pornography use contributes to decreased subjective well-being in adolescent men. They found, limited evidence of the contradictory contribution of pornography use to female adolescents' dysregulated mood and self-evaluation.

Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner (2019) made a study on Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. This research determined the effect of Internet user age and email content such as weapons of influence (persuasive techniques that attackers can use to lure individuals to fall for an attack) and life domains (a specific topic or aspect of an individual’s life that attackers can focus an emails on) on spear-phishing (targeted phishing) susceptibility. One-hundred young and 58 older users received, without their knowledge, daily simulated phishing emails over 21 days. A browser plug in recorded their clicking on links in the emails as an indicator of their susceptibility. Forty-three percent of users fell for the simulated phishing emails, with older women showing the highest susceptibility. While susceptibility in young users declined across the study, susceptibility in older users remained stable. The relative effectiveness of the attacks differed by weapons of influence and life domains with age-group variability. For inclusion in the data analysis, participants needed to complete 21 days of study intervention and have at least 50% recorded daily email checking activities .These criteria excluded 33.1% (n = 78) of the total 236 volunteers originally enrolled. Excluded individuals were equally distributed across age group and gender. In addition, older compared to young users reported lower susceptibility awareness. Accommodating for the hierarchical structure of the data (i.e., email clicks nested within participants), they conducted three multilevel logistic regression models to address our research questions. The first multilevel logistic regression model tested the extent to which susceptibility differed between young and older users (*Q1a-b*). The second multilevel logistic regression model tested the extent to which susceptibility varied as a function of the weapons of influence in young and older users (*Q2a-b*). The third multilevel logistic regression model tested the extent to which susceptibility varied as a function of life domains in young and older users (*Q3a-b*). The findings support effects of Internet user demographics and email content on susceptibility to phishing and emphasize the need for personalization of the next generation of security solutions. Overall, susceptibility to phishing was high, with 43.3% of users clicking on at least one of the 21 simulated phishing email links and 11.9% of users clicking on more than one link during the 21 -day study period.

Conclusion

The review of these studies helped the investigator to acquaint with the current knowledge in the area of the present study. These studies enlighten the investigator to proceed along the right path. The investigator reviewed the studies related to technology mediated interpersonal crimes. Most of the studies conducted internationally where as few studies are from India. The studies were confined to technology mediated interpersonal crimes such as cyber bullying cyber stalking, Identity theft, Child Pornography, Happy slapping, Phishing, Espionage, Spamming. A study on computer mediated interpersonal crimes a study of cyber bullying among college students in cosmopolitan cities (New Delhi, Mumbai, Kolkata, Chennai and Bengaluru) included in the review. Also the studies like awareness on cyber crime conducted in kochi, Malaysia, Karnataka, Trivandrum, Gujarath, Mangaluru, were included in the study these studies confined to college students.

From all these studies investigator found that no studies have been conducted among higher secondary school students about the awareness on technology mediated interpersonal crimes using technological gadgets. So the investigator conducted the study among higher secondary school students in Calicut district. It was Entitled as “Technology Mediated Interpersonal Crimes among Higher Secondary School Students”

CHAPTER III

METHODOLOGY

- Variable of the Study
- Objectives of the Study
- Hypotheses of the Study
- Sample of the Study
- Tool used for Data Collection
- Data Collection Procedure
- Scoring and Consolidation of Data
- Statistical Techniques used for the Analysis

METHODOLOGY

Research is considered to be a more formal, systematic, extensive process of carrying on the scientific method of analysis (Best, 1997). Research method is of great importance in a research process. The success of any research is depending largely on the suitability of method and the tools and techniques used for the data collection of data. The decision about the methods depends upon the nature of the research problem and the kind of data necessary for its solution. A suitable method helps the researcher to explore the diverse area of the study.

The present study is entitled as "TECHNOLOGY MEDIATED INTERPERSONAL CRIMES AMONG HIGHER SECONDARY SCHOOL STUDENTS". The study is an attempt to find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students. The methodology of the present study is explained under the following sections.

Variable of the Study

Objectives of the Study

Hypotheses of the Study

Tools Used for Data Collection

Sample of the Study

Data Collection Procedure

Scoring and Consolidation of Data

Statistical Techniques used for Data Analysis

Variable of the study

The present investigation has the only variable named as Technology Mediated Interpersonal Crimes.

Objectives of the Study

1. To find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students for the total sample and the relevant subsamples based on gender, locale of the students and type of management of schools.

2. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

3. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

4. To find out whether there exist any significant difference in the awareness on technology mediated interpersonal crimes for the subsample based on type of management of schools.

Hypotheses of the study

1. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

2. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

3. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes for the sub sample based on type of management of schools.

Sample of the Study

The population concerned for the study is the higher secondary school students of Kerala, which is a huge and infinite one. The investigator therefore conducted the study using a sample of 600 students of standard XI drawn from various schools of Kozhikode district, selected through stratified random sampling technique. Due representation was given to different strata like gender, locale and type of management of schools.

- Gender of the Student (Male and Female)
- Locality of the Student(Urban and Rural)
- Type of the Management (Government, Aided and Unaided)

The details of intended sample are given in the Table 1.

Table 1

Breakup of the Final Sample

Sample	Categories	No of Student	Total
Gender	Male	272	600
	Female	328	
Locale of Students	Rural	193	600
	Urban	407	
Type of management	Government	280	600
	Aided	243	
	Unaided	77	

List of schools selected for the study was given as Appendix 3.

Tool used for the study

Data collection is one of the major parts of research process. For an effective data collection an effective tool has to be selected and the necessary step in the preparation of tool has to be adopted. For the present study the following tool was constructed by the investigator with the help of supervising teacher.

Awareness test on technology mediated interpersonal crimes

Awareness test on technology mediated interpersonal crimes was constructed by the investigator with the help of supervising teacher. The questions were made out of considering the description of each crime done by using technological gadgets. The development of the tool was as follows.

Planning and Preparation of the Test

In the present study the investigator used an Awareness test on technology mediated interpersonal crimes prepared by the investigator with the help of supervising teacher in order to measure the awareness level of technology mediated interpersonal crimes among higher secondary school students.

It consists of 53 items of various technology mediated crimes. While preparing the awareness test on technology mediated interpersonal crimes the investigator with the help of supervising teacher selected the categories of technology mediated interpersonal crimes. The technology mediated interpersonal crimes such as Cyber bullying, Cyber Defamation, software piracy, Hacking & Cracking, Child Pornography, Spoofing, Credit Card Fraud, Internet Relay Chat Crime, Cyber Theft, Cyber Squatting, E-mail Spamming, Denial of Service attacks, Forgery, Investment Frauds, Data Diddling, Espionage, Sniffing Attack, Cyber Stalking, Salami Slicing Attack, Happy Slapping, Phishing, Cyber Terrorism were included in the test. The details of the technology mediated interpersonal crimes with one example are described below.

Cyber bullying

Cyber bullying is a form of bullying that takes place via internet connected devices like smart phones, computers, or tablets.

Example:

The act of harassing other person using technological gadgets known as

A) Hacking

B) Cyber Theft

C) Cyber bullying

D) Email Stalking

Cyber Defamation

Cyber Defamation is the intentional infringement of another person’s right to his good name and tarnishing the image, respect or dignity of any person in front of right thinking members of the society through the electronic gadgets.

Example:

The process of tarnishing the image, respect or dignity of any person in front of right thinking members of the society through the electronic gadgets

A) Bullying

B) Stalking

C) Cyber Defamation

D) Data Diddling

Software Piracy

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software. Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work.

Example:

Copying a copy righted software without the permission of the owner?

A) Cyber Defamation

B) Software Piracy

C) Logic Bomb

D) Data Digging

Hacking and cracking

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use readymade computer programs to attack the target computer. Crackers may steal or modify data or insert viruses or worms which damage the system.

Example:

Which among the following classification considered as type of hacking?

A) Grey Hat ,Black Hat, Blue Hat, Elite Hacker

B) Grey Hat ,Red Hat, Blue Hat, Worm

C) Yellow Hat ,Grey Hat, Green Hat, Red Hat

D) Skiddle, Newbie, Green Hat, Red Hat

Child Pornography

Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Example:

Act of sending sexually explicit images by cell phone/by emails

A) Child Pornography

B) Vishing

C) Online Sextortion

D) Sexting

Spoofing

Spoofing means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained actual password. He creates a new identity by fooling the computer into thinking he is the genuine system operator. The hacker then takes control of the system. He can commit innumerable number of frauds using this false identity.

Example:

A protocol that resolves IP address for transmitting data called as?

A) Domain Spoofing

B) Address Resolution Protocol Spoofing

C) Website Spoofing

D) Spoofing Internet Protocol Spoofing

Credit Card Fraud

Credit Card Fraud is the act of misusing the credit card credentials of another person or the act of impersonating the credit card owner;

Example:

The act of misusing the credit card credentials of another person or the act of impersonating the credit card owner?

A) Forgery

B) Credit card jacking

C) Cyber Defamation

D) Credit Card Fraud

Internet Relay Chat Crime

Internet Relay Chat (IRC) is a protocol for real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message as well as chat and data transfer, including file sharing.

Example:

The synchronous conferencing used by hackers to share the techniques of hacking known as

A) Internet Relay Chat

B) Internet Conference Chat

C) Internet Instant Chat

D) Internet Group Chat

Cyber squatting

The term cyber squatting refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names. Cyber squatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner.

Example:

Cyber squatting refers

A) Information accessed without authorization

B) Act of copying and using others information without their knowledge

C) Stealing personal information such as customer ID or pin

D) Registering a domain name with the intent of profiting from the goodwill

E-mail Spamming

E-mail "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter is called email spamming.

Example:

The unsolicitated commercial email send to a large number of addresses is known as –

A) Email Spamming

B) Spoofing

C) Phishing

D) Software Piracy

Denial of Service Attack

Flooding a computer resource with more requests than it can handle. This causes the resource to crash there by denying access of service to authorized users.

Example:

Overloading a system with so many requests is known as

A) Tracking

B) Espionage

C) Denial of Service Attack

D) Fraud

Forgery

Forgery involves a false document, signature, or other imitation of an object of value used with the intent to deceive another. Those who commit forgery are often charged with the crime of fraud.

Example:

The fraud act committed by using a false document, signature, or other imitation of an object of value used with the intent to deceive another known as-

A) Cyber Defamation

B) Logic Bomb

C) Data Diddling

D) Forgery

Investment Frauds

The fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site or the non-delivery of products purchased through an Internet auction site.

Example:

The fraud leads to the misrepresentation of a product advertised for sale through an internet ?

A) Investment Fraud

B) Accounting Fraud

C) Bank Fraud

D) Lottery Fraud

Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing. in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.

Example:

The action of skewing data entire in the users system is –

A) Online Scams

B) Identity Theft

C) Data Diddling

D) Salami Attack

Espionage

Espionage or spying is the act of obtaining secret or confidential information or divulging the same without the permission of the holder of the information.

Example:

Practice of obtaining data and information without the permission and knowledge of the owner?

A) Cyber Squatting

B) Espionage

C) Website Defacement

D) Pharming

Sniffing Attack

Sniffing attack or a sniffer attack, in context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets)

Example:

The procedure used by hackers to capture all the network packets is known as

A) Trojan Attack

B) Scam

C) Sniffing Attack

D) Spoofing

Cyber Stalking

Stalking refers to repeated unwanted intrusive behaviours that result in the victim experiencing fear, physical or psychological harm or emotional distress .Cyber Stalking refers to trailing activities conducted in ‘cyber space’ using information and communication technologies.

Example:

Cyber Stalking involves

A) Sending threatening emails or sending viruses and spam

B) Hacking into a victims computer and taking control of it

C) Connecting a device to a phone line to listen to Conversation

D) Spreading rumors or tracking victims on the Web

Salami Slicing Attack

A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size.

Example:

Stealing tiny amounts of money from each transaction

A) Salami Slicing Attack

B) Key logger

C) Espionage

D) Fraud

Happy Slapping.

The practice whereby a group of people assault a stranger at random, filming the incident on a mobile device and to circulate the images or post them online.

Example:

Happy slapping means that

A) Unauthorized filming of an incident in a device

B) Stealing of personal data

C) Make a direct contact through phone calls, emails, or even in person

D) Order to attack computers by sending spams or malware.

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Example:

Phishing involves

A) Malicious attempt to interrupt regular traffic of a targeted server

B) Web hacking techniques used to destroy database

C) Deceiving individuals to gain private or personal information

D) Attempt to destroy data saved in computer

Cyber Terrorism

The concept of cyber terrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks.

Example:

The term cyber terrorism was coined by

A) Ardit Ferizi

B) Winn Schwastaw

C) John Arquilla

D) Barry Collin

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

Example:

Deliberate use of the identity of others without their permission for a financial advantage is

A) Phishing

B) Spamming

C) Identity Theft

D) Defamation

Logic Bomb

Logical bombs are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.

Example:

These programs are created to do something ,only when a certain event occurs ?

A) Information Theft

B) Espionage

C) Logic Bomb

D) Software Piracy

Scoring procedure

The awareness test on technology mediated interpersonal crimes consisted of 53 multiple choice items with four alternatives. One right answer is given for each item. One score was given to right option. The scores on all the items are added to get the total score on technology mediated interpersonal crimes awareness.

Validity

An index of validity shows the degree to which a test measures what it intends to measure when compared with accepted criterion. Validity as the quality of a data gathering instrument or procedure that ensures to measure what is supposed to measure (Best & Khan, 2012).

The validity of the present awareness test was ensured using content validity. A test is said to have content validity if it measures knowledge of the content domain of which it was designed to measure knowledge. Another way of saying this is that content validity concerns, primarily, the adequacy with which the test items adequately and representatively sample the content area to be measured. The items in the present awareness test were phrased in the least ambiguous way and the meaning of all the terms were clearly defined, so that the subjects responded to the items without difficulty and misunderstanding .Hence the test possesses content validity.

Reliability

Reliability is the degree of consistency that the instrument or procedure demonstrate. Reliability refers to the consistency of evaluation results. If we obtained quite similar scores, when the same test is administered to the same group on two different occasions, we can conclude that the results have a high degree of reliability.

According to Best (1996), “reliability is the degree of consistency that the instrument or procedure demonstrates, whatever it is measuring it does so consistently.

To find out the reliability of the study, the investigator used the test-retest method.

Higher the correlation more will be the reliability. Here reliability is established by testing whether two results of both of the tests reveal stability and equivalence in pupil performance. This is considered as the evidence of consistency. For determining the test – retest reliability the investigator selected 50 students who participated in the final tests. The reliability of the test on the awareness test on technology mediated interpersonal crimes was found to be 0.99 which indicates that reliability of the test is very high.

Data Collection Procedure

After deciding the sample for the present study, the investigator contacted the Principals of selected schools and requested permission through a permission letter to administer the test and to collect data. The investigator personally administered the teat in all selected schools. The investigator addressed the students at their respective class and explains the nature and confidentiality of the study. The awareness test on technology mediated interpersonal crimes was administered as per the instructions given and separate answer sheets were provided for the students. They were given enough time to complete the test. After completing the test both the test and answer sheets were collected back from the students. Uniform procedures were adopted in administering the tests in different schools.

Scoring and Consolidation of Data

The answer sheets were scored as per the scoring key prepared by the investigator. The scores obtained on the test were then consolidated and tabulated for further analysis. After rejecting the incomplete answer sheets, the investigator had 600 answer sheets for scoring.

Statistical Techniques used for the analysis

For the present study the investigator used the following statistical techniques to analyse the collected data

Preliminary analysis

Preliminary Analysis was done in order to arrive at conclusion about the nature of distribution. The important statistical constants such as Mean, Median, Mode, Standard Deviation, Skewness and Kurtosis of the variable were computed for the total sample and the relevant sub samples based on gender, locale , type of management of schools.

Test of Significance of difference between mean scores (t-test)

Test of significance of difference between two mean is known as t test. It involves the computation of the ratio between observed difference between means which is used to find out whether there exists any significant difference in the awareness level of technology mediated interpersonal crimes between relevant sub sample

$$\frac{\bar{x}^2 - \bar{x}^2}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}}$$

Where,

$\bar{x}_1$ = Mean of the upper group

$\bar{x}_2$ = Mean of the upper group

σ_1 = standard deviation of the upper group

σ_2 = standard deviation of the lower group

N_1 = Sample size of the upper group

N_2 = Sample size of the lower group

Significance of critical ratio

If the obtained critical ratio is greater than the required table value at 0.05/0.01 levels of significance, the mean difference is considered to be significant.

CHAPTER IV

ANALYSIS AND INTERPRETATION

- **Objectives of the study**
- **Hypotheses of the study**
- **Preliminary Analysis**
- **Major Analysis**

ANALYSIS AND INTERPRETATION

This chapter deals with the details of statistical analysis of the data by the means of standardized tools and its interpretations. Analysis can be defined as the thorough study of collected data, which is converted to tabulated forms, so as to determine the actual facts, which are inherent. The data collected have analyzed statistically with reference to the objectives of the study.

The main purpose of the study is to find out the awareness on technology mediated interpersonal crimes among higher secondary school students. The data was collected and analyzed as per the procedure described in the previous chapter. The data collected from the sample was analyzed to accomplish the objectives of the study**.**

Objectives of the Study

1. To find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students for the total sample and the relevant subsamples based on gender, locale of the students and type of management of schools.

2. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

3. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

4. To find out whether there exist any significant difference in the awareness on technology mediated interpersonal crimes for the subsample based on type of management of schools.

Hypotheses of the Study

1. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

2. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

3. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes for the sub sample based on type of management of schools.

Extent of Awareness on Technology Mediated Interpersonal Crimes Among Higher Secondary School Students.

As the first step of analysis, the important statistical constants such as Mean, Median, Standard Deviation and t value worked out for the variable technology mediated interpersonal crimes for the total sample and sub samples. The preliminary analysis was done to find out whether the total sample was normally distributed or not with criterion variable. For this the important statistical constants such as mean, median, mode, SD, Skewness and kurtosis were calculated for the total samples.

Summary of the preliminary analysis for the total sample is presented in Table 2.

Table 2

Descriptive Statistics of the Awareness on Technology Mediated Interpersonal Crimes among Higher Secondary School Students for the Total Sample.

Sample	N	Mean	Median	Mode	SD	Skewness	Kurtosis
Total	600	13.36	13	12	3.76	0.94	3.2

Table 2 shows that the mean, median and mode obtained for the distribution of awareness on technology mediated interpersonal crimes among higher secondary school students are 13.36, 13 and 12. It reveals that the value of mean, median and mode coincide approximately for the total sample. The standard deviation obtained is 3.76. The value of skewness is 0.94, it indicates that the distribution is positively skewed. The value of kurtosis is 3.2, it indicates that the distribution is leptokurtic. Thus it is seen that the distribution of awareness on technology mediated interpersonal crimes among higher secondary school students for the total sample are approximately normal for the distribution.

Discussion

Since the obtained mean is 13.36 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes among higher secondary school students is low.

Extent of Awareness on Technology Mediated Interpersonal Crimes Among Higher Secondary School Students Based on Gender.

The results of descriptive statistics for the distribution of scores for the awareness on technology mediated interpersonal crimes among higher secondary school students in the relevant subsample based on gender are presented in Table 3.

Table 3

Descriptive Statistics of Awareness on Technology Mediated Interpersonal Crimes among Higher Secondary School Students based on Gender

Gender	N	Mean	Median	Mode	SD	Skewness	Kurtosis
Male	272	13.19	13	12	3.92	1.47	5.07
Female	328	13.50	13	15	3.61	0.40	1.28

Table 3 shows that the mean, median and mode obtained for the distribution of awareness on technology mediated interpersonal crimes among male students are 13.19, 13 and 12. It indicates that the value of mean, median and mode coincide approximately for the total male. The standard deviation obtained is 3.92. It also shows that the mean, median and mode obtained for the female students are 13.50, 13 and 15. The value of mean, median and mode coincide approximately for the total female. The standard deviation is 3.61.The value of skewness obtained for male and female students are 1.47 and 0.40 this value indicates the distribution is positively skewed. The value of kurtosis obtained for male and female is 5.07 and 1.28, it reveals that the distribution is leptokurtic for male and platykurtic for female.

Discussion

Since the obtained mean 13.19 and 13.50 for male and female students are lesser than 26.5 (the middle score of the test) which is considerable. Hence the awareness on technology mediated interpersonal crimes among male and female higher secondary school students are low. Also the obtained mean for both male and female are remarkably lower than maximum score on the scale 53.

Extent of Awareness of Technology Mediated Interpersonal Crimes among Higher Secondary School Students Based on Locality

The results of descriptive statistics for the distribution of scores for the awareness on technology mediated interpersonal crimes among higher secondary school students in the relevant subsample based on locality are presented in Table 4.

Table 4

Descriptive statistics of awareness on technology mediated interpersonal crimes among higher secondary school students based on locality

Locality	N	Mean	Median	Mode	SD	Skewness	Kurtosis
Urban	407	13.15	13	12	3.56	0.7	2.28
Rural	193	13.78	13	14	4.11	1.21	3.88

Table 4 shows that the mean, median and mode obtained for the distribution of awareness on technology mediated interpersonal crimes among students from urban are 13.15, 13 and 12. Here the value of mean, median and mode coincide approximately for the students from urban. The standard deviation obtained is 3.56. It also indicates that the mean, median and mode obtained for students from rural are 13.78, 13 and 14. It is clear from the values that the mean, median and mode obtained coincide approximately for the students from rural. The standard deviation obtained is 4.11.The value of skewness obtained for urban and rural students are 0.7 and 1.21 this value indicates that the distribution is positively skewed. The value of kurtosis for urban and rural is 2.28 and 3.88, it indicates that the distribution is platykurtic for the students from urban and leptokurtic for the students from rural.

Discussion

Since the obtained mean 13.15 and 13.78 for the students from urban and rural are lesser than 26.5 (the middle score of the test) which is considerable. Hence the awareness on technology mediated interpersonal crimes among urban and rural higher secondary school students is low. Also the obtained mean for both urban and rural are remarkably lower than maximum score on the scale 53.

Extent of Awareness of Technology Mediated Interpersonal Crimes among Higher Secondary School Students based on Type of Management

The results of descriptive statistics for the distribution of scores for the awareness on technology mediated interpersonal crimes among higher secondary school students in the relevant subsample based on type of management are presented in Table 5.

Table 5

Descriptive Statistics of Awareness on Technology Mediated Interpersonal Crimes among Higher Secondary School Students based on Type of Management

Type of Management	N	Mean	Median	Mode	SD	Skewness	Kurtosis
Government	280	13.15	13	11	3.42	0.18	1.02
Aided	243	12.84	13	12	3.13	0.21	0.34
Unaided	77	15.72	14	12	5.49	1.18	1.35

Table 5 shows that the mean, median and mode obtained for the distribution of awareness on technology mediated interpersonal crimes among government school students are 13.15, 13 and 11. The standard deviation obtained is 3.42. The value of mean, median and mode coincide approximately for the government school students. It also shows that the mean, median and mode obtained for aided school students are 12.84, 13 and 12. The value of mean, median and mode coincide approximately for the aided school students. The standard deviation obtained is 3.13. It also shows that the mean, median and mode obtained for unaided school students are 15.72, 14 and 12. This values reveals that the mean, median and mode coincide approximately for the unaided school students. The standard deviation is 5.49. The value of skewness obtained for government, aided and unaided school students are 0.18, 0.21 and 1.18 this value indicates that the distribution is positively skewed.

The value of kurtosis obtained for government, aided and unaided school students are 1.02, 0.34, and 1.35 indicates that the distribution is platykurtic for government, aided and unaided school students.

Discussion

Since the obtained mean for government ,aided and unaided higher secondary school students are 13.15, 12.84 and 15.72 which is lesser than 26.5 (the middle score of the test) which is considerable. Hence the awareness on technology mediated interpersonal crimes for government, aided and unaided higher secondary school students are low. Also the obtained mean is remarkably lower than maximum score on the test 53.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Male and Female Higher Secondary School Students.

The investigator tested the significance of difference between the mean scores of male and female higher secondary school students in their awareness on technology mediated interpersonal crimes using the “t” test. The data and results of the test of significance difference between mean scores of awareness are presented in the Table 6.

Table 6

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Male and Female Higher Secondary School Students

Gender	N	Mean	S.D	t value	Level of significance
Male	272	13.19	3.92	1.00	NS
Female	328	13.50	3.61		

Table 6 indicates that the mean scores obtained for awareness on technology mediated interpersonal crimes between male and female are 13.19 and 13.50 .The standard deviation obtained for male and female students are 3.92 and 3.61. The t-value obtained is 1.00, which is less than the tabled value at 0.05 level (1.96). Since the t-value obtained is less than the tabled value, it can be concluded that there exists no significant difference in the mean scores.

Discussion

The mean scores of awareness on technology mediated interpersonal crimes between male and female student were found. It is clear that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes among male and female higher secondary school students. So it can be concluded that the male and female higher secondary school students have the same level of awareness on technology mediated interpersonal crimes.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Urban and Rural Higher Secondary School Students.

The investigator tested the significance of difference between the mean scores of urban and rural higher secondary school students in their awareness on technology mediated interpersonal crimes using the “t” test. The data and results of the test of significance difference between mean scores of awareness are presented in the Table 7.

Table 7

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Urban and Rural Higher Secondary School Students

Locality	N	Mean	S.D	t value	Level of significance
Urban	407	13.15	3.56	1.92	NS
Rural	193	13.78	4.11		

Table 7 indicates that the mean score of awareness of students from urban area is 13.15 and the mean score on awareness of students from rural area is 13.78. The standard deviation obtained of awareness of students from urban area is 3.56 and rural area is 4.11. The t-value obtained is 1.92, which is less than the tabled value at 0.05 level (1.96). Since the t-value obtained is less than the tabled value, it can be concluded that there exists no significant difference in the mean scores.

Discussion

The mean scores of awareness on technology mediated interpersonal crimes between urban and rural students were found. It is clear that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes among urban and rural higher secondary school students. So it can be concluded that the urban and rural higher secondary school students have the same level of awareness on technology mediated interpersonal crimes.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes based on Type of Management

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes in the Relevant Subsamples based on Type of Management of Schools are described through the following heads.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Government and Aided Higher Secondary School Students

The investigator tested the significance of difference between the mean scores of government and aided higher secondary school students in their awareness on technology mediated interpersonal crimes using the “t” test. The data and results of the test of significance difference between mean scores of awareness are presented in the Table 8.

Table 8

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Government and Aided Higher Secondary School Students

Type of Management	N	Mean	S.D	t value	Level of significance
Government	280	13.15	3.42	1.05	NS
Aided	243	12.84	3.13		

Table 8 shows that the mean score obtained for awareness of students from government school is 13.15 and the mean score for awareness of students from aided school is 12.84. The standard deviation obtained for awareness of students from government school is 3.42 and aided school is 3.13. The t-value obtained is 1.05, which is less than the tabled value at 0.05 level 1.96. Since the t-value obtained is less than the tabled value, it can be concluded that there exists no significant difference in the mean scores.

Discussion

The mean scores of awareness on technology mediated interpersonal crimes between government and aided higher secondary school students were found. It is clear that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes among government and aided higher secondary school students. So it can be concluded that the government and aided higher secondary school students have the same level of awareness on technology mediated interpersonal crimes.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Government and Unaided Higher Secondary School Students

The investigator tested the significance of difference between the mean scores of government and unaided higher secondary school students in their awareness on technology mediated interpersonal crimes using the "t" test. The data and results of the test of significance difference between mean scores of awareness are presented in the Table 9

Table 9

Comparison of the Mean Scores of Awareness on Technology mediated Interpersonal Crimes between Government and Unaided Higher Secondary School Students

Type of Management	N	Mean	S.D	t value	Level of significance
Government	280	13.15	3.42	5.04	0.05
Unaided	77	15.72	5.49		

Table 9 shows that the mean score obtained for awareness of students from government school is 13.15 and the mean score for awareness of students from unaided school is 15.72. The standard deviation obtained for awareness of students from government school is 3.42 and unaided school is 5.49.The t-value obtained is 5.04, which is greater than the tabled value at 0.05 level (1.96). Since the t-value obtained is greater than the tabled value, it can be concluded that there exists significant difference in the mean scores.

Discussion

The mean scores of awareness on technology mediated interpersonal crimes between government and unaided higher secondary school students were found. It is clear that there is significant difference in the mean scores of awareness on technology mediated interpersonal crimes among government and unaided higher secondary school students. So it can be concluded that the government and unaided higher secondary school students have the different level of awareness on technology mediated interpersonal crimes.

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Aided and Unaided Higher Secondary School Students

The investigator tested the significance of difference between the mean scores of aided and unaided higher secondary school students in their awareness on technology mediated interpersonal crimes using the 't' test. The data and results of the test of significance difference between mean scores of awareness are presented in the Table 10.

Table 10

Comparison of the Mean Scores of Awareness on Technology Mediated Interpersonal Crimes between Aided and Unaided Higher Secondary School Students

Type of Management	N	Mean	S.D	t value	Level of significance
Aided	243	12.84	3.13	5.74	0.05
Unaided	77	15.72	5.49		

Table 10 indicates that the mean score obtained for awareness of students from aided school is 12.84 and the mean score for awareness of students from unaided school is 15.72. The standard deviation obtained for awareness of students from aided school is 3.13 and unaided school is 5.49. The t-value obtained is 5.74, which is greater than the tabled value at 0.05 level (1.96). Since the t-value obtained is greater than the tabled value, it can be concluded that there exists significant difference in the mean scores.

Discussion

The mean scores of awareness on technology mediated interpersonal crimes between aided and unaided higher secondary school students were found. It is clear that there is significant difference in the mean scores of awareness on technology mediated interpersonal crimes among aided and unaided higher secondary school students. So it can be concluded that the aided and unaided higher secondary school students have the different level of awareness on technology mediated interpersonal crimes.

CHAPTER V

SUMMARY, FINDINGS, CONCLUSIONS AND SUGGESTIONS

- Study in Retrospect
- Restatement of the Problem
- Variable of the study
- Objectives of the study
- Hypotheses of the study
- Methodology
- Major findings of the Study
- Conclusions
- Tenability of Hypotheses
- Educational Implications
- Suggestions for Further Research

SUMMARY, FINDINGS, CONCLUSIONS AND SUGGESTIONS

This chapter provides an overview of the significant aspects of the various stages of the study, the major findings of the study and their educational implications, and suggestions for further research. The chapter is organized under the following headings:

Study in Retrospect

Restatement of the Problem

Variable of the study

Objectives of the study

Hypotheses of the study

Methodology

Major findings of the Study

Conclusions

Tenability of Hypotheses

Educational Implications

Suggestions for Further Research

Study in Retrospect

This section tries to make a retrospective study of different stages of the present study such as the title, variables of the study, objectives of the study, hypotheses and methodology used for the study.

Restatement of the Problem

The problem of the present investigation is entitled as Technology Mediated Interpersonal Crimes among Higher Secondary School Students

Variable of the Study

Technology Mediated Interpersonal Crimes is the variable for the present study.

Objectives of the Study

1. To find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students for the total sample and the relevant subsamples based on gender, locale of the students and type of management of schools.

2. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

3. To find out whether there exists any significant difference in the awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

4. To find out whether there exist any significant difference in the awareness on technology mediated interpersonal crimes for the subsample based on type of management of schools.

Hypotheses of the Study

1. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

2. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

3. There exists a significant difference in the level of awareness on technology mediated interpersonal crimes for the sub sample based on type of management of schools.

Methodology

The purpose of the present study is to find out the extent of awareness on technology mediated interpersonal crimes among higher secondary school students. Survey method was used by the investigator in order to collect necessary information.

Sample of the Study

The population concerned for the study is the higher secondary school students of Kerala, which is a huge and infinite one. The investigator therefore conducted the study using a sample of 600 students of standards XI drawn from the various schools of Kozhikode district, selected through stratified random sampling technique. Due representation was given to different strata like gender, locale and type of management of schools.

Tool Used for Data Collection

For such a type of research the investigator needs a certain method and instrument to gather information. The selection of suitable techniques and tools is of vital importance in a successful research.

In the present study the investigator used an Awareness test on technology mediated interpersonal crimes prepared by the investigator with the help of supervising teacher in order to measure the awareness level of technology mediated interpersonal crimes among higher secondary school students.

Statistical Techniques Used for Analysis

Apart from the preliminary statistical analysis including the mean and standard deviation the investigator used test of significance of difference between means.

Major Findings of the study

1. The obtained mean value is 13.36 which is lower than the middle score of the test which is 26.5. Hence, the extent of awareness on technology mediated interpersonal crimes in higher secondary school students is low.

2. The obtained mean is 13.19 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in male higher secondary school students is low.

3. The obtained mean is 13.50 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in female higher secondary school students is low.

4. The obtained mean is 13.15 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in urban higher secondary school students is low.

5. The obtained mean is 13.00 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in rural higher secondary school students is low.

6. The obtained mean is 13.15 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in government higher secondary school students is low.

7. The obtained mean is 12.84 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in aided higher secondary school students is low.

8. The obtained mean is 15.72 which is lesser than 26.5 (the middle score of the test) which is considerable and hence the awareness on technology mediated interpersonal crimes in unaided higher secondary school students is low.

9. The t-value obtained for the awareness on technology mediated interpersonal crimes between male and female higher secondary school students is found to be 1.00, which is less than the tabled value at 0.05 level (1.96). Since the t-value obtained is less than the tabled value, it reveals that there exists no

significant difference in the mean scores of awareness on technology mediated interpersonal crimes between male and female higher secondary school students.

10. The t-value obtained for the awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students is found to be 1.92 , which is less than the tabled value at 0.05 level (1.96). Since the t-value obtained is less than the tabled value, it reveals that there exists no significant difference in the mean scores of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students.

11. The t-value obtained for the awareness on technology mediated interpersonal crimes between government and aided higher secondary school students is found to be 1.05, which is less than the tabled value at 0.05 level (1.96). Since the t-value obtained is less than the tabled value, it reveals that there exists no significant difference in the mean scores of awareness on technology mediated interpersonal crimes between government and aided higher secondary school students.

12. The t-value obtained for the awareness on technology mediated interpersonal crimes between government and unaided higher secondary school students is found to be 5.04, which is greater than the tabled value at 0.05 level (1.96). Since the t-value obtained is greater than the tabled value, it reveals that there exists significant difference in the mean scores of awareness on

technology mediated interpersonal crimes between government and unaided higher secondary school students.

13. The t-value obtained for the awareness on technology mediated interpersonal crimes between aided and unaided higher secondary school students is found to be 5.74 , which is greater than the tabled value at 0.05 level (1.96). Since the t-value obtained is greater than the tabled value, it reveals that there exists significant difference in the mean scores of awareness on technology mediated interpersonal crimes between aided and unaided higher secondary school students.

Conclusions

The present study summarized that the awareness on technology mediated interpersonal crimes among higher secondary schools students is low. There exists no significant difference in awareness on technology mediated interpersonal crimes among higher secondary schools students based on gender, locale. So it is clear from the findings that the awareness on technology mediated interpersonal crimes is same for the male and female students and for urban and rural students. There exists significant difference in the awareness on technology mediated interpersonal crimes among government and unaided higher secondary schools students as well as aided and unaided higher secondary school students. It is clear from the findings that the awareness on technology mediated interpersonal crimes is different for government and unaided higher secondary school students and for aided and unaided higher secondary school students. It was found that there exists no significant difference in the awareness on technology mediated interpersonal crimes among government and aided higher secondary schools students. So it is clear from the findings that the awareness on technology mediated interpersonal crimes is same for the government and aided higher secondary school students.

Tenability of Hypotheses

1. **Hypotheses (1)** states that there exists significant difference in the mean scores of awareness on technology mediated interpersonal crimes between male and female higher secondary school students. From the study it was found that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes between male and female of higher secondary school students. Hence the hypotheses is rejected.

2. **Hypotheses (2)** states that there exists significant difference in the mean scores of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students. From the study it was found that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes between urban and rural higher secondary school students. Hence the hypotheses is rejected.

3. **Hypotheses (3)** states that there exists significant difference in the mean scores of awareness on technology mediated interpersonal crimes between government aided and unaided higher secondary school students. From the study it was found that there is no significant difference in the mean scores of awareness on technology mediated interpersonal crimes between government and aided higher secondary school students. Here the hypotheses

is rejected. Whereas findings revealed there exists significant difference in the mean scores of awareness on technology mediated interpersonal crimes between government and unaided higher secondary school students and for aided and unaided higher secondary school students. Hence the hypotheses are accepted.

Educational Implications

The present study explores the awareness on technology mediated interpersonal crimes among higher secondary school students. The study gave the investigator a vivid picture of the awareness on technology mediated interpersonal crimes among higher secondary school students. The value of the research lies in its implications.

Based on the findings of the study the Investigator put forward some suggestions to improve the educational practice.

1. The present study helps to understand the awareness on technology mediated interpersonal crimes among higher secondary schools students.

2. Incorporate the study on Technology Mediated Interpersonal Crimes in the curriculum

4. Improve the awareness on technology mediated interpersonal crimes among higher secondary schools students through discussion, debates.

5. An awareness classes and workshops on topics related to technology mediated interpersonal crimes must be conducted.

6. Those with system must use comprehensive security software and keep system updated.

7. Proper training should be given to parents to be aware on technology mediated interpersonal crimes so as to train their children to be away from such crimes and be alert.

8. If you are victim of technology mediated interpersonal crime call the right person for help.

9. Take measures to protect students from such technology mediated crimes.

10. Proper cyber education should be provided to higher secondary school students.

Suggestions for Further Research

The findings of the study and the limitations encountered in the present study helped the investigator to suggest the following for further research.

1. A similar study may be conducted on a higher level sample.

2. The same study can be conducted on a wider sample state level or national level.

3. A relationship study of screen time and interpersonal crimes may be conducted.

4. A critical analysis study of the impact of internet addiction on technology mediated interpersonal crimes may be conducted.

5. A Study may be conducted on technology mediated interpersonal crimes laws and security.

6. A case study may be conducted on technology mediated interpersonal crime.

7. A critical analysis study of the impact of technology mediated interpersonal crime on Society can be conducted.

8. A study may be conducted on the Psychological impact of Technology Mediated Interpersonal crimes on students.

BIBILIOGRAPHY

BIBILIOGRAPHY

Beck, Ulrich., (1992). *Risk society Towards a New Modernity,* Sage Publications, New Delhi.

Best, J. W., & Kahn, J. V. (1997). *Research in Education*. New Delhi: PHI Learning Private Limited.

Best, J. W., & Kahn, J. V. (2012). *Research in Education* (10th Edition). New Delhi: PHI Learning Private Limited.

Cassidy, W., Jackson, M., & Brown, K. N. (2009). Sticks and Stones Can Break My Bones, But How Can Pixels Hurt Me? : Students' Experiences with Cyber-Bullying. *School Psychology International,* 30(4), 383–402. Retrieved from https://doi.org/10.1177/0143034309106948

Chan, Stephanie & Khader, Majeed & Ang, Jansen & Tan, Eunice & Khoo, Katharine & Chin, Jeffery. (2012). Understanding "Happy Slapping". *International Journal of Police Science & Management*. 14. 42-57. Retrieved from https://journals.sagepub.com/doi/10.1350/ijps.2012.14.1.252

Das, B., Sahoo, S. Jyothi., (2011). Social Networking Sites – A Critical Analysis of Its Impact on Personal and Social Life. *International Journal of Business and Social Science,* 2(14). Retrieved from https://www.ijbssnet.com/journals/Vol._2_No._14%3B_July_2011/25.pdf

Davey, S., & Davey .,A (2014).Cyber Crimes in Kerala: A study Assessment of Smartphone Addiction in Indian Adolescents: A Mixed Method Study by Systematic-review and Meta-analysis Approach. *International Journal of Preventive Medicine*, 5(12). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4336980/

Federal Bureau of Investigation. (2011). *A parents' guide to Internet safety*. Retrieved from http://www.fbi.gov/stats-services/publications/parent-guide.

Furnell, Steven. (2002). *Cybercrime: Vandalizing the information society*. Retrieved from https://capitadiscovery.co.uk/brighton-ac/items/867046.

Glasner, A. T. (2010). On the Front Lines : Educating Teachers about Bullying and Prevention Methods Aviva Twersky Glasner Department of Criminal Justice, Massachusetts Aggression Reduction Center . *Journal of Social Sciences*, 6(4), 535–539.

Goel, U. (2014). Awareness among B.Ed teacher training towards Cyber-crime-A Study, Hindu College of Education, Sonepat, Haryana, India. *Learning Community: 5(2 and 3):New Delhi Publishers.* All rights reserved DOI Number: 10.5958/2231-458X.2014.00013.X. Retrieved from http://ndpublisher.in/admin/issues/LCV5N3b.pdf

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behaviour*, *29*(2), 129-156.

Halder, Debarati & Jaishankar, K. (2013). Revenge Porn by Teens in the United States and India: A Socio-Legal Analysis. *International Annals of Criminology*, 51(1-2), 85-111. Retrieved from https://ssrn.com/abstract=2493178

Hasan, Md., Rahman, Rashidah., Abdillah, Sharifah & Omar, Normah. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11, 395-404. Retrieved from https://doi.org/10.3844/jssp.2015.395.404

Holt, Thomas J (2011), Crime *Online : Correlates Causes and Contexts. Durham,* Caroline Academic Press, USA. Retrieved from https://cap-press.com/books/isbn/9781611636772/Crime-Online-Third-Edition.

Hunter, H. A. (2009). *Computer Crime and Identity theft.* Regis University, ePublications at Regis University ,All Regis University Theses. Retrieved from https://epublications.regis.edu/cgi/viewcontent.cgi?article=1040&context=theses.

Jaishankar, K.(2011). *Cyber Criminology : Exploring Internet Crimes and Criminal Behaviour.* CRC Press: Taylor and Francis Group, USA. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.9196&rep=rep1&type=pdf.

Jose, T ., Babu, Y., Sasidhar., Manimegalai , P., & Vijayalakshmi. (2017). Advances in Computational Sciences and Technology, ISSN 0973-6107

10(5), pp. *1153-1159 Research India Publications.* Retrieved from http://www. ripublication.com.

June Ahn (2012). Teenagers' Experiences with Social Network Sites: Relationships to Bridging and Bonding Social Capital, *The Information Society*, 28(2), 99-109, Retrieved from: https://doi.org/ : 10.1080/01972243.2011.649394

Khan, Z. Afrozulla., Thakur, R. Vaishnavi ., & Arjun. (2018). Cyber Crime Awareness among MSW Students, School Of Social Work, Mangaluru . *Journal of Forensic Sciences and Criminal Investigation*, 9(2). Retrieved from https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555757.pdf

Kohut, T., Stulhofer, A. (2018). Is pornography use a risk for adolescent well-being? An examination of temporal relationships in two independent panel samples. *PLOS ONE* ,*13*(8): e0202048. Retrieved from https://doi.org/10.1371/journal. pone.0202048

Kraft, E. (2006). Cyberbullying: A worldwide trend of misusing technology to harass others. *WIT Transactions on Information and Communication Technologies. 36*. 155-166. 10.2495/IS060161. Retrieved from www.witpress.com, ISSN 1743-3517.

Lawsky, D. (2008). American youth trail in Internet use: survey. Reuters. Retrieved from http://www.reuters.com/article/2008/11/24/usinternetyouthidUSTRE4AN0MR20081124.

Lenhart, A. (2015). *Teens, social Media & technology overview.* Retrieved from http://www.pewinternet.org/2015/04/09/teens-socialmedia-technology-2015/

Lin, T., Daniel E. Capecci., Donova, M., Ellis., Harold, A. Rocha., Dommaraju ,S., Daniela S. Oliveira, & C. Ebner, C. Natalie., (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content, *HSS Author Manuscript*, *26*(5). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7274040/

Maarten, Botterman, Heuven, M. V., & Spiegeleire, D.S., (2003). *Managing New Issues: Cyber Security in an Era of Technological Change* [Kindle Edition] Rand

Mathias, D.A Prathima., & Suma, B. (2018). A Survey Report on Cybercrime Awareness Among Graduate And Postgraduate Students of Government Institutions in Chickmagaluru, Karnataka, India and a Subsequent Effort to Educate them through a Seminar , *International Journal of Advanced Research in Engineering and Technology (IJARET) 9*(6), pp. 214–228. Retrieved from http://www.iaeme.com/IJARET/issues.asp?Jtype=IJARET&vtype=9&itype=6 ISSN Print: 0976-6480 and ISSN Online: 0976-6499 © IAEME Publication

Mehta, S.,& Singh, V. (2013) A study of awareness about cyber laws in the Indian society. *International Journal of Computing and Business Research (IJCBR)* ISSN (Online): 2229-6166, *4*(1), Retrieved from https://pdfs.semanticscholar.org/a7ff/ca31b105434de2cbbcf2394952d833d18ecc.pdf

Mishra,Rajendra (2013). Social Networking Sites raging Craze among teens. *The Times of India* . Retrieved from https://timesofindia.indiatimes.com/city/ranchi/Social-networking-sites-raging-craze-among-teens/articleshow/18788654.cms

Narahari, C. Archana ., Shah, V. (2016). Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India) *IJARIIE-ISSN(O)-2395-4396,2*(6), 2395-4396 3502. Retrieved from: http://ijariie.com/AdminUploadPdf/Cyber_Crime_and_Security_%E2%80%93_A_Study_on_Awareness_among_Young_Netizens_of_Anand__Gujarat_State__India__ijariie3502.pdf.

Ng, B.D., Wiemer-Hastings., P.M. (2005). Addiction to the Internet and Online Gaming. *Psychology, Medicine, Computer Science Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society, 8*(2), 110-3. Retrieved from https://www.researchgate.net/publication/7802995_Addiction_to_the_Internet_and_Online_Gaming/citation/download.

Pittaro, M.L. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology (IJCC),1*(2),180–197. Retrieved from https://www.cybercrimejournal.com/pittaroijccvol1is2.htm

Rao, R., D., G. (2014). *Cyber Crime and Social Networking Websites a Study on the Victims and Vulnerabilities of Social Networking Sites*, University of

Madras, Department of Criminology. Retrieved from https://shodhganga.inflibnet.ac.in/handle/10603/183081?mode=full

Saima, B., (2015). *Cyber Crime Awareness amongst students of Government Law College, Trivandrum – A Legal Survey*, Government Law College, Trivandrum. Retrieved from http://glctvpm.com/images/att/PA00010/A000052.pdf

Saini, H., Rao, Y.S., & Panda, T.C. (2012). *Cyber-Crimes and their Impacts : A Review*. Retrieved from https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Reviews

Sreehari ,A., Abinanth K.J., Sujith ,B., Unnikuttan, P.S., & Jayashree. (2018). A Study of Awareness of Cyber Crime among College Students with special Reference to Kochi, *International Journal of Pure and Applied Mathematics, 119*(16). Retrieved from http://www.acadpubl.eu/hub/

Sivakumar, R. (2013). *Computer mediated interpersonal crimes: A study of cyber bullying among college students in cosmopolitan cities* (Doctoral dissertation). Retrieved from https://shodhganga.inflibnet.ac.in/handle/10603/61041

Skinner, W.F., & Fream, A.M. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518. Retrieved from http://www.ncjrs.gov/App/publications/abstract.aspx?ID=170551.

Sukanya, K. P., & Raju, C. V. (2017). Cyber Law Awareness among Youth of Malappuram District. *Journal of Humanities And Social Science (IOSRJHSS), 22*(4), 23-30. Retrieved from www.iosrjournals.org

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, *4*(1), 71–92. Retrieved from https://journals.sagepub.com/doi/10.1177/14614440222226271

Smith, P.K., Mahdavi, J.,Carvalho, M.F., Fisher, S., Russell, S., & Tippett, N. (2008).Cyberbullying: its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry, and allied disciplines*, *49*(4), 376-385.

Stringhini, G., Krügel, C., & Vigna, G. (2010). Detecting spammers on social networks. ACSAC&#39;10. Retrieved from https://sites.cs.ucsb.edu/~chris/research/doc/acsac10_snspam.pdf

Varghese, G. (2016). A sociological analysis of cyber crime security awareness among teenagers. *International Journal of Advanced Research*, *4* (12), 1048-1054. Retrieved from https://www.researchgate.net/publication/312341993_A_Sociological_Analysis_Ofcyber_Crime_Security_Awareness_Among_Teenagers/citation/download.

Walther, J. B. (1992). Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective. *Communication Research*, *19*(1), 52–90. Retrieved from https://doi.org/10.1177/009365092019001003.

Welsh, J., (2011). Is Constant "Facebooking" Bad for Teens? *Livescience,*. Retrieved from https://www.livescience.com/15433-facebook-social-media-effects-teens.html.

Wilder, M. U., (2017). The Psychology of Espionage and Leaking in the Digital Age. *Studies in Intelligence, 61*(2). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-61-no-2/pdfs/why-spy-why-leak.pdf.

Yar., Majid., (2006). *Cyber Crime and Society*, Sage Publications. London. Retrieved from https://books.google.co.in/books?hl=en&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&dq=Yar.,+Majid.,+(2006).+Cyber+Crime+and+Society,+Sage+Publications.+London.&ots=flyYmbCsOU&sig=IYDYrUGLuPjJ42xvwHxAoJAiKQs#v=onepage&q=Yar.%2C%20Majid.%2C%20(2006).%20Cyber%20Crime%20and%20Society%2C%20Sage%20Publications.%20London.&f=false

APPENDICES

APPENDIX 1

FAROOK TRAINING COLLEGE

AWARENESS TEST ON TECHNOLOGY MEDIATED INTERPERSONAL CRIMES

Dr. T.K UMER FAROOQUE
Assistant Professor
Farook Training College

SNEHA.T.S
M.Ed Student
Farook Training College

INSTRUCTION

This test is prepared for measuring the awareness on technology mediated interpersonal crimes among higher secondary school students. There are 53 items in the test. Each item carries four alternative responses A,B,C and D. Mark the correct answer by putting 'x' mark in the given response sheet.

1. The act of harassing other person using technological gadgets known as

A) Hacking B) Cyber Theft

C) Cyber bullying D) Email Stalking

2. The process of tarnishing the image, respect or dignity of any person in front of right thinking members of the society through the electronic gadgets ?

A) Cyber Squatting B) Cyber Stalking

C) Cyber Sniffing D) Cyber Defamation

3. Copying a copyrighted software without the permission of the owner?

A) Defamation B) Software Piracy

C) Logic Bomb D) Data Digging

4. Which among the following classification considered as type of hacking?

A) Grey Hat ,Black Hat, Blue Hat, Elite Hacker

B) Grey Hat ,Red Hat, Blue Hat, Worm

C) Yellow Hat ,Grey Hat, Green Hat, Red Hat

D) Skiddle, Newbie, Green Hat, Red Hat

5. Act of sending sexually explicit messages by cell phone/by emails

   A) Child Pornography B) Vishing

   C) Online Sextortion D) Sexting

6. A protocol that resolves IP address for transmitting data called as?

   A) Spoofing Internet Protocol Spoofing

   B) Address Resolution Protocol Spoofing

   C) Website Spoofing

   D) Domain Spoofing

7. The act of misusing the credit card credentials of another person or the act of impersonating the credit card owner?

   A) Forgery B) Credit Card Fraud

   C) Cyber Defamation D) Credit card jacking

8. Cyber Defamation is also called?

   A) Cyber Smashing B) Cyber Frauding

   C) Cyber Smearing D) Cyber Jacking

9. Cyber squatting refers

   A) Registering a domain name with the intent of profiting from the goodwill

   B) Act of copying and using others information without their knowledge

   C) Stealing personal information such as customer ID or pin

   D) Information accessed without authorization

10. The unsolicitated commercial email send to a large number of addresses is known as –

    A) Spoofing B) Spamming

    C) Phishing D) Software Piracy

11. Overloading a system with so many requests is known as

A) Tracking B) Espionage

C) Denial of Service Attack D) Fraud

12. The fraud act committed by using a false document, signature, or other imitation of an object of value used with the intent to deceive another known as-

A) Cyber Defamation B) Logic Bomb

C) Data Diddling D) Forgery

13. The fraud leads to the misrepresentation of a product advertised for sale through an internet?

A) Investment Fraud B) Accounting Fraud

C) Bank Fraud D) Lottery Fraud

13. The action of skewing data entire in the users system is –

A) Data Diddling B) Identity Theft

C) Online Scams D) Salami Attack

14. Practice of obtaining data and information without the permission and knowledge of the owner?

A) Cyber Squatting B) Espionage

C) Website Defacement D) Pharming

15. The procedure used by hackers to capture all the network packets is known as

A) Trojan Attack B) Scam

C) Sniffing Attack D) Spoofing

16. Cyber Stalking involves

A) Sending threatening emails or sending viruses and spam

B) Hacking into a victims computer and taking control of it

C) Connecting a device to a phone line to listen to Conversation

D) spreading rumors or tracking victims on the Web

17. Stealing tiny amounts of money from each transaction

A) Salami Slicing Attack

B) Key logger

C) Espionage

D) Fraud

18. These programs are created to do something ,only when a certain event occurs?

A) Information Theft

B) Espionage

C) Logic Bomb

D) Software Piracy

19. Phishing involves

A) Malicious attempt to interrupt regular traffic of a targeted server

B) Web hacking techniques used to destroy database

C) Deceiving individuals to gain private or personal information

D) Attempt to destroy data saved in computer

20. The term cyber terrorism was coined by

A) Ardit Ferizi

B) Winn Schwastaw

C) John Arquilla

D) Barry Collin

21. What is the rank of India among the nations facing cyber attack?

A) 5th Rank

B) 3rd Rank

C) 2nd Rank

D) 8th Rank

22. The Capital State of Cyber Crime in India

A) Trivandrum

B) Bangalore

C) Mumbai

D) Hyderabad

23. The technique used by the attacker for stealing his money is named as

    A) Salami Slicing Attack

    B) Cyber Attack

    C) Electronic Money Laundering

    D) Spam

24. Disguising a communication from an unknown source as being from a known, trusted source is called as

    A) Spamming B) Defamation

    C) Cracking D) Spoofing

25. Cyber Defamation are of……….. type

    A) 2 B) 4

    C) 7 D) 5

26. The synchronous conferencing used by hackers to share the techniques of hacking known as?

    A) Internet Instant Chat

    B) Internet Relay Chat

    C) Internet Conference Chat

    D) Internet Group Chat

27. Which of the following is an example for phishing?

    A) Spamming B) Spoofing

    C) Whaling D) Cracking

28. The best programming language for the hacking?

    A) SQL B) Python

    C) C++ D) All the above

29. Happy slapping means that

    A) unauthorized filming of an incident in a device

    B) Stealing of personal data

    C) Make a direct contact through phone calls, emails, or even in person

    D) Order to attack computers by sending spams or malware.

30. Which among the following is a cyber crime against individual?

    A) Credit Card Fraud B) Spoofing

    C) Logic Bomb D) Virus Attack

31. Which among the following is a cyber crime against organization?

    A) Cyber Terrorism

    B) Intellectual Property Attack

    C) Data Diddling

    D) Credit Card Fraud

32. Which among the following is cyber crime against property?

    A) Forgery B) Web Jacking

    C) Trojan Horse D) Credit Card Fraud

33. The techniques used by hackers to obtain confidential matters from your computer

    A) Cracking B) Spamming

    C) Botnets D) Spoofing

34. Written communication of false statement about others is known as

    A) Bullying B) Defamation

    C) Stalking D) Spamming

35. What is a person called when they try to hurt a group of people with the use of a computer?

A) Cyber Terrorist B) White Hat Intruder

C) Cracker D) Social Engineer

36. Flooding of the internet with misguiding messages are known as

A) Web Jacking B) Hacking

C) Spoofing D) Spamming

37. Physical Destruction, Psychological operation, Information attacks are major categories of-

A) Cyber Terrorism B) Cyber Squatting

C) Cyber Bullying D) Cyber Sniffing

38. Crashing Services is the type of …………. Attack

A) Salami Slicing Attack B) Deniel of Service Attack

C) Virus Attack D) Cyber Attack

39. Deliberate use of the identity of others without their permission for a financial advantage is

A) Phishing B) Spamming

C) Identity Theft D) Defamation

40. Act of sending sexually explicit videos by cell phone/by emails?

A) Online harassing B) Sexting

C) Online Sextortion D) Child Pornography

41. Spy invade into the government of another country to learn valuable state secrets is an example for?

A) Espionage B) Cyber Infilteration

C) Flooding Attack D) Spear Attack

42. A set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects known as?

A) Virus Haox B) Logic bombs

C) Sniffing D) Botnet

43. A computer ________ is a malicious code which self-replicates by copying itself to other programs.

A) Domain B) Application

C) Virus D) Malware

44. The fraud leads to the misrepresentation of a product advertised for sale through an internet?

A) Lottery Fraud B) Accounting Fraud

C) Bank Fraud D) Investment Fraud

45. The process of selling items on the internet which are not permitted under the law to be sold

A) Software Piracy B) Internet Marketing

C) e-Shopping D) Web Store

46. In this strategy the attacker compromises the DNS (Domain Name System) servers or on the user PC with the goal that traffic is directed towards malicious site

A) Software Piracy B) Spoofing

C) Pharming D) Network Enumeration

47. In which year the cyber crime recorded firstly

A) 1840 B) 1830

C) 1820 D) 1810

48. Which among the following is a type of Forgery?

A) Archaeological forgery. B) Art forgery

C) Identity document forgery D) All of the above

49. Which among the following is type of cyber squatting?

A) Typo Squatting B) Domain Squatting

C) Credit Squatting D) Trojan Squatting

50. ……….. refers to the criminal use of Internet.

A) Cyber space B) Net-crime

C) Cyber law D) Cyber investigation

51. The usage of the Internet for hours by an unauthorized person which is actually paid by another person is called __________

A) Denial of Service Attack B) Virus attack

C) Internet time theft D) Cyber defamation.

52. Spammers are classified into __________

A) Trojan and Hucksters B) Hucksters and Warez

C) Hucksters and Piracy D) Hucksters and Fraudsters

53. When a logic bomb is activated by a time related event, it is known as _____.

A) Time bomb

B) Trojan horse

C) Time related bomb sequence

D) Virus Hoax Mails

APPENDIX 2

RESPONSE SHEET

AWARENESS TEST ON TECHNOLOGY MEDIATED INTERPERSONAL CRIMES

NAME : ....

STD : ....SUBJECT : …………………………SEX:MALE/FEMALE

SCHOOL : ....PLACE : URBAN /RURAL

Sl. No.	A	B	C	D
1.	□	□	□	□
2.	□	□	□	□
3.	□	□	□	□
4.	□	□	□	□
5.	□	□	□	□
6.	□	□	□	□
7.	□	□	□	□
8.	□	□	□	□
9.	□	□	□	□
10.	□	□	□	□
11.	□	□	□	□
12.	□	□	□	□
13.	□	□	□	□
14.	□	□	□	□
15.	□	□	□	□
16.	□	□	□	□
17.	□	□	□	□
18.	□	□	□	□
19.	□	□	□	□
20.	□	□	□	□
21.	□	□	□	□
22.	□	□	□	□
23.	□	□	□	□
24.	□	□	□	□
25.	□	□	□	□
26.	□	□	□	□
27.	□	□	□	□

Sl. No.	A	B	C	D
28.	□	□	□	□
29.	□	□	□	□
30.	□	□	□	□
31.	□	□	□	□
32.	□	□	□	□
33.	□	□	□	□
34.	□	□	□	□
35.	□	□	□	□
36.	□	□	□	□
37.	□	□	□	□
38.	□	□	□	□
39.	□	□	□	□
40.	□	□	□	□
41.	□	□	□	□
42.	□	□	□	□
43.	□	□	□	□
44.	□	□	□	□
45.	□	□	□	□
46.	□	□	□	□
47.	□	□	□	□
48.	□	□	□	□
49.	□	□	□	□
50.	□	□	□	□
51.	□	□	□	□
52.	□	□	□	□
53.	□	□	□	□

APPENDIX 3

List of schools selected for the study

Sl. No.	NAME OF SCHOOLS	TYPE OF MANAGEMENT
1	GOVERNMENT VOCATIONAL H.S.S. FOR GIRLS, NADAKKAVU	GOVERNMENT
2.	FAROOK H.S.S	AIDED
3.	GOVERNMENT VOCATIONAL H.S.S, MEENCHANDA	GOVERNMENT
4.	VEDAVYASA VIDYALAYAM	UNAIDED
5	RAMAKRISHNA MISSION H.S.S	AIDED
6	PROVIDENCE GIRLS H.S.S	AIDED
7	GOVERNMENT BEYPORE H.S.S	GOVERNMENT
8	AL FAROOK H.S.S.	UNAIDED
9	ST JOSEPH BOYS H.S.S	AIDED
10	GOVT. GANAPATH MODEL GIRLS H.S.S	GOVERNMENT
11	B.E.M GIRLS H.S.S	AIDED
12	VENERINI H.S.S	UNAIDED
13	GOVERNMENT MODEL H.S.S	GOVERNMENT
14	GOVERNMENT GANAPATH VOCATIONAL H.S.S., FEROKE	GOVERNMENT