PERCEPTION OF WOMEN INTERNET USERS ON CYBER CRIME AGAINST WOMEN IN COIMBATORE CITY

Thesis Submitted in Partial Fulfillment of the Degree of

Master of Philosophy (M.Phil)

by

KALPANA.R

(14MPECF001)

Department of Economics

Avinashilingam Institute for Home Science and Higher Education for Women

Coimbatore-641043

July 2017

PERCEPTION OF WOMEN INTERNET USERS ON CYBER CRIME AGAINST WOMEN IN COIMBATORE CITY

Thesis Submitted in Partial Fulfillment of the Degree of

Master of Philosophy (M.Phil)

by

KALPANA.R

(14MPECF001)

Department of Economics

Avinashilingam Institute for Home Science and Higher Education for Women

Coimbatore-641043

July 2017

DECLARATION

I hereby declare that the Dissertation entitled **"Perception of Women Internet Users on Cyber Crime Against Women in Coimbatore city"** submitted to Avinashilingam Institute for Home Science and Higher Education for Women for the degree of Master of Philosophy (M.Phil) is a record of research work done by me during the period August 2016 to July 2017 under the guidance of Dr.Malarvizhi.V, Assistant Professor (SG), Department of Economics, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore and has not formed the basis for the award of any Degree/ Diploma/ Associate Ship/ Fellowship or other titles in this university or any other university or other similar institutions of higher learning.

Signature of the Candidate

Signature of the Supervisor

CERTIFICATE

This is to certify that dissertation entitled **"Perception of Women Internet Users on Cyber Crime Against Women in Coimbatore city"** submitted to Avinashilingam Institute for Home Science and Higher Education for Women for the degree of Master of Philosophy (M.Phil) by Kalpana.R is the record of original research work carried out by her during the period August 2016 to July 2017 under my guidance and supervision and that this work has not formed the basis for the award of any Degree/ Diploma/ Associate Ship/ Fellowship or other titles in this university or any other university or other similar institutions of higher learning.

Signature of the Supervisor

Signature of the Head of the Department

ACKNOWLEDGEMENT

First and foremost, the investigator is extremely thankful to the Lord Almighty for the grace and blessings showered to complete the thesis work in a successful way.

The investigator expresses her immense gratitude to **Dr. P.R. Krishnakumar,** Chancellor, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for providing the opportunity and exposure to a world of knowledge.

The investigator expresses her immense gratitude to **Dr. (Mrs.) Premavathy Vijayan**, Vice–chancellor, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for providing the opportunity to carry out the study in this esteemed institution.

The investigator expresses her thanks to **Dr. (Mrs.) S. Kowsalya** Registrar, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for the administrative support given for the successful completion of the study.

The investigator expresses her hearty thanks to **Dr. (Mrs.) P. Ambiga Devi**, Dean of Humanities, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for her inspiring motivation to undertake the research work

The investigator expresses her hearty thanks to **Dr. (Mrs.) K.T. Geetha,** Professor and Head of the Department of Economics, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for her guidance and help in the conduct of the study.

The investigator specially acknowledges her gratitude and considers most fortunate enough to have received an opportunity to work under the guidance of **Dr. Malarvizhi.V,** Assistant Professor (SG) of Economics, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for her expertise, inspiration, sincerity and excellent guidance and support from the beginning till the end of the entire

research period which had enriched me to develop an understanding of the subject profoundly.

The researcher extends her thanks to all the **staff members** in the Economics Department for their timely help, guidance and support for the successful conduct of the research work. Further, the researcher owes her gratitude to the **Librarian** of Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore for their encouragement and care.

The investigator extends her thanks to the **Library and Office staff** of Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for their valuable support in completion of the study.

On a more personal note, the investigator is highly grateful to **her parents, family members and friends** for their support, encouragement, understanding, care and patience rendered throughout the period of the study.

LIST OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Technological advancement and economic growth are truly related to each other. The level of technology is also an important determinant of economic growth. The rapid rate of growth can be achieved through high level of technology. Schumpeter observed that innovation or technological progress is the only determinant of economic progress. But if the level of technology becomes constant the process of growth stops. Thus, it is the technological progress which keeps the economy moving. Inventions and innovations have been largely responsible for rapid economic growth in developed countries.

The importance of expanding the access of developing countries to the Internet has been recognized by governments and international agencies with increasing consensus that the Internet and related telecommunications technology should be regarded as strategic national infrastructure (Kenney, 1995; Mansell & Wehn, 1998). The establishment of such strategic infrastructure is considered critical for developing countries where the marginal impact of improved network communications can be very high, leading to improved economic productivity, governance and education, health and quality of life, particularly in rural areas (Adam,1996; Press,1996). For example, in Africa, the growth of small scale, low cost electronic networks has been influential in building an academic and research community within the continent that discusses and shares topics of concern (Adam, 1996; Panos, 1998).

The Internet is changing the way we work, socialize, create and share information, and organize the flow of people, ideas, and things around the globe. Yet the magnitude of this transformation is still underappreciated. The Internet accounted for 21 percent of the GDP growth in mature economies over the past 5 years. In that time, we went from a few thousand students accessing Face Book to more than 800 million users around the world, including many leading firms, who regularly update their pages and share content. While large enterprises and national economies have reaped major benefits from this technological revolution, individual consumers and small, upstart entrepreneurs have been some of the greatest beneficiaries from the Internet’s empowering influence. If Internet were a sector, it would have a greater weight in GDP than agriculture or utilities.

And yet we are still in the early stages of the transformations the Internet will unleash and the opportunities it will foster. Many more technological innovations and enabling capabilities such as payments platforms are likely to emerge, while the ability to connect many more people and things and engage them more deeply will continue to expand exponentially. As a result, governments, policy makers, and businesses must recognize and embrace the enormous opportunities the Internet can create, even as they work to address the risks to security and privacy the Internet brings. As the Internet's evolution over the past two decades has demonstrated, such work must include helping to nurture the development of a healthy Internet ecosystem, one that boosts infrastructure and access, builds a competitive environment that benefits users and lets innovators and entrepreneurs thrive, and nurtures human capital. Together these elements can maximize the continued impact of the Internet on economic growth and prosperity

New information and communications technologies (ICT), in particular high-speed internet, are changing the way companies do business, transforming public service delivery and democratizing innovation. With 10 percent increase in high speed Internet connections, economic growth increases by 1.3 percent. "The mobile platform is emerging as the single most powerful way to extend economic opportunities and key services to millions of people," says Christine Zhen-Wei Qiang 2009.

Cybercrime is simply as criminal activity involving the information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

HISTORY OF CYBER CRIME

The first recorded cyber-crime took place in the year 1820, which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber-crime. Today computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

Cyber-crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber-crime has assumed rather sinister implications. Major cyber-crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland.

CYBER-CRIMES DIVIDED INTO 3 MAJOR CATEGORIES

Cyber-crimes against persons, property and Government. Cyber-crimes committed against persons include various crimes like transmission of obscene messages, harassment of any one with the use of a computer such as e-mail, cyber-bullying and cyber-stalking. The second category of Cyber-crimes is that of Cyber-crimes against organization or all forms of property. These crimes include illegal and unauthorized computer trespassing, and transmission of important and critical information

outside the organization which can lead to a great loss to the organization. The third category of Cyber-crimes relate to Cyber-crimes against Government which includes Cyber Terrorism (Nidhi Agarwal & Neeraj Kasuhik 2014).

TYPES OF CYBER – CRIMES

Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as follows: 1. Cyber-stalking, 2. Harassment via e-mails, 3. Cyber Bullying, 4. Morphing, 5. Email spoofing and 6. Cyber Defamation.

- **CYBER STALKING:** Cyber Stalking is one of the most widespread net crimes in the modern world. The word “stalking” means "pursuing stealthily". Cyber stalking can be used interchangeably with online harassment and online abuse [Muthu kumaran 2008]. It is the use of the Internet or other electronic means to stalk or harass aperson [Kumar 2010]. The utilization of technology allows stalkers to harass their target from oceans away [Cyber Stalking 2011].

  It involves invading the privacy by following a person's movements across the Internet by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language.

  While Cyber Stalking affects both men and women, women are disproportionately targets, especially of age group of 16-35, who are stalked by men. It is believed that Over 75percent of the victims are female. More than one million women and 370,000 men are stalked annually in the United States. An astonishing one in twelve women and one in forty-five men will be stalked in their lifetimes [Moore 2009]. In Cyber Stalking, stalker access the victim’s personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim [The Times of India, 2013].
- **HARASSMENT VIA EMAIL:** There is no doubt that email has become one of the most heavily used electronic tools of the last decade. Many people, send and receive in around 100 emails every day [Email Harassment in Business].

Harassment on the Internet can take place in a number of ways [Harvey]. One form may include Harassment through e-mails includes blackmailing, threatening, bullying, [Halder] constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime. In general they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman.

- **CYBER BULLYING**: Today, people all over the world have the capability to communicate with each other with just a click of a button and technology opens up new risks. Cyber bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else [Child net International]. Cyber bullying is "willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature". Globally, India is third behind China and Singapore in cyber bullying or called online bullying [Simhan]. Cases of suicides linked to cyber bullying have grown over the past decade.

  Bullying classmates, juniors or even seniors in the school is a common culture among the young school students in India [Halder, Jaishankar]. Social networking sites used in nearly half of cases. Girls are about twice as likely as boys to be victims [Do Something]. With 24 female cases were reported compared with 17 males, reveals that the victims are more often female. India is third on the list behind China and Singapore in the cases of cyber-crime according to a report, highlighting the need to take actions and increase education about online behavior.
- **MORPHING:** Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing. It was observed that female's pictures are downloaded from websites by fake users and again reposted/uploaded on different websites by creating fake profiles after editing

them. This amounts to violation of I.T. Act, 2000. The violator can also be booked under IPC also for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation [Agarwal].

- **EMAIL SPOOFING:** A spoofed e-mail may be said to be one, which misrepresents its origin [Legal India]. It shows its origin to be different from its actual source. E-mail spoofing is a popular way of scamming online. E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a known or authorized source. By changing certain properties of the email, such as its header, from, Return-Path and ReplyTo fields etc., hostile users can make the email appear to be from someone other than the actual sender. Email spoofing is possible because the main protocol used in sending emails i.e. Simple Mail Transfer Protocol (SMTP), does not allow an authentication mechanism. Email spoof can cause monetary damage also.
- **CYBER DEFAMATION:** Cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable. This occurs when defamation takes place with the help of computers and/or the Internet when someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. You build a great brand over 20 years and all it takes is 2 days to destroy it, on the Net [The Times of India 2010]. Unfortunately cyber defamation is not defined by the IT Act 2000 and it is treated by the criminal justice system under the same provisions of publication of obscene materials in the internet. With the exponential increase in the use of the internet as a medium of communication and sharing of information, chances of use of the web

for publication of defamatory content has increased multi-fold and there is a coherent need for a clear law in this area.

CYBER-CRIMES IN INDIA

Rising at an alarming rate, the number of cyber-crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges, an Assocham-Mahindra SSG study has warned. The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. India has emerged as a favourite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud.

As per the study's findings, total number of cyber-crimes registered during 2011, 2012, 2013 and 2014 stood at 13,301, 22,060, 71,780 and 1,49,254 respectively. "What is causing even more concern is that the origin of these crimes is widely based abroad in countries like China, Pakistan, Bangladesh and Algeria, among others," Assocham Secretary General D S Rawat said. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. Maximum number of offenders belong to the 18-30 age group, added the report.

With increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions, protection of personal and sensitive data have assumed paramount importance. "The economic growth of any nation and its security whether internal or external and competitiveness depends on how well is its cyberspace secured and protected," said Rawat. The attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, the study revealed.

Smartphone users rarely check for security certificates while downloading apps (games, music and other software) from third party or unsecured sites, the study said, adding that mobile banking apps store data such as PIN and account number, on the phone. There is a risk that if the phone is hacked or stolen, then the information is compromised, the study said. It further stated that mobile frauds are an area of concern

for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015.

Rising Internet penetration and online banking have made India a favourite among cybercriminals, who target online financial transactions using malicious software (malware). India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014, the study said. Andhra Pradesh, Karnataka and Maharashtra have seen the highest number of cyber-crimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries (Indian Express 2015).

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'cyberspace'. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet.

The growing importance of Information Technology can be visualized from the fact that in India for the first time a Delhi based businessman has made a digital will of the secret information saved in his e-mail account. Digital will is a foreign concept which is gaining momentum in India also. Therefore, Internet has something to offer to everybody and in the process it only increases and never diminishes.

CYBER SECURITY ISSUES

As of 2015, India had 319 million Internet and 213 million mobile Internet users. Reported security breaches raise major concerns about privacy and security of confidential data over the web. As India continues to increase its leadership in information technology (IT) in the world, Indian citizens, political organizations, public sector, and government websites have been systematically targeted for cyber-attacks and cyber security incidents. These incidents are increasing.

A state-wise breakup of cyber-crime cases registered in 2013 under various sections of the IT Act shows Maharashtra at the top with 681 cases, Andhra Pradesh with

635 cases and Karnataka with 513 cases. As many as 426 persons were arrested in cases registered under IT Act in Maharashtra, as compared to 296 in Andhra Pradesh and 283 in Uttar Pradesh. Among the cities, Bengaluru accounted for the highest incidence of cyber-crimes with 399 cases, followed by Visakhapatnam with 173 cases, Hyderabad with 159 cases and Delhi with 131 cases. In terms of arrests made under IT Act across various cities in 2013, Visakhapatnam led with 86 arrests, followed by Hyderabad with 83 arrests, Jodhpur with 69 arrests and Indore with 59 arrests. The maximum cases under IT Act registered countrywide were related to hacking at 2,516. Another set of interesting data relates to age profile of cyber-crime suspects booked under IT Act. Of the total 2,098 persons arrested under IT Act in 2013, as many as 1,190 were in 18-30 age group and 722 aged 30-45 years. Interestingly, as many as 45 minors, including 17 in Maharashtra alone and 9 each in Andhra Pradesh and Kerala, were arrested under the Act.

CYBER CRIME AGAINST WOMEN IN TAMILNADU

Of 17,060 cyber-crime complaints, only 737 registered across Tamil Nadu. The Cyber Cell of Crime Branch-Criminal Investigation Department (CB-CID) informed the Madras High Court Bench that though 17,060 complaints related to cyber-crime were received across the State in the last 10 years, only 737 of them were registered. Statistics related to cyber-crimes since 2004, Superintendent of Police (Cyber Cell) M.V. Jaya Gowri said of the total number of complaints received in connection with Internet crimes, 2,556 were related to offences committed against women though only 182 got registered. The data showed that the complaints had been increasing steadily since 2004 when only 341 complaints were received by cyber-crime cells across the State to 467 in 2005, 554 in 2006, 581 in 2007, 539 in 2008, 699 in 2009, 1,359 in 2010, 2,165 in 2011, 3,309 in 2012 and 4,066 in 2013.

The corresponding figures with respect to complaints connected with cyber-crimes against women were 76 in 2004, 98 in 2005, 103 in 2006, 97 in 2007, 100 in 2008, 154 in 2009, 204 in 2010, 278 in 2011, 501 in 2012, 683 in 2013 and 262 until August 2014. Ms. Gowri also pointed out that the number of cases registered by the police for investigation had increased from a miniscule number of 15 in 2004 to 139 in 2013.

Consequently, the number of cases registered in connection with offences against women had risen from just four in 2004 to 40 in 2013.

Data showed complaints were increasing steadily since 2004.

TABLE 1.1

INTERNET OFFENCES

Year	No of Petition Received on Cyber Crime in TN in the last 10 Years	No. of Petition on Crime Against Women	No. of Cyber Crime case Registered in last 10 years	No. of Cyber Crime Cases on Crime Against Women
2004	341	76	15	4
2005	467	98	30	9
2006	554	103	18	6
2007	581	97	34	10
2008	539	100	45	5
2009	699	154	96	11
2010	1354	204	96	20
2011	2165	278	90	20
2012	3309	501	114	29
2013	4066	683	139	40
2014	2980	262	102	28
Total	**17,060**	**2,556**	**779**	**182**

Source: Times of India, 2015

Even as Section 66A gets consigned to history, it remains to be seen what impact it will have on reporting of cyber-crimes. Data available with the National Crime Records Bureau (NCRB) shows that cyber-crime cases registered under IT Act witnessed a steady increase from 1,791 in 2011 to 2,876 in 2012 and 4,356 in 2013. Arrests too headed north from 1,184 in 2011 to 1,522 in 2012 and 2,098. In comparison, IPC was a less chosen

tool to book cyber criminals. As many as 422 cases were registered in 2011 under the relevant sections of IPC dealing with cyber-crimes, as against 601 in 2012 and 1,337 in 2013. Similarly, arrests under IPC rose from 446 in 2011 to 549 in 2012 and 1,203 in 2013.In 2014, Tamil Nadu registered 146 cyber-crime issues, with Chennai reporting 34. Kochi is the cyber-crime capital of the state of Kerala. In 2014, police received over 6,117 complaints under the Information Technology (IT) Act, including; email abuse, threatening emails, email/computer hacking, mobile phone theft, online scams, abuse of social networking sites, abusive language via phone, and stolen personal information via phone.

CYBER CRIME AGAINST WOMEN IN COIMBATORE CITY

Coimbatore City recorded less number of grave and violent offences during 2012 but crimes against women, besides rape and dowry deaths, were more when compared to Madurai and Tiruchirapalli City Police Commissionerates. Coimbatore city recorded less number of kidnapping and abduction cases in 2012 (offences under sections 363, 369, 371 and 373 of IPC). Coimbatore city had 20 cases contributing 0.09 per cent, while Chennai had 87 cases with 1.10 per cent with Madurai reporting 65 cases accounting 4.4 per cent and Tiruchirapalli 22 cases contributing 2.2 per cent. Similarly, the numbers of murder cases in Coimbatore were 29 contributing 1.3 per cent while Chennai reported 180 cases (2.1 per cent).In crimes against children, number of cases in Chennai last year was 108 contributing 1.1 per cent to the national crime graph, while it was 23 in Coimbatore recording 0.2 per cent. The following table shows that statistical record on cyber-crime in Coimbatore city during 2013- 2017.

TABLE 1.2

DATA ON CYBER CRIMES IN COIMBATORE CITY FROM 2013 TO FEB 2017

S.No	Particulars / Years	Petitions					Case Registered				
		2013	2014	2015	2016	2017	2013	2014	2015	2016	2017
1	E-mail/Face Book obscene	87	226	267	255	27	1	4	2	3	1

	Comments/ Hacking/Threat										
2	Mobile/Laptop theft/Loss	114	402	174	302	54	1	2	2	2	0
3	Obscene Calls/Threatening SMS	82	275	198	136	34	1	2	2	2	1
4	Net Banking/Online Bank Fraud/Cheating	14	25	94	97	14	1	5	2	4	1
5	Lottery or Nigerians Scam	30	21	9	0	0	0	0	0	0	
6	Job cheating	0	6	21	44	13	0	0	0	1	0
7	ATM / Credit Card Fraud	15	206	279	384	74	1	5	1	4	1
8	Others	108	182	279	226	44	1	2	1	2	1
	Total	**450**	**1343**	**1321**	**1444**	**260**	**6**	**20**	**10**	**18**	**05**

Source: Coimbatore Commissioner Office, 2017

In the table, in 2013 there were totally 450 petitions received but only 6 cases registered under cyber-crime against women. The cyber-crime were increased every year in 2014, 1343 petitions were received, in 2015, 1321 petitions were received and in 2016 still crime petitions increased to 1444 and the cases registered only few i.e, in the year 2014, 20 cases registered; in the year 2015, 10 cases registered and in the year 2016, 18 cases were only registered. The table revealed that maximum number of cases not registered because of women not show interest on crime against them due to our social problems on them.

RATIONALE FOR THE STUDY

The popularity of Internet Users among people is not unique to India, but it is a worldwide phenomenon. The formation of a global culture around Internet Users is an

emerging topic of academic interest and research. Several studies have been conducted on the Cyber Crimes among Women Internet Users in different countries across the world such as Japan, Norway, Finland, USA, and Britain. The study adds to the growing body of research by providing empirical information about the Cyber Crimes among Women in India. Academic research on Internet usage among Women in different countries has looked at various issues such as their use as fashion items for communication with friends and family, to access news and their use for personal entertainment. Therefore, a study on perception of women internet users on cyber-crime against women in Coimbatore city was undertaken with the following Objectives

The specific **objectives** of the study are:

(a) To study the characteristics of women internet users in Coimbatore City.

(b) To examine the reasons and types of Cyber Crime against Women.

(c) To elucidate the problems faced by women on Cyber Crime.

(d) To analyze the awareness about Cyber Crimes among Internet Users.

(e) To give suggestions to curb the Cyber Crime against Women.

HYPOTHESES

In the course of the study the following hypotheses were examined.

- Inter users are young and highly educated.
- The opinions of respondents regarding Internet services do not differ significantly.
- There were no significant differences in the Harassments in Online across Victimized and Non-victimized respondents of Cyber Crime.
- The respondents did not differ in the ranking of the Location of Online Abuse of Cyber Crimes.
- The problems in Cyber space are the same for the victimized and non-victimized respondents
- There is no association between Awareness on Cyber Culture among Indian Internet users among the Victimized and Non-victimized respondents.
- The strategies suggested by the internet users for reducing crimes on internet are the same for victims and non-victims respondents.

CHAPTER II

REVIEW OF LITERATURE

The review of literature for the present study is presented and discussed under the following heads:

I. Cyber Crimes against Women in Foreign Countries

II. Cyber Crimes against Women in India

III. Crimes or Violence against Women in India

IV. Related studies

CYBER CRIMES AGAINST WOMEN STUDIES RELATED TO FOREIGN COUNTRIES

Michelle F. Wright (2016) examined the longitudinal, bidirectional associations between Cyber victimization, suicidal ideation, depression, and anxiety among college students, using cross-lagged models. These relationships were examined over 4 years. Participants were 1,483 college students (Mage ¼ 24.67; 60percent female; 35percent White, 15percent Black/African American, 10percent Latino/Latina, 6percent Asian, and 4percent biracial) from South-eastern universities in the United States. The study completed self-reports of face-to-face and Cyber victimization and questionnaires on suicidal ideation, depression, and anxiety at four time points over 4 years. The study revealed that, Cyber victimization contributed to suicidal ideation, depression, and anxiety over time, and that suicidal ideation, depression, and anxiety each contributed to Cyber victimization over times well.

Anna Leppanen, et.al, (2016) studied the Cyber-physical space of a small nation is policed. The qualitative study is based on content analysis of expert interviews. The study found that, the country is protected and daily incidents solved by a network of government agencies and private companies, forming a loose public–private partnership network. The study detected two problems as the major finding of the study; first, it was not clear that sufficient focus would be available to resolve several simultaneous large incidents and second, Cyber-Crimes are still under-reported, which may hinder the police in building investigation capacity.

Ryan C. Maness and Brandon Valeriano (2016) examined the impact of Cyber conflict on foreign policy relationships. The study used weekly events data to examine exactly what happened between countries when Cyber conflict is utilized as a foreign policy choice. The study used previously constructed data set of Cyber actions and measured conflict and cooperation after a Cyber operation to understand the true impact of this new way to harm a state and society. The study found that only one method of Cyber malice, denial of service, and one tactical goal, seeking a change in behaviour in the opposing side, impacts conflict–cooperation dynamics between states.

Jackson T.C.B. Jack and Robert W.Ene (2016) examined the nature and dynamics of cybercrime in Nigeria and its contribution to the socio-economic development challenges in the country. The study adopted the library research method as secondary data sourced from articles, journals, periodicals and publications were utilized. Anchored on the risks society theory, the study argued that the internet revolution and the advent of mobile telephone technology in the country has posed unintended risks to the society evident in increasing surge in cybercrime such as yahoo-yahoo-advanced fee fraud, hacking, cyber stalking, virus attacks, espionage, character defamation, pornography, online gambling and so on. The study concludes that widespread cybercrime has negative impact on the socio-economic development of Nigeria as it tarnishes the image of the country at the global scale, deters foreign investments, and reduces confidence in the digital economy; with huge financial loses to individuals, business organizations and the government. Following these submissions, the study recommended that the Nigerian government should enact comprehensive laws to curb cybercrime, while building the capacity of security experts on contemporary cyber technology; also the government should provide jobs and entrepreneurial development opportunities to engage young people to keep them away from crime, while pursuing vigorous enlightenment campaigns for the citizens on basic preventive and protective measures against cybercrime.

Michelle F. Wright (2015) discussed multiple sources of strain, particular Cyber victimization, and perceived stress from parents, peers, and academics, in relation to late adolescents' (ages 16-18; *N* = 423) Cyber aggression, anxiety, and depression, each assessed 1 year later (Time 2). Three-way interactions revealed that the relationship

between Time 1 Cyber victimization and later depression was more positive when adolescents experienced high perceived stress (i.e., parents, peers, academics) and engaged in high Cyber aggression. Time 2 anxiety and Time 1 Cyber victimization were more strongly associated at higher levels of Time 1 perceived peer stress such that Cyber aggression did not have the same joint role in these associations as it did with depression. The study found that dual sources of strain combined with aggressive behaviours might negatively affect adolescents' well-being, particularly their depression.

Sheryl A. Hemphill et.al, (2015) compared the individual, peer, family, and school risk and protective factors for both traditional and Cyber-bullying victimization. The study drawn on data from 673 students from Victoria, Australia and to examine Grade 7 (aged 12-13 years) predictors of traditional and Cyber-bullying victimization in Grade 9 (aged 14-15 years). The participants were completed a modified version of the Communities That Careyouth survey. There were few similarities and important differences in the predictors of traditional and Cyber-bullying victimization. For Grade 9 Cyber-bullying victimization, in the fully adjusted model, having been a victim of traditional bullying in Grade 7 and emotional control in Grade 7 were predictors. For Grade 9 traditional bullying victimization, predictors were Grade 7 traditional bullying victimization, association with anti-social peers, and family conflict, with family attachment and emotional control marginally statistically significant. The use of evidence-based bullying prevention programs is supported to reduce experiences of both traditional and Cyber-bullying victimization, as is the implementation of programs to assist students to regulate their emotions effectively. The study concluded that the traditional bullying victimization may be reduced by addressing association with anti-social friends, family conflict, and bonding to families.

Alison Marganski and Lisa Melander (2015) explored the extent of Cyber aggression victimization in intimate relationships and its co-occurrence with in-person experiences of psychological, physical, and sexual partner violence. The data were collected from 540 college students who reported being in a dating relationship in the past 12 months. Participants were asked to complete an online questionnaire that included measures assessing intimate partner victimization experiences in differing social contexts

(through socially interactive technology and in face-to-face encounters). The indicated that intimate partner Cyber aggression victimization is not uncommon, as nearly three quarters of respondents reported having experienced some form of it in the past year. Multivariate analyses also indicated that such aggression may be part of a larger violence nexus given its relation to in-person psychological, physical, and sexual partner violence victimization experiences.

Brandon Valeriano and Ryan C Maness (2014) the study discussed of the concept of Cyber war, Cyber conflict, and the changed dynamic of future security interactions is founded upon the study of what could be, conjured through spectacular flights of the imagination. The aim of the study is to exhaustively collect information on Cyber interactions between rival states in the last decade. The study can delineate the patterns of Cyber conflict as reflected by evidence at the international level. The field of Cyber security needs a clear return to social science in order to be able to definitively engage the Cyber debate with facts, figures, and theory. The study provided a data set of Cyber incidents and Cyber disputes that spans from 2001 to 2011 and data include 110 Cyber incidents and 45 Cyber disputes. The study found that, the actual magnitude and pace of Cyber disputes among rivals does not match with popular perception; 20 of 126 active rivals engaged in Cyber conflict.

Duygu Solak and Murat Topaloglu (2014) examined the differences among the Cyber-Crime perceptions of undergraduate students at Trakya University in terms of demographic factors. The method of the study were questionnaire that was given to lecturers and students at Trakya University sample and it was designed to measure and assessed the levels of interest in technology, the severity of Cyber Crimes and the individuals' perceptions of Cyber-Crimes in terms of ethics and law. The study defined the level of common perception of Cyber-Crimes and the meaningful differences between separate groups.

Lorena Montoya (2014) analyzed the relationship between the extent of economic activities and services and five types of Crimes using data from Utrecht in Holland. The study based on primary data collection method. The study showed that, (a) a relationship

does exist, (b) the effect of some sectors is constant across Crime types, and (c) some activities have a positive relation whilst others a negative relation with Crime.

Odumesi and John Olayemi (2014) studied the Global Information Infrastructure creates unlimited opportunities for commercial, social and other human activities. However, it is increasingly under attack by cybercriminals; as the number, cost, and sophistication of attacks are increasing at an alarming rate. The study set out to examine the sociological and technological factors that impact cybercrime and cybersecurity and thereby articulates the relevant circumstances and threats of cybercrime in Nigeria. The study approached the issue of cybercrime from theoretical and investigative points of views. Structured interviews with law enforcement agencies and governmental institution for cyber security were conducted. Data obtained through these research instruments were subjected to descriptive analysis and frequency counts in order to explain the activities of Nigerian cybercriminals based on existing theories of crime, and to understand their intents, purposes and methods. Four theories of crime, namely, Structural Functionalism Theory, Marxian Theory, Routine Activity Theory and Technology Enabled Crime Theory were all found to be relevant to Nigerian cybercrime. At the level of existing laws, the study established that there are no existing laws in the Nigerian statues that directly address cybercrime.

Lewis Herrington and Richard Aldrich (2013) analysed the future landscape of UK Cyber-resilience and found that 80 per cent of the UK's critical national infrastructure is in private hands and the last decade has seen efforts to legislate away some of the problem of resilience by creating legal duties for service providers. This has contributed to a new ecology for intelligence, security and resilience consisting of complex state–private citizen partnerships. The study further extended robust Cyber-defence after the Stuxnet event of 2010. Arguably, any system that depends on information technology, however well protected, is now vulnerable. There is a dawning realisation that the best technical solutions offer only partial assurance. Paradoxically, in an era when the Internet seems ubiquitous, a mixture of analogue and manual systems – often called systems diversity – offers a solution. However, with the threat of serious state-based Cyber-war

now looming, experts view human beings together with ‘heritage theme park’ systems as the last line of defence against a sophisticated Cyber-attack.

Adam C. Tagert (2010) examined the guidance that is being given to developing nations that are rapidly deploying information and communication technologies. He studied the African countries of Rwanda and Tunisia to draw lessons of the situation and potential methods of improving the situation. The study found that developing nations are often recommended to implement a conglomeration of existing rules and regulations found in other countries especially in European countries and in the United States. Developing countries are also recommended to create national CERTs, organizations of cyber security experts to coordinate a nation to respond to cyber incidents. The proposed rules and regulations are largely irrelevant for developing nations and the proposed missions of a CERT do not match the needs of those countries. In promoting better guidance, the thesis identifies and discusses several challenges. It finds policy makers in developing nations are aware of the cyber threat, and that the cyber threat is different and often smaller in less ICT developed nations even if they are using similar equipment and software. To help craft better recommendations, the thesis identifies the benefits of ICT especially in agriculture, education and government. These benefits are analyzed to determine whether they would be protected by current guidance and the analysis determines that protecting ICT use in government should be the priority. In crafting future guidance the challenges are that nations have differences in ICT architecture and ICT use, and developing nations have fewer resources but also they have different resources to use. Another such difference is the common lack of a private cyber security sector and different expectations of government. This thesis concludes with discussing unexpected results. The first is Rwandan policy makers desire good enough security and have a higher risk tolerance concerning cyber threats than is found in more developed nations. In addition, open source software can be a potential way to reduce the cost of cyberspace defense and this thesis makes an initial investigation. The lesson of the thesis is that cyber security strategy is not a one size fits all and so it must be customized for each country.

Ibrahim Baggili and Marcus Rogers (2009) focused on understanding psychological concepts related to Cyber Crime. The study is based on Primary Data collection, the participants were randomly assigned to three groups with varying degrees of anonymity and the participants were asked to self-report their Cyber Crime engagement, and pre-employment integrity. The study indicated that, the anonymity manipulation had a main effect on self-reported Cyber Crime engagement and also showed that there is a statistically significant negative relationship between self-reported Cyber Crime engagement and pre-employment integrity.

Sudershan Pasupuleti et.al, (2009) aimed towards Crime, criminals, punishment, and treatments are shaped by social forces, which differ across nations. The study compared the Crime views of Indian and U.S. college students. The study found that there were significant differences between Indian and U.S. respondents in their views toward Crime, criminals, punishment, and treatment. There were mixed views on punishment and rehabilitation among both groups of students. In a multivariate analysis controlling for gender, age, academic level, and religious saliency, nation of the respondent was one of the best predictors for these views. The differences in views were attributed partly to the cultural differences between the two nations.

CYBER CRIMES AGAINST WOMEN IN INDIA

Teena Jose et.al, (2016) 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 Trissur are taken for analysis. A district wise analysis of the cybercrimes in Kerala is made.

Japleen Pasricha (2016) reported that in India, as elsewhere in the world, online harassment of women and marginalized genders and sexualities is rampant, in contrast

to Internet's initial premise of equal opportunity and neutrality. Today is a flawed internet that reflects the offline world people live in, where women and marginalized communities are abused, harassed, threatened, stalked and violated on a daily basis. The research report aims to analyse the unique threats that women and marginalized sections in India face online and how Indian laws affect these problems. The report used both qualitative and quantitative research method, including analysis of media reports involving online harassment of high profile women; a survey of 500 social media users; and interviews with ten of the respondents. The majority of survey respondents were women under 35, living in major cities, and educated to college level or above. The report found that Online abuse is a serious issue in India, affecting more than half of survey respondents, yet women and other targets lack support and understanding to respond effectively.

Mayank R. Kothawade and Preeti Agarwal (2016) analyzed every crime has its impact specifically on society, nation and the world to the great extent. By the surveillance of cybercrime and its phenomenon it is exposed that similar to former crimes it has badly affected social life of humans. To understand the influence of cybercrime, it is necessary to look into the impact of two things computer technology and internet on people as cybercrime is no doubt originating out of these. There are inherent challenges to the field of IT security and services through individuals and critical infrastructure. Socially, people are now more open to communicate and interrelate with others compared to past which widen the objectives from the personal relations to the professional ones. Today, there is no single reason for the people to interact through internet but thousands. The advantage behind this mediator is its collaborating and speedy communication which is lacked in other medium of communications. Technological innovation is an evolutionary process. Personally the researchers also finds IT to be interesting, intriguing and powerful, at a same time challenging, confusing and risky. The study focused on critical infrastructure scenario in India, facts around usage of internet and exploration of cybercrimes under diverse heads across India.

T Neelam Seam (2015) he expanding reach of information technology has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that

enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior towards women. Any technological development is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment. The study attempt to highlight the cybercrimes against women in India. To make the study richer a brief glance of the cyber-crime protection laws especially for women in UK and USA is taken as reference point. However the economic, political and social conditions of these countries are different to each other. Moreover the problem against women is also treated of the same nature worldwide. The study throws light on the types of cyber-crimes against women in India in the light of Information Technology Act, 2000. And viz-a-viz the problems and loopholes behind dealing with Cyber Crimes against Women. The study found some precautionary measures, so that women can protect themselves from the cybercrime instead of make their dependence upon legal system.

Anjana Kumari, et.al, (2015) presented a predictive analysis of Cyber Crimes against women in India and laws that prevent Cyber victimization in general and women in especially. The study was divided into four parts. The first part gives the introduction and the related work on Cyber Crime against women. The part two provided actual analysis of Cyber victimization of women in India. The part three of the study predicted the effectiveness of current legal protection that are available to women victims in India of Cyber Crimes such as Cyber stalking, harassments, threatening, blackmailing, and defamation in the Cyber space. The part four discussed various loopholes that exist in Indian law, especially the Indian Information Technology Act 2000 & 2008, and suitable solutions are provided. The study examined that Cyber abuse or the Cyber Crimes goes unreported as Indian women's are unaware of such offences this nature provided the chance to escape after the commission of Cyber Crime. The study found that, the biggest problem of the Cyber Crime lies in the modus operandi and the motive of the Cyber criminals.

Jaspreet Singh (2015) mainly focused on violence against women through Cyber space and internet; he outlines the condition of Indian women in Cyber space and the

factors leading to Cyber victimization against women. The study used both primary and secondary resources like book, reports, articles, news, web and electronic sources, etc. The study concludes that the visibility to overcome the Cyber Crimes against women as a whole is challenging and the only way is to understand Cyber Crimes. Government needs to strengthen the legal system to lower Cyber Crimes, because criminals consider it much easier than traditional Crimes due to less chance of being caught and fewer penalties. Secondly, the needs to be changed are the sense or attitude of the society towards women, not to consider woman as a commodity. People have to understand that violence against women is nothing but a manifestation of gender discrimination and inequality in gender power relations. Thirdly, women should understand that the time has come to reject the silence or reticence and come forward for fighting against Cyber Crimes and for their rights. Fourthly, it requires that the regular research and attention on Cyber Crimes needs to be studied in detail which should be funded by government. Fifthly, police personnel must be given training in order to tackle and handle Cyber Crimes. For this purpose, workshops and seminars on Cyber space education must be organized and women should also participate in such type of activities.

Shivani Grover (2015) explained that Nation Crime Record Bureau (NCRB) report showed the rapid increase in Cyber Crime in India by 50percent from 2012 to 2013. As we move in 2016, cyber-attacks will continue to become more innovative and sophisticated. There have been several incidences of cybercrimes on corporate and individual level in the past few years. Putting the data of 1.2 billion people on the cloud could be risky and could threaten the security. Hence the Digital India project demands very strong network security at all levels of operation. It is undoubtedly one of the largest and most exciting initiatives that we have embarked upon in the last decade.

Pooja suman (2015) examined Cyber-crime is a new horizon controlled by machine for information and any criminal activity where computer or network is used as the source, tool or target is known Cybercrime. The common types of cybercrime discussed under the following heads: hacking, cyber stalking, cyber pornography, phishing, web jacking, software piracy, and cyber terrorism. Cybercrime against women in India is relatively a new concept. When India started her journey in the field of

Information Technology, the priority was given to the protection of electronic commerce (e-commerce) and communications under Information Technology Act, 2000 whereas cyber socializing communications has remained untouched. The Act turned out to be a half-baked law as the operating area of the law stretched Cyber Victimization of Women and Cyber Laws in India. The study attempted to highlight the cybercrimes against women in India. To make the study richer a brief glance of the cyber-crime protection laws especially for women in UK and USA is taken as reference point. One might question these reference countries, but there is not much harm to draw some inferences based on their laws. The reason is that nature of the problems originated from the information and communication technology remain more or less same across the world, however the economic, political and social conditions of these countries is different to each other. Moreover the problem against women such as Harassment via e-mails, Cyber-stalking, Cyber pornography, Defamation, Morphing, Email spoofing, etc. are also treated of the same nature worldwide. The study throwed light on the types of cyber-crimes against women in India in the light of Information Technology Act, 2000.

Shalini Kashmiria (2014) studied the Cyber Crimes against women in India, Comparative analyses have been used between the Cyber laws regulating Cyber Crimes in India, United Kingdom and United States of America. Secondary data Source have been used for data collection. The study found various Crimes against women and the legal framework regulating these Crimes in India. The study conclude that guard again the sophisticated skills of Cyber criminals, a global culture of Cyber Security needs to be developed in turn required besides good policing and legislation, though ICT based majors uniform in applications beyond jurisdiction.

Tanaya Saha and Akancha Srivastava (2014) examined the various reasons behind the fact as to why Indian Women are being victimized and a conceptual model of Cyber victimization of Indian women is proposed. The study represented a conceptual model of reasons of Indian Women Victimization, online. The study concluded from the model that various drivers are triggering Cyber Crimes through women victimization.

CRIMES OR VIOLENCE AGAINST WOMEN

Nithya N.R (2013) discussed the forms and types of violence against women. In all societies, to a greater or lesser degree, women and girls are subjected to physical, sexual and psychological abuse that cuts across lines of income, class and culture. The study is based on Secondary data collection method. The study found that, the most common Crimes against women in India are sexual harassment, rape, dowry, child marriage, female infanticide and sex-selective abortion, domestic violence and trafficking. The study concludes that, the women empowerment approach to combat violence against women should be well integrated and inter woven into all policies and programs of the governments. Women should be equal partners not only at the public places but should have adequate control of their own resources.

Sophia J. Ali (2011) the study investigated the challenges facing women in career development, and the study found that most of the women employees were dissatisfied with career development programmers and women were discriminated against in career development opportunities. The study recommended that, organizations should strive to ensure that career development programmers were set to enhance career development amongst women employees. Top management should also be committed to the career development of women, and organizations should also introduce affirmative action to urgently address career development of women.

The World's Women (2010) report of the United Nations Organization, noted that violence against women is a universal phenomenon. Women are subjected to different forms of violence – physical, sexual, psychological and economic–both within and outside their homes. Rates of women experiencing physical violence at least once in their lifetime vary from several per cent to over 59 per cent depending on where they live. Current statistical measurements of violence against women provide a limited source of information, and statistical definitions and classifications require more work and harmonization at the international level.

R.N. Mangoli and Ganapati M. Tarase (2009) explored the main causes in increasing the trend of Crime against women, the effectiveness and impact of existing laws to control followed by important suggestions to prevent further commission of

particular Crimes in India. The study is based on both primary and secondary data like Crime reports, journals, books and internet surveys etc. The study concludes that the Crime rates from (7.6percent) in 2003 to (8.8percent) 2007 in last five years at the national level and when the study, only compared mega cities with the total national Crime rate, it is sharply increased from (24,709) in 2007 to (21,861) in 2006, a total increase of (13.0percent) in just one year that the hazardous situation in the country like India with respect safety and security of women. Not only that even foreigners are also not been spared who are coming to India as many cases have been booked under rape and murders against the foreigners. In this era of globalization there is an urgent need to motion our Criminal Justice System of India in maintaining law and order situation of the country that one should feel safe and secure.

Ahmad and Aminah (2007) discussed the work-family conflict experienced by 239 married female production operators in dual-career families, the social support they received and the coping strategies used to manage the conflict. The study found that, the women experienced more work interference with family than family interference with work. The intensity of work interference with family was significantly higher in the earlier life-cycle stage than in the later stage. About two thirds of the women indicated that, they intended to leave their job upon having another child, mainly due to the rising cost of child-care services. They received the least social support from their supervisors compared to other sources, and tended to cope with conflict using reactive role behaviour and personal role redefinition strategies.

Tark and Kleck (2004) in their work, Resisting Crime: The Effects of Victim Action on the Outcomes of Crimes, concluded in their study that in case of sexual assault the most effective measure in prevention is victim's resistance. They have suggested various means to resist assailant's assault. These can be forceful physical resistance such as free fist flows, blows on face, abdomen or pelvic region or kicking, non-forceful physical resistance such as dodging assailant's hits or blocking hits and verbal resistance such as yelling, threatening, calling for help and other noise scaring tactics. In their research they found that it is the injury which occurs first in case of victim's resistance, followed by sexual assault

Chandan Mukherjee, et.al, (2001) in their work Crimes against Women in India: Analysis of Official Statistics stated that social scientists have neglected the study of crime despite its increasing presence in our daily lives. They attempt to see what official, published data reveal, whether there are clear-cut regional patterns and if so whether they can lead to meaningful hypotheses for future work. There are some significant researches being conducted by scholars in finding important factors influencing reporting behaviour of victims of violence.

Sheela Saravanan (2000) "Violence against women in India-A literature Review" opined that violence against women is partly a result of gender relations that assumes men to be superior to women. Given the subordinate status of women, much of gender violence is considered normal and enjoys social sanction. Manifestations of violence include physical aggression, such as blows of varying intensity, burns, attempted hanging, sexual abuse and rape, psychological violence through insults, humiliation, coercion, blackmail, economic or emotional threats, and control over speech and actions.

As per **World Health Organization Report, (2013)** an estimated 35 percent of all the women worldwide have faced crimes against them in the hands of current or ex-partners. United Nations recognized the crimes against women in various other forms of crimes such as human trafficking, honor killing or forced prostitution which have taken an endemic route worldwide. To address the problem of crimes against women had been inadequate from legalperspective and the role of Victimology and dedicated NGO's in the latter half of the 20th century brought significant attention to the problem of crimes against women.

RELATED STUDIES

Shubham Kumar et.al, (2015) discussed internet in India is growing rapidly. It has given rise to new opportunity in every field like – entertainment, business, sports, education etc. It is universally true that every coin has 2 sides, same for the internet, it uses has both advantage and disadvantage, and one of the most disadvantage is Cyber-crime. Cyber-crime is any illegal activity which is committed using a computer network (especially the internet). Also, cyber-crime involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software. In India most

of cyber-crime cases are committed by educated person (some cyber – crime requires skills). So, it is required the deep knowledge about the cyber –crime and it prevention. Also, in India most of the cases found where, crimes are committed due to lack of knowledge or by mistake. The study discussed various categories and cases of cyber-crime which is committed due to lack of knowledge or sometimes due to intention behind. The study suggested various preventive measures against these unlawful acts in day to day life.

Manisha M. More et.al, (2015) investigated that in the era of globalization Internet banking or online banking has revolutionized an integral activity of our modern twenty first century. The man developed various ways for communication to the exchange of information, ideas and knowledge which is of great importance to him as a social being. The evolution of e-banking technology makes the task very easy, banking transactions becomes very fast within a click. Online and mobile banking make daily banking fast and convenient. The misuse of information technology in the cyber space is clutching up which gave birth to cyber-crimes at the national and international level. The percentage of risks and the challenges associated with it is increased. However online and mobile banking is never 100 per cent safe. The purpose of the research is to review current scenario of online banking and cyber-attacks. The study focused on cyber-crimes related to online banking and new tricks and techniques used by hackers. It also gives the details on Indian cybercrime Statistics. The latest cybercrime news related to online banking is also identified. The study totally based on the secondary data. To review and analyze the current scenario of cybercrimes, they focused on the annual reports of National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (CERT), Internet Crime Complaint Center (IC3), the Global Information Security Survey 2014-15, Press Information Bureau English Releases, Reserve Bank of India publications. The findings of the research paper shows that the IT usage and cybercrime related to online banking in India are on the rise. Majority of the cybercrimes have been committed by young people in the age group 18-30 years and were male gender. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber-crime. Finally researcher has given some suggestions for the prevention and safety use of online banking services.

Nidhi Agarwal & Dr Neeraj Kasuhik (2014) studied Information technology has widened itself over the last two decades and has become the axis of today's global and technical development. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. The study explored the Cyber-crimes and the online security vulnerabilities against women. Cyber-crime is emerging as a challenge for national and economic security. Various issues that discussed like: Cyber Stalking, Harassment via Email, Cyber Defamation, Morphing, and Email Spoofing against women.

Janhavi J Deshmukh and Surbhi R Chaudhari (2014) analyzed that there has been tremendous growth in use of Internet .Technology give rise to Cyber Crime. Cyber Crime is technology based crime committed by technocrats. The study dealt with variants of cyber-crime like Salami Attack, Packet Sniffing, Tempest Attacks, and Bot Networks. It also included real world cyber-crime cases their scenario and modus operandi. The global spam rate, malware rate and phishing rate is increasing rapidly. And there is a potential impact of cyber-crime on economics, consumer trust and production time. The counter measures like GPRS Security architecture, Intrusion Detection and prevention System and Agent Based Distributed Intrusion Detection System are used for security purposes.

Sumanjit Das and Tapaswini Nayak (2013) studied the facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber-crime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of cyber-crimes is dependent on proper analysis of their behaviour and understanding of their impacts over various levels of society. Therefore, the manuscript was a systematic understanding

of cyber-crimes and their impacts over various areas like Socio-eco-political, consumer trust, teenager etc., with the future trends of cyber-crimes were explained.

Yougal Joshi and Anand Singh (2013) observed Cybercrime is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately.

Shobhna Jeet (2012) surveyed in the digital age, Information and Communication Technology (ICT) is benefiting billions across the world by bridging certain gaps and multiplying human potential in every walk of life. Digital services provision that is being developed for our society has enormous positive potential. The internet has revolutionized the way businesses approach and conduct work. For consumers, the idea of purchasing online is appealing for several reasons. A well designed and implemented e-commerce system can lower transaction costs, reduce inefficiencies, promote better information flow and encourage better co-operation between buyers and sellers. With little more than a click of a mouse, business can communicate, engage in commerce, and expand their business opportunities. At the same time, there are certain social, political, and economic implications being observed globally either in the form of ‘spying websites’ like ‘wikileaks’1 hacking activities or cybercrimes against women. Along with promoting the use of Information and Communication technologies since their inception, countries have been looking at ways to counteract the negatives simultaneously.

Hemraj Saini et.al, (2012) analysed in the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behaviour is difficult to early understanding hence difficult to restrict in the early phases of the cyber-attacks. Cyber-attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cybercrime and they have serious impacts over the

society in the form of economical disrupt, psychological disorder, threat to National defence etc. Restriction of cyber-crimes is dependent on proper analysis of their behaviour and understanding of their impacts over various levels of society. Therefore, the study provided the understanding of cyber-crimes and their impacts over society with the future trends of cyber-crimes.

Kamini Dashora (2011) explored the world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Cyber-crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. The study attempted to provide a glimpse on cyber-crime in society and various reports from news media and news portal.

Ronald J. Burke, et.al, (2010) examined the relationship of the perceived presence of organizational practices designed to support women's career advancement and their work attitudes and satisfaction and their psychological well-being. Data were collected from 286 women in managerial and professional jobs working in a large Turkish bank, a 72 percent response rate. Five organizational experiences were considered: negative attitudes towards women, equal treatment, support, career barriers and male standards. Women reporting more supportive organizational experiences and practices were more engaged in their work, more job and career satisfied, and indicated greater levels of psychological wellbeing.

Jock Collins (2007) focused on Sydney, the aim of the study is to explore a number of aspects of immigrant victimology in Australia: immigrants as victims of Crime· as victims of the fear of Crime; as victims of racial abuse and violence in the aftermath of the 11th of September, 2001; and as victims of media discourses about 'ethnic Crime'. The study were conducted with the article draws on national and international research

into immigrant Crime and immigrant victimology and on two sources of primacy data: a Sydney survey of 825 youth and adults (eighty per cent of whom were immigrant minorities) and data from a Hotline established in Sydney in the immediate aftermath of 9/11. The study provides evidence of each dimension of migrant victimology and concluded that there has been a disproportionate focus on, and fears of, immigrant or 'ethnic' Crime in the Sydney media.

Madan Mohan Oberoi (2002) study aims to evolve a framework for developing regulatory enforcement policy related to e-commerce / cyber-crime. It makes an attempt to identify and critically discuss various regulatory and enforcement issues concerning e-commerce and cyber-crimes. The broad objectives of the study include comparative analysis of different cyber laws; examining the impact of various factors on growth of e-commerce and cyber-crime; analysis of policy implications of electronic money; analysis of legal, social, economic, political and strategic policy implications of electronic commerce; identification of problems faced by law enforcement agencies in tackling cyber-crime and steps to be taken to remove them. A reasonably comprehensive survey of literature was done. It has been organized under five broad heads namely, e-commerce, cryptography concepts & issues, electronic money, cyber laws and cyber-crime. Review of literature helped in identifying the issues. The important issues included uniform global cyber laws, security of electronic records, privacy of personal information, investigation of cyber-crimes, intrinsic value of e-money, systemic and other risks of e-commerce and so on. The principles of flexible systems methodology have been used for study design. The entire study design was divided in three parts namely exploratory, empirical and analysis & synthesis. A matrix of cyber laws was prepared on 43 dimensions, using 12 cyber laws. Options Field Methodology was used to generate list of options for all 43 dimensions. Four case studies were also used. Indian IT Act was analyzed using options fields generated and the case studies. The policy implications arising out of various issues concerning e- money were analyzed. The implications were analyzed from the point of view of four actors namely, government, banks, consumers, and law enforcement agencies. The major policy issues were identified as power to issue

e-money, intrinsic value of e-money, systemic and tither risks, control of monetary aggregates, liability of stolen / compromised e-cash. Factors influencing growth of e-commerce and cyber-crime were studied. Idea engineering workshop generated 40 variables influencing them. These were grouped in 10 broad factors using Interpretive Structural Modeling (ISM). An Interpretive Structural Model was also prepared for modeling the influence of these broad factors. Exhaustive lists of legal, social, economic, political and strategic policy implications of E-Commerce were prepared from survey findings. These were analyzed in SAP paradigm from the point of view of the following major actors: Government, Enforcement Agencies, Judiciary, Legislature, and Business Organizations. A survey was also conducted to find the perception of users (Business organizations, policy making bodies of government and enforcement agencies) of e-commerce about various regulatory / enforcement issues. The survey findings were also used to identify the problems being faced by enforcement agencies in investigating cyber-crimes and solutions thereof. The research study concluded with the discussion of significant contributions of the research, limitations of the work and scope for further research in the area.

CHAPTER – III

METHODOLOGY

The methodology for the present study is discussed under the following heads:

I. Locale of the Study
II. Selection of the Sample
III. Data base of the Study
IV. Period of the Study
V. Techniques of Analysis
VI. Limitations of the Study

I. LOCALE OF THE STUDY

Coimbatore, popularly known as the Manchester of South, is the third largest city and the second among the most industrialised cities in Tamil Nadu. It is located in the western part of Tamil Nadu, on the banks of river Noyyal. It is surrounded by the Fairy Queen; The Nilgiris (the Blue Hills) in the north, the revolutionary Western Ghats side of Kerala in the west, newly formed Tiruppur in the south and south east, and the highly agriculturally commercial turmeric Erode District in the East. This highly progressive, entrepreneurial and commercial district of Tamil Nadu lies between 10, " - 10' and 11," -30' Northern latitude and 76,"-40’ and 77,"-30’ Eastern longitude. The district has a geographical area of 7469 sq.kms. With the formation of Tiruppur district in 2008, the geographical area of Coimbatore shrank to 4,849.89 sq.kms. The district is divided into three revenue divisions, 9 taluks, 19 blocks and 482 revenue villages.

According to 2011 Census, Coimbatore had a population of 3,458,045 with a sex-ratio of 100 females for every 1,000 males, much above the national average of 929. A total of 319,332 were under the age of six, constituting 163,230 males and 156,102 females. The average literacy of the city was 76.23 percent, compared to the national average of 72.99 percent. There were a total of 1,567,950 workers, comprising 75,411 cultivators, 201,351 main agricultural labourers, 44,582 in household industries, 1,121,908 other workers, 124,698 marginal workers, 4,806 marginal cultivators, 28,675 marginal agricultural labourers, 5,503 marginal workers in household industries and 85,714 other marginal workers. Located in the rain shadow region of Western Ghats,

Coimbatore enjoys pleasant weather throughout the year. The rich red loam soil and red sandy soil in the district are favorable for production of cotton and a wide variety of cereals and food grains, spices, and condiments. The region has a total cultivable area of 3,30,584 hectares. Forest coverage spans across 158,801 hectares and is primarily suitable for timber, mango, walnut, and silk cotton.

Coimbatore district is an educational hub of Tamil Nadu, with a large base of educational institutes. From 2011 Census, the literacy ratio among males and females was about 86.77 percent and 73.44 percent respectively. The district comprises of a number of universities and schools including five universities, more than 1,400 primary schools, 420 middle schools and 165 higher secondary schools. Coimbatore is well connected with other cities and states through a vast road network across 322 kms of National Highways and 4,058 kms of State Highways. The three National Highways, NH-47 (Kanyakumari–Salem), NH-67 (Coimbatore– Nagappattinam), and NH-209 (Bangalore–Dindigul) pass through the city. The district has 20 railway stations with Podanur and Coimbatore North being the two prominent junctions. The rail network comprises both broad gauge and meter gauge with total route length of 211.7 kms and track length of 327.62 kms. Coimbatore also has an International Airport at Peelamedu, which handles domestic and International passengers and various types of cargo. The nearest major port is located in Cochin.

Coimbatore is amongst the fastest growing tier-II cities in India and a major hub for textiles, industries, commerce, education, information technology, healthcare and manufacturing in Tamil Nadu. Coimbatore houses more than 25,000 small, medium and large industries with the city's primary industries being engineering and textiles. Coimbatore is called the "Manchester of South India" due to its extensive textile industry, fed by the surrounding cotton fields. TIDEL Park Coimbatore in ELCOT SEZ was the first special economic zone (SEZ) set up in 2006. In 2010, Coimbatore ranked 15th in the list of most competitive (by business environment) Indian cities. Coimbatore also has a 160,000 square feet (15,000 m2) trade fair ground, built in 1999 and is owned by CODISSIA. It is also the country's largest pillar-free hall, according to the Limca Book of Records.

Coimbatore region experienced a textile boom in the 1920s and 1930s. Though, Robert Stanes had established Coimbatore's first textile mills as early as the late 19th century, it was during this period that Coimbatore emerged as a prominent industrial centre. Coimbatore is home to more than 17percent of the fibre textile mills in India. Coimbatore has trade associations such as CODISSIA, COINDIA and COJEWEL representing the industries in the city. Coimbatore houses a number of textile mills and is the base of textile research institutes like the Sardar Vallabhbhai Patel International School of Textiles & Management, Central Institute for Cotton Research (CICR) and the South India Textile Research Institute (SITRA). Kovai Cora Cotton saree is a recognised Geographical Indication.

Coimbatore is the second largest producer of software in the state, next only to capital Chennai. TIDEL Park Coimbatore and other Information technology parks in the city has aided in the growth of IT and Business process outsourcing industries in the city. It is ranked at 17th among the top global outsourcing cities by Tholons. The City has major software companies like Amazon, Bosch, Cognizant, Dell, Ford, TCS, Wipro, HCL, Hexaware, Deloitte, Cameron International, UST Global. Coimbatore is the second largest hub in India for Cognizant Technology Solutions employing more than 10,000 people. Coimbatore has largest R&D development centre of Bosch outside Germany employing more than 6,000 people. Coimbatore is one of the top 10 cities in India which has large number of Start-ups. Software exports stood at ₹.7.1 billion (US$110 million) for the financial year 2009–10 up 90percent from the previous year. Coimbatore has a large and diversified manufacturing sector, research institutes and a number of engineering colleges producing about 50,000 engineers annually.

Coimbatore is a major centre for the manufacture of automotive components in India with car manufacturers Maruti Udyog and Tata Motors sourcing up to 30percent, of their automotive components from the city. G.D. Naidu developed India's first indigenous motor in 1937. India's first indigenously developed diesel engine for cars was manufactured in the city in 1972. The city is also a major centre for small auto component makers catering to the automobile industry, from personal to commercial and farm vehicles. The city contributes to about 75percent of the 1 lakh total monthly output of wet

grinders in India. The industry employs 70,000 people and had a yearly turnover of ₹.2,800 Crore (US$430 million) in 2015. The term "Coimbatore Wet Grinder" has been given a Geographical indication.

Coimbatore is also referred to as "the Pump City" as it supplies nearly 50percent of India's requirements of motors and pumps. The city is one of the largest exporters of jewellery renowned for diamond cutting, cast and machine made jewellery. There are about 3,000 jewellery manufacturers employing over 40,000 goldsmiths.

Coimbatore has a large number of poultry farms and is a major producer of chicken eggs. The city contributes to nearly 95percent of processed chicken meat exports. Coimbatore has some of the country's oldest flour mills and these mills which cater to all the southern states, have a combined grinding capacity of more than 50,000 MT per month. The hospitality industry has seen a growth in the 21st century with new upscale hotels being set up like Vivanta by Taj, Le Meridien, The Residency Hotels, Aloft, Radisson, Marriott, ITC, etc. Coimbatore is the largest non-metro city for e-commerce in South India.

Coimbatore was ranked the best emerging city in India by India Today in the 2014 annual Indian city survey. The city was ranked fourth among Indian cities in investment climate by Confederation of Indian Industry and 17thamong the top global outsourcing cities by Tholons. Coimbatore has been selected as one of the hundred Indian cities to be developed as a smart city under Prime Minister Narendra Modi's flagship Smart Cities Mission. Coimbatore was rated as the safest city in India for women according to National Crime Records Bureau report in 2015.

As of 2015, India had 319 million Internet and 213 million mobile Internet users. Reported security breaches raise major concerns about privacy and security of confidential data over the web. As India continues to increase its leadership in information technology (IT) in the world, Indian citizens, political organizations, public sector, and government websites have been systematically targeted for cyber-attacks and cyber security incidents. These incidents are increasing. In 2014, Tamil Nadu registered 146 cyber-crime issues, with Chennai reporting 34. Kochi is the cybercrime capital of the state of Kerala. In 2014, police received over 6,117 complaints under the Information

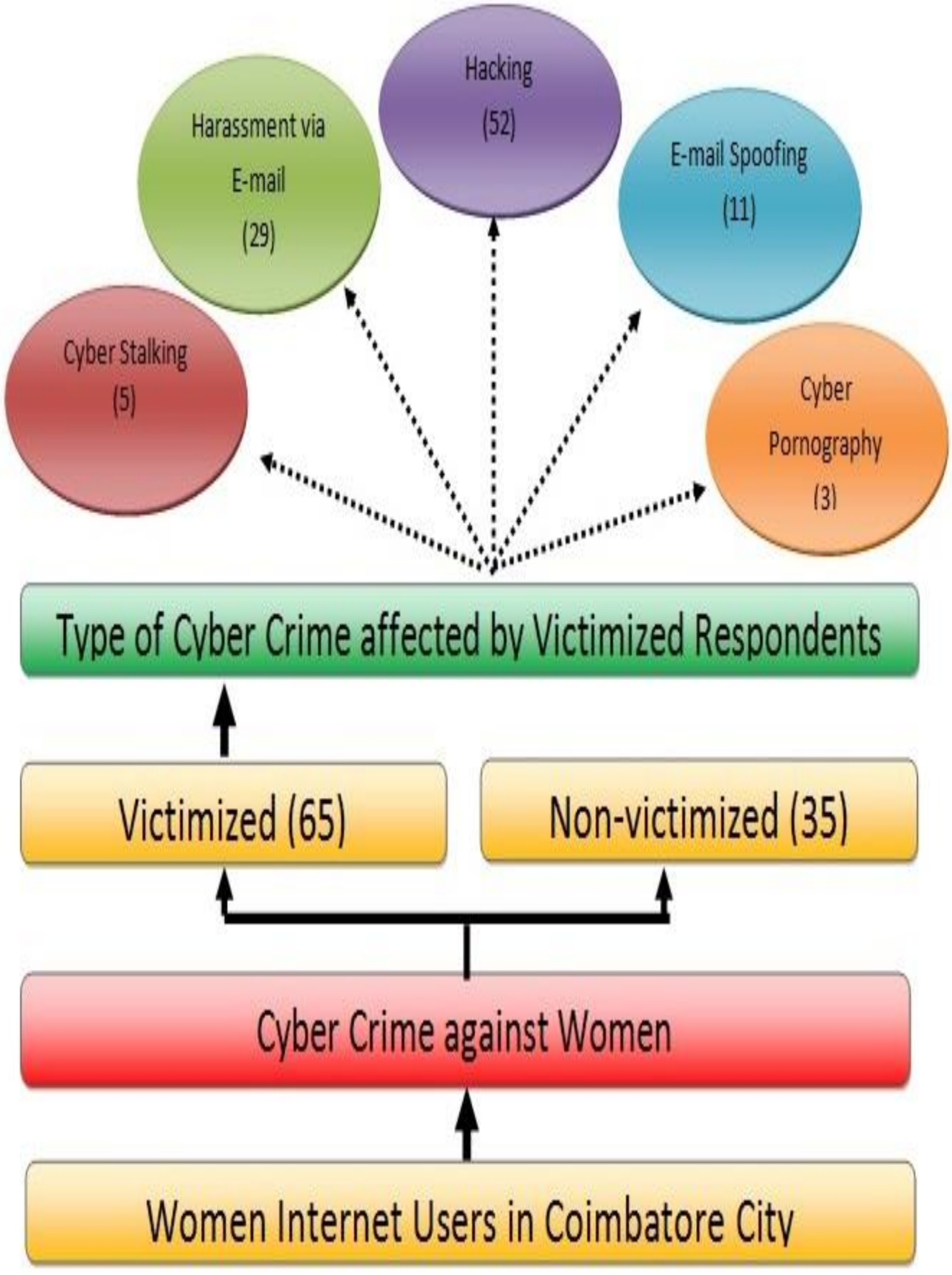
Technology (IT) Act, including; email abuse, threatening emails, email/computer hacking, mobile phone theft, online scams, abuse of social networking sites, abusive language via phone, and stolen personal information via phone.

Coimbatore City recorded less number of grave and violent offences during 2012 but crimes against women, besides rape and dowry deaths, were more when compared to Madurai and Tiruchirapalli City Police Commissionerates. The highest number of IPC cases were reported in Chennai City (19,881) followed by Coimbatore City (10,357), Madurai City (3,261), and Trichy City (2,926). The Salem city average crime rate per 100,000 in the Commissionerates for 2012 was 267.26 compared to 267.37 in 2011. The crime rate was the highest in Coimbatore City (474.47) followed by Trichy City (282.26), Tirunelveli City (267.05), Salem City (249.74), Chennai City (224.29) and Madurai City (219.78).In this context, a micro level study assumes immense connotation to evaluate the crimes against women in cyber space in Coimbatore city.

II. SELECTION OF THE SAMPLES

The population of the study consisted of Women Internet Users in Coimbatore City. From these selected areas 100 samples were selected by adopting incidental purposive sampling technique. The term incidental sampling is applied to those samples that are taken because they are most readily available. The basic assumption behind purposive sampling is that with good judgment and an appropriate strategy one can handpick the cases to be included in the sample and thus develop samples that are satisfactory in relation to one's needs (Guilford, 1978). A common strategy of purposive sampling is to pick up cases that are judged to be typical of the population, in which one is interested, assuming that errors of judgment in selection will tend to counter balance each other if sufficiently large sample is taken. Questionnaire was administered to Women Internet users within the city. Women Internet Users was asked to complete the questionnaire. A total of 100 Women Internet Users were contacted. Hence, the investigator approached only those peoples were willing to cooperate and supply the needed information.

FIGURE 3.1
SAMPLE DESIGN



III. DATA BASE OF THE STUDY

Relevant and required data for the present study were collected from the primary source by administering an interview schedule to the selected Women Internet users. The interview schedule was first pre-tested to check for clarity and specificity and the necessary modifications were made on the basis of the experience gained during pre-testing. The finalized schedule used in the study is given in Annexure.

IV. PERIOD OF THE STUDY

The field investigation and data collection for the study was carried out during the period December-March (2017).

V. TECHNIQUES OF ANALYSIS

Data collected were tabulated and analysed for giving precise and concise information. Besides, percentages and graphs, the following statistical tools were used.

Garrett's Rating Scale

To determine the major location of online abuse, the respondents were asked to rank the various Sources. The ranks were converted into percent by using the following formula:

$$\text{Percent Position} = \frac{100\ (R_j - 0.5)}{N}$$

Where R_j is the rank given by the j^{th} respondents for the major location of online abuse and N is the number of item ranked. Based on the percent position, individual score was determined, on a scale of 100 by using Garratt' scoring table. (Garrett, 2005).

Chi-Square Test

The χ^2 test is one of the simplest and most widely used non-parametric test in statistics. The quantity χ^2 describes the magnitude of the discrepancy between theory and observation and is symbolized as:

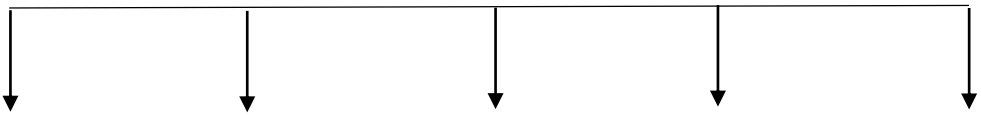
$$\chi^2 = \Sigma \frac{(O-E)^2}{E}$$

where O refers to observed frequency and E refers to expected frequency.

In the present study, Chi-square test was applied to find the association between the Victimized and Non-victimized respondents of Cyber Crime and Major harassments in Online with factors like verbally abused, physically threatened, intentionally tried to embarrass another, stalked and sexually harassed.

Likert's Summated Scale

The Likert's Summated Scale was used to scale the Reasons for Using the Internet, Harassments in Online, Problems faced by women's in Cyber Crime, Awareness of Cyber Culture among women Internet Users and Suggestions for Cyber Crimes. In the Likert scale, the respondent was asked to respond to each of the statements in terms of five degrees of agreement or adjustment.



Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(5)	(4)	(3)	(2)	(1)

Each point on the scale carries a score. Response indicating the lowest favourable degree of satisfaction is given the least score (say 1) and the most favourable is given the highest score (say 5). This way the instrument yields a total score for the respondents which would then measure the respondents' favourableness or otherwise towards the given point of view.

Cronbach's Alpha

Cronbach's alpha evaluates the uni dimensionality of a set of scale items. It's a measure of the extent to which all the variables in a scale are positively related to each other. In fact, it is really just an adjustment to the average correlation between every variable and every other. The formula for alpha is

$$\alpha_{standardized} = \frac{K.\bar{r}}{(1+(K-1).\bar{r})}$$

where k is the number of variables and $\bar{r}$ is the average correlation among all pairs of variables. Cronbach's alpha values ranges from 0 to 1. The higher the score, the more reliable the generated scale is. Nunnally (1978) has indicated 0.7 to be an acceptable reliability coefficient but lower thresholds are sometimes used in the literature. In the study, the reliability testing was done for reasons for Using Internet, problems faced by Women in Cyber Culture and Suggestions for Cyber Crimes in India.

Factor Analysis

Factor analysis is a multivariate statistical analysis whose objective is to define the underlying structure in the data matrix. Broadly speaking, it addressed the problem of analysing the structure of interrelationship (correlation) among a large number of dimension and the explanation of each variable are determined, so that the two primary uses for factor analysis, namely summarization and data reduction can be achieved. In summarizing the data, factor analysis derives underlying dimensions that, when interpreted and understood, describe the data in a much small number of concepts than the original individual variables.

Factor analysis was used in the present study to identify the underlying pattern of relationship between the various dimensions of reasons for using Internet, Harassments in Online, problems faced by Women in Cyber Culture, Awareness of Cyber culture among women Internet Users and some statements on Cyber Crimes and whether these factors can be grouped in terms of a composite variable.

ANOVA

The ANOVA test is used to determine the impact of independent variables on the dependent variables. The one-way analysis of variance is used to determine whether there is any significant difference between the means of one or more independent groups on dependent variable.

One independent variable experiment is called one-way ANOVA, it stands for Analysis of Variance, the generic name given to a set of techniques for studying the cause and effect of one or more factors on a single dependent variable. In the present study

ANOVA is used to determine whether the Problems on faced by Women in Cyber Space differed across Victimized and Non-victimized respondents by Cyber Crime and the awareness on Cyber culture among Indian Internet Users differed across Victimized and Non-victimized respondents of Cyber Crime.

LIMITATIONS OF THE STUDY

- The study seeks to provide a helicopter view of the field reality and hence inference drawn do not provide conclusive evidence to any social characteristics in particular albeit they aid us in spotting an underlying trend.
- The present study relies only on the information's gathered through surveys, and personal interviews, which are subject to bias.
- The findings are based entirely upon the research conducted in Coimbatore and hence may not be applicable directly to other metropolitan cities of socio-cultural diversity and contextual factors.
- Due to constraints of time, certain topics have not been touched upon at all during the course of the study while some of them like the actual purchase pattern have been explored in a 'limited' manner. An in-depth analysis may be further taken up in each of sub-topics covered.
- Moreover the survey is not representative of the whole Coimbatore. The sample was collected only from in and around the city. Therefore, caution needs to be taken when generalizing these research results to user groups in other geographical areas and environment.

  These limitations are no way negates the findings of the study and offer scope for further research in future.

CHAPTER IV

RESULTS AND DISCUSSION

The major findings of the study are presented and discussed under the following heads:

I. Socio-Economic Profile of the Selected Respondents.
II. Place of Internet Usage
III. Details on Internet Usage.
IV. Reasons for Using Internet.
V. Details on Cyber Crime Victimization.
VI. Harassments in Online.
VII. Location of Online Abuse.
VIII. Awareness on Cyber Culture among Indian Internet Users.
IX. Problems faced by Women's in Cyber Crime
X. Suggestions for Cyber Crimes.

I. SOCIO-ECONOMIC PROFILE OF THE SELECTED RESPONDENTS

In the traditional and structured society, socio-economic factors play a significant role in shaping the personality and characteristics of an individual. Hence, to develop a proper perspective analysis, all the components of social and economic environment must be considered. The general notion is that, the social environment is a combination of factors such as Age, Marital Status and Number of Members in the Family, while economic environment is made up of factors such as Education, Occupation and Income. A total of 100 Women Internet users were surveyed, of which 65 were Victimized by Cyber Crime and 35 were Non-Victimized by Cyber Crime. The socio-economic characteristics of the respondents were presented in the table 4.1

TABLE 4.1
SOCIO-ECONOMIC PROFILE OF THE RESPONDENTS

Socio-Economic Status	Characteristics	Victimized	Non-Victimized	Total
Age	15-20 Years	3 (4.6)	2 (5.7)	5 (5.0)
	20-30 Years	33 (50.8)	16 (45.7)	49 (49.0)
	30-40 Years	28 (43.1)	14 (40.0)	42 42.0)
	40-50 Years	1 (1.5)	3 (8.6)	4 (4.0)
Marital Status	Married	27 (41.5)	9 (25.7)	36 (36.0)
	Unmarried	29 (44.6)	23 (65.7)	52 (52.0)
	Separated	7 (10.8)	1 (2.9)	8 (8.0)
	Widow	2 (3.1)	2 (5.7)	4 (4.0)
Family Members	2 Members in a Family	10 (15.4)	7 (20.0)	17 (17.0)
	3 Members in a Family	29 (44.6)	14 (40.0)	43 (43.0)
	4 Members in a Family	25 (38.5)	13 (37.1)	38 (38.0)
	5 Members in a Family	1 (1.5)	1 (2.9)	2 (2.0)
Education	Secondary Level	4 (6.2)	2 (5.7)	6 (6.0)
	Diploma Level	17 (26.2)	7 (20.0)	24 (24.0)
	UG	18 (27.7)	19 (54.3)	37 (37.0)
	PG	24 (36.9)	7 (20.0)	31 (31.3)
	Professionals	2 (3.1)	0 (0.0)	2 (2.0)
Occupation	Student	34 (52.3)	13 (37.1)	47 (47.0)
	Private Employees	27 (41.5)	17 (48.6)	44 (44.0)
	Government Employees	4 (6.2)	5 (14.3)	9 (9.0)

Income	Zero income	34 (52.3)	13 (37.1)	47 (47.0)
	Below ₹.10000	2 (3.1)	3 (8.6)	5 (5.0)
	₹.10001- ₹.20000	14 (21.5)	13 (37.1)	27 (27.0)
	₹. 20001- ₹.30000	10 (15.4)	5 (14.3)	15 (15.0)
	₹.30001- ₹.40000	4 (6.20	1 (2.9)	5 (5.0)
	Above ₹.40000	1 (1.5)	0 (0.0)	1 (1.0)

Source: Field Survey

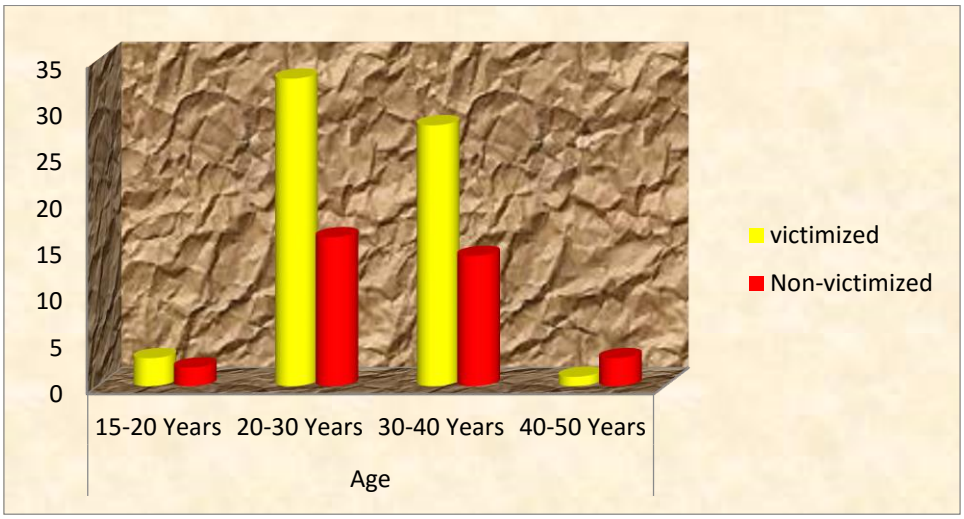
Figures within parentheses indicate percentage

Age

Table 4.1 presents the age-wise distribution of the respondents. Nearly 49 percent of the Women Internet users were in the age group of 20 to 30 years, 42 percent between 30 to 40 years, 5 percent between 15 to 20 years and 4 percent between 40 to 50 years. Among the Victimized Women Internet users, majority of the respondents 51 percent were in the age group of 20 to 30 years, 43 percent were between 30 to 40 years, 5 percent between 15 to 20 years and 2 percent between 40 to 50 years. Among the Non-Victimized Women Internet users, majority of the respondents 46 percent were in the age group of 20 to 30 years, 40 percent were between 30 to 40 years, 6 percent between 15 to 20 years and 9 percent between 40 to 50 years. The study found that, the majority of the respondents were belonged to 20 to 30 years categorized as Young adults using Internet facilities for their day to day purpose.

FIGURE 4.1

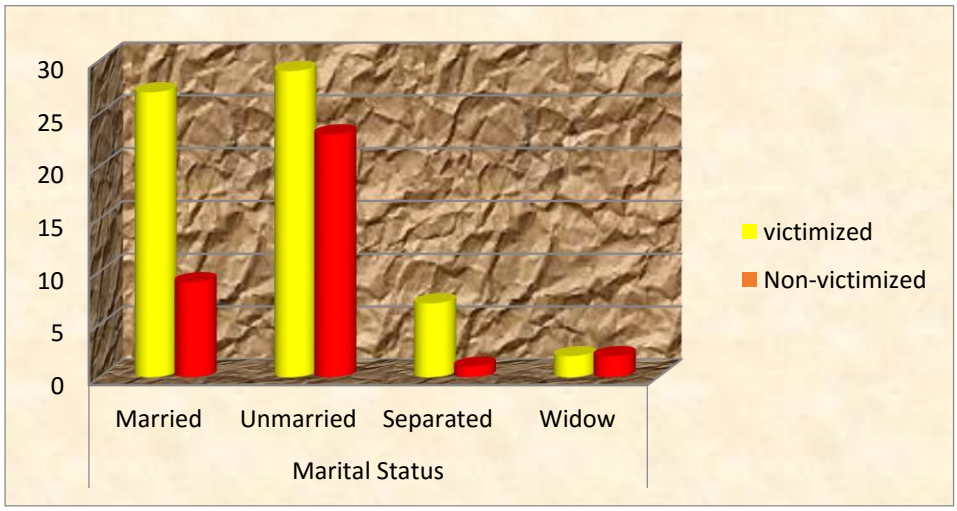
AGE OF THE RESPONDENTS



Source: Estimation based on Field Survey

FIGURE 4.2

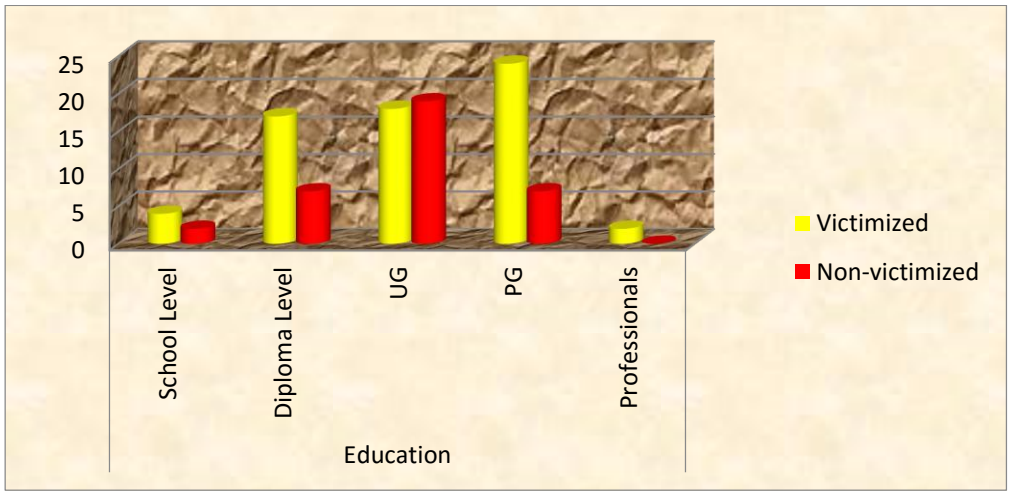
MARITAL STATUS OF THE RESPONDENTS



Source: Estimation based on Field Survey

FIGURE 4.3

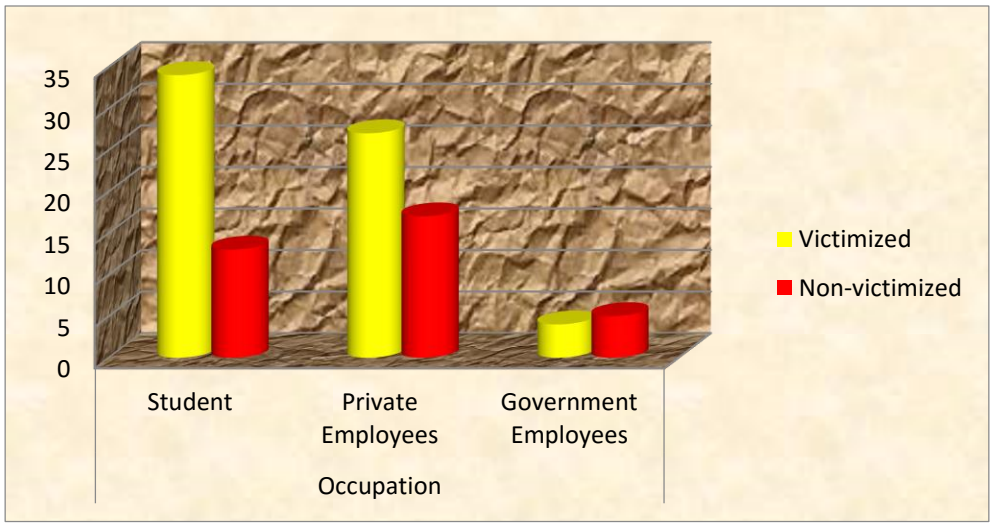
EDUCATIONAL STATUS OF THE RESPONDENYS



Source: Estimation based on Field Survey

FIGURE 4.4

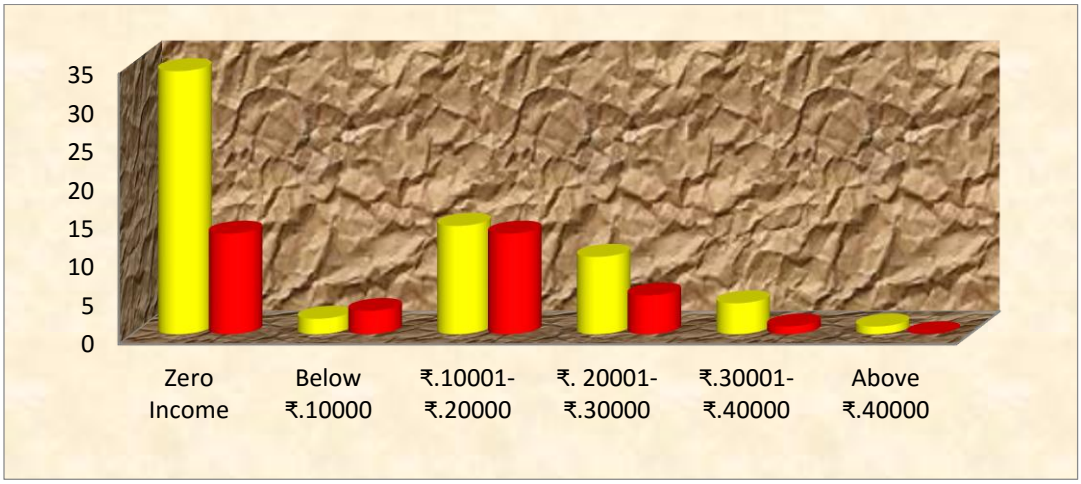
OCCUPATIONAL STRUCTURE OF THE RESPONDENTS



Source: Estimation based on Field Survey

FIGURE 4.5

INCOME STATUS OF THE RESPONDENTS



Source: Estimation based on Field Survey

Marital Status

Marital status of the individuals is quite important in any socio-economic study. There is a change in the life style of the individual after marriage, which is more pronounced in the case of women. Even the usage of internet by women to some extent has been due to the initiative of their husband. In the present study, majority of them were married in both among the victimized respondents of cyber crime (42 percent) and non-victimized respondents of cyber crime (28 percent). The next important category comprised to unmarried persons of victimized respondents and non-victimized respondents were 45 percent and 66 percent respectively. The usage of victimized respondents of cyber crime who were either divorced or widowed were less than 11 percent. The present study found that, majority of the Women Internet users were Unmarried Women.

Size of the Family

Size of the family of the Women Internet users were found from the survey that majority (43 percent) of the respondents had three members in their family, 38 percent had four members in their family, 17 percent had two members in their family and 2 percent had five members in their family. Hence, the present study found that majority of them had small size of the family.

Education

Internet users are generally dominated by the educated people. Among the Victimized Women Internet users 37 percent were Post Graduates, followed by 28 percent of the respondents were completed Graduation, 26 percent were completed Diploma level Education, 6 percent were completed Secondary level education and 3 percent were professionals. Among the Non-Victimized respondents users 54 percent were graduates, followed by 20 percent of the respondents were completed post graduates, 20 percent were completed Diploma level education, 6 percent were completed Secondary level Education and there were no professionals respondents in Non-victimized category of Cyber Crime. The study revealed that, Majority of the Victimized respondents were educated who were affected by Cyber Crime.

Occupation

Occupation or Employment is central in determining the well being of the individual or households. Being time savvy, Internet is becoming very popular among Businessmen, Professionals and Students. The occupation of the respondents included Private Employees and Government Employees. Among the Victimized Women, Majority (52 percent) were Students, followed by Private Employees (42 percent) and Government Employees (6 percent). Among the Non-Victimized Women, Majority (49 percent) were Private Employees, followed by Students (37 percent) and Government Employees (14 percent). The study found that, majority of the respondents were belongs to Students and Private Employees who were Victimized.

Monthly Income

The existence of inter-personal variations in income among a large size of sample is well organized. From the table, both Victimized and Non-victimized 27 percent of the respondents were earned income between ₹.10,001 to ₹.20,000 followed by 15 percent were earned between ₹.20,001 to ₹.30,000; each 5 percent earned income between ₹.30,001 to ₹.40,000 and below ₹.10,000 respectively. The majority of the respondents (47 percent) were belonged to Student Category, they won't earn income, but they dependent on their parents income. Hence, the study revealed that majority of the Victimized belonged to no income category (i.e.) Students.

Place of Internet Usage by respondents

Below table and figure shows that, the Place where Internet used by the respondents. The places of Internet usage were classified as at Home, at Office, at Cyber Cafe, at Public Place and Other Places.

TABLE 4.2

PLACE OF INTERNET USAGE

S.No	Usage	At Home	At Office	At Cyber Cafe	At Public Place	Others Place
1	Daily	59	47	4	27	4
2	Weekly	27	41	29	32	65
3	Monthly	5	4	8	5	2
4	Sometimes	9	8	59	36	29
Total		**100**	**100**	**100**	**100**	**100**

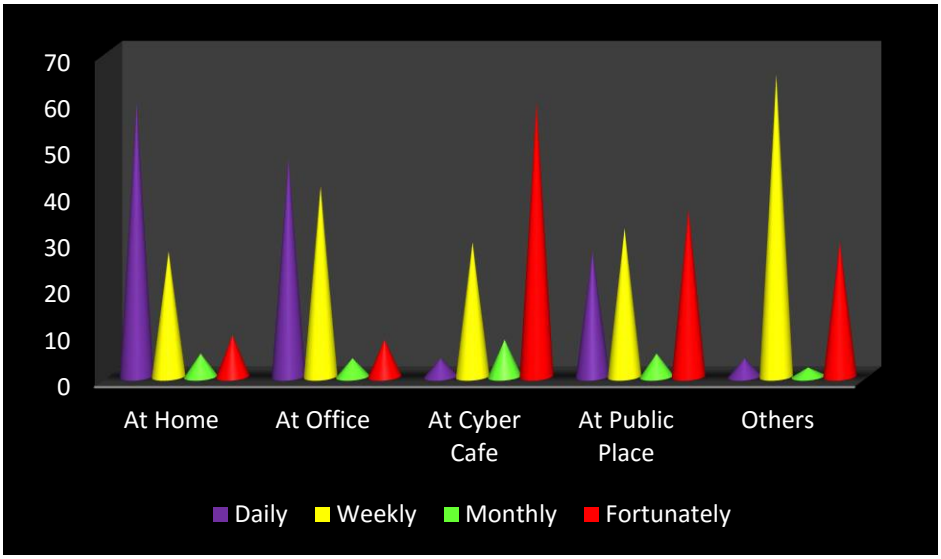
Source: Estimation based on Field Survey

Above table and figure shows the Place where Internet used by the respondents. At Home 59 percent of the respondents were used Internet Daily; 27 percent of them were using Weekly; 9 percent of them using sometimes and the remaining 5 percent of the respondents were using Monthly. At Office 47 percent of them were using Daily; 41 percent of them were using Weekly; 8 percent of them were using Sometimes and the remaining 4 percent of them were using Monthly. At Cyber Cafe, 59 percent of them were using Sometimes followed by 29 percent of them were using Weekly, followed by 8 percent and 4 percent them were using by Monthly and Daily. At Public Place, 36 percent of them were using Sometimes; 32 percent of them were using Weekly; 27 percent of them were using Daily and 5 percent of them were using Monthly. At Other Place 65 percent of them were using Weekly; 29 percent of them were using Sometimes and 4 percent and 2 percent of them were using Internet Daily and Weekly respectively. The study found that, majority of the sample respondents used Internet daily at Home, Weekly

at Office and Sometimes at Cyber Cafe. Use of Internet by the sample respondents at Public places and other places were only at less proportion.

FIGURE 4.6

PLACE OF INTERNET USAGE



Source: Estimation based on Field Survey

Other Internet Users at Home

Below table and figure shows that the Internet users at Home other than the respondents.

TABLE 4.3

OTHER INTERNET USERS AT HOME

S.No	Internet Users at Home	Percentage of the respondents
1	Father	6
2	Mother	8
3	Brother	45
4	Sister	28
5	Grand Parents	2

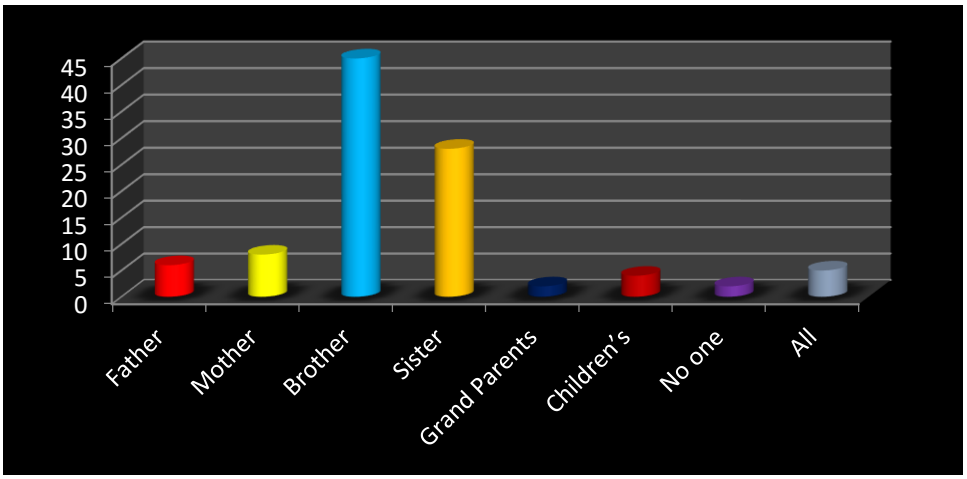
6	Children's	4
7	No one	2
8	Everyone at home	5
	Total	**100**

Source: Estimation based on Field Survey

From the table, it is clear that, majority of the persons who were using Internet were Brothers and Sisters (45 percent and 28 percent) other than the respondents; followed by Father and Mother (6 percent and 8 percent); 4 percent of the users were Children; 2 percent were Grand Parents; Everyone in the family using Internet at home other than the sample respondents were 5 percent and the remaining 2 percent won't use Internet at all. The study found that, majority of the Internet users at home were Siblings other than the sample respondents.

FIGURE 4.7

OTHER INTERNET USERS AT HOME



Source: Estimation based on Field Survey

Usage of Mail Account

Having of Mail account is common among Internet users, below table shows that the usage of Mail Account by the sample respondents.

TABLE 4.4

USAGE OF MAIL ACCOUNT

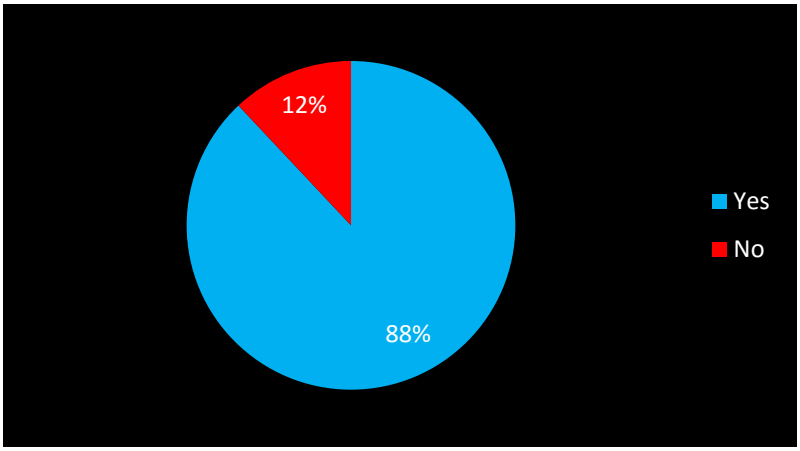
S.No	Usage of Mail Account	Percentage of the respondents
1	Yes	88
2	No	12
	Total	**100**

Source: Estimation based on Field Survey

The above table and figure shows that the usage of mail account by the respondents, the majority of them were using mail account (88 percent) frequently and the remaining 12 percent were not used the mail account frequently. The study found that, majority of the sample respondents were using mail account.

FIGURE 4.8

USAGE OF MAIL ACCOUNT



Source: Estimation based on Field Survey

Privacy locks for Social Media

The use of privacy locks for social media is very important among Internet users to avoid many crimes and to protect personal Information's. Below table shows that privacy locks for Social Media used by sample respondents

TABLE 4.5

PRIVACY LOCKS FOR SOCIAL MEDIA

S.No	Privacy Locks	Percentage of the respondents
1	Yes	62
2	No	38
Total		**100**

Source: Estimation based on Field Survey

The above table shows the privacy locks for their Social Media used by sample respondents, majority (62 percent) of them were using the privacy locks and the remaining 38 percent of them were not using privacy locks for their accounts. The study found that majority of them were felt that Privacy locks must to keep their account safely and avoid crime against them.

Frequently used Social Network

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Below table shows that the frequently used Social Network by the sample respondents

TABLE 4.6

FREQUENTLY USED SOCIAL NETWORK:

S.No	Using Social Network	Percentage of the respondents
1	Orkut	9
2	Face Book	36

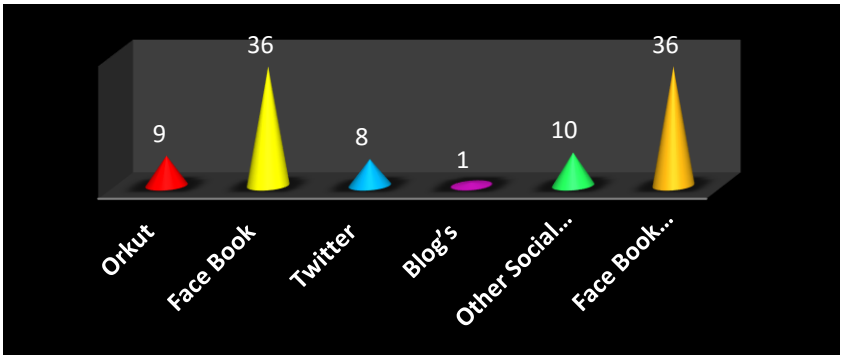
3	Twitter	8
4	Blog's	1
5	Other Social Networks	10
6	Face Book and Other Social Network	36
	Total	**100**

Source: Estimation based on Field Survey

From above table and figure, majority (36 percent) of the sample respondents were using Face Book and Other Social Network and only Face Book; followed by each 10 percent were using other Social network sites and Orkut respectively; followed by 8 percent Twitter and the remaining 1 percent of them were using Blog's. The study found that, majority of the respondents were using Face Book and Other Social Network for their Communication.

FIGURE 4.9

FREQUENTLY USED SOCIAL NETWORKS



Source: Estimation based on Field Survey

Downloading from Internet

A download manager is a computer program dedicated to the task of downloading (and sometimes uploading) possibly unrelated stand-alone files from (and sometimes to) the Internet for storage. Some download managers can also be used to accelerate download speeds by downloading from multiple sources at once.

TABLE 4.7

DOWNLOADING FROM INTERNET

S.No	Downloading from Internet	Percentage of the respondents
1	Movies	1
2	Songs	1
3	Applications	2
4	Study Materials	1
5	Media (Movies and Songs)	8
6	Movies, Songs and Study Materials	2
7	Movies, Songs, Applications, Study Materials and Government Documents	18
8	Movies, Songs, Applications, Study Materials and Software's	42
9	Movies, Songs, Applications, Study Materials, Software's and Government Documents	25
	Total	**100**

Source: Estimation based on Field Survey

The above table shows the major downloads from internet by the respondents. From the table it's clear that the majority were download Movies, Songs, Applications, Study Materials and Software's by 42 percent; followed by Movies, Songs, Applications, Study Materials, Government Documents and Software's by 25 percent; followed by Movies, Songs, Applications, Study Materials and Government Documents by 18 percent; followed by Movies and Songs by 8 percent, Movies, Songs and Study Materials by 2 percent; followed by only Applications by 2 percent, Study Materials, Movies and Songs by each 1 percent, respectively. The study found that majority of the respondents were used internet for downloading Movies, Study Materials and Software's.

Frequently used Internet Browser

An Internet Browser, also known as a web browser or simply a browser, is a software program that you use to access the Internet and view web pages on your computer. The main purpose of an Internet Browser is to translate, or render, the code that websites are designed in into the text, graphics and other features of the web pages that we are all used to seeing today.

TABLE 4.8

FREQUENTLY USED INTERNET BROWSER

S.No	Mostly used Internet Browser	Percentage of the respondents
1	Internet Explorer	8
2	Google Chrome	28
3	Mozilla Firefox	4
4	Opera Mini	1
5	Internet Explorer, Google Chrome and Mozilla Firefox	16
6	Internet Explorer and Google Chrome	8
7	Every Browser	35
	Total	**100**

Source: Estimation based on Field Survey

The above table shows frequently used Internet Browser by the respondents, Majority (35 percent) of the respondents were used Internet Explorer, Google Chrome, Mozilla Firefox and Opera Mini; followed by Google Chrome 28 percent; followed by Internet Explorer, Google Chrome and Mozilla Firefox 16 percent; followed by Internet Explorer and Google Chrome and Internet Explorer 8 percent each; Mozilla Firefox by 4 percent and Opera Mini by 1 percent. The study found that Majority of the respondents used every Browser frequently for their browsing.

Changing Password

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website. Passwords can vary in length and can contain letters, numbers and special characters. Other terms that can be used interchangeably are passphrase for when the password uses more than one word, and pass code and passkey for when the password uses only numbers instead of a mix of characters, such as a personal identification number. For security purpose changing password is must for the users whenever they feel insecurity. The below table shows the interval of changing their passwords.

TABLE 4.9

CHANGING PASSWORDS

S.No	Changing Password	% of the respondents
1	Daily	1
2	Weekly	11
3	Monthly	48
4	Sometimes	40
	Total	**100**

Source: Estimation based on Field Survey

In the table, Majority (48 percent) of the respondents were changing their passwords monthly; 40 percent of them were changing Sometimes; 11 percent of them were changing Weekly and the remaining 1 percent of them were changing Daily. The study found that, majority of the sample respondents changes their passwords monthly due to their insecurity feel while using Mail.

Awareness to Internet

Aware means having knowledge about things, awareness is very essential to users of internet, as soon as ICT has developed the thinking and searching of things have been increasing (Adithya Kumari H, et.al., 2013). How, the respondents got awareness to use Internet were shown in below table 4.10

TABLE 4.10

AWARENESS TO INTERNET

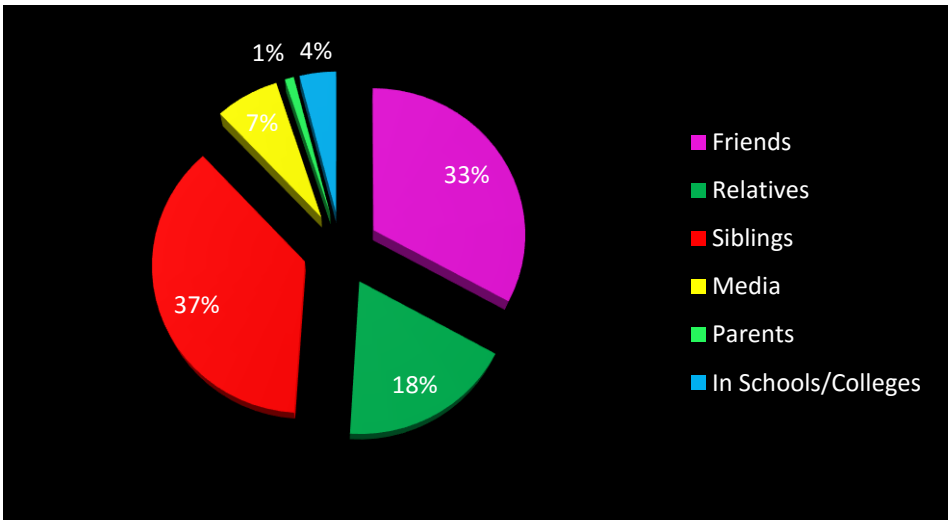
S.No	Awareness to Internet	Percentage of the respondents
1	Friends	33
2	Relatives	18
3	Siblings	37
4	Media	7
5	Parents	1
6	In Schools/Colleges	4
	Total	**100**

Source: Estimation based on Field Survey

In the table, majority (37 percent) of them got awareness of Internet through Siblings; 33 percent of them known through Friends; 18 percent of them known through Relatives; 7 percent of them known through Media; 4 percent of them known from Schools/Colleges and the remaining 1 percent of them known through their Parents. The study revealed that, majority of the respondents got awareness through their Siblings. The figure 4.10 shows the awareness of Internet.

FIGURE 4.10

AWARENESS TO INTERNET



Source: Estimation based on Field Survey

Factor Analysis

There are many things to like about Internet: the convenience, the functionality, even the fashion component. An attempt was made to gauge attitude of the respondents on the reasons for using Internet and the respondents were asked to rate the statement on a five point scale, with maximum point five given most favourable statement and a minimum of one given to least favourable statement. Factor analysis was used to identify the underlying dimensions among the factors on reasons for using Internet. To determine the reliability of applying factor analysis the Cronbach's alpha test was applied and was estimated to be 0.835, which was greater than 0.7 indicating the reliability of the constructs. To determine the appropriateness of applying factor analysis the KMO and Bartlett's test measures were computed and the results are presented in table.4.11.

TABLE 4.11

KMO AND BARTLETT'S TEST MEASURES

Kaiser-Meyer-Olkin Measures of Sampling	.720
Bartlett's test of Sphericity approx: chi-square	980.875
Degrees of freedom	66

Significance	.000

Source: Estimation based on Field survey

The KMO statistics for all respondents was 0.720, signifying higher than acceptable adequacy of sampling. The Bartlett's test of sphericity was also found to be significant at 1 percent level providing evidence of the presence of relationship between the variables to apply factor analysis.

The communalities for variable were computed to determine the amount of variance accounted by the variable to be included in the factor rotation and the results are shown in table.4.12.

TABLE 4.12

COMMUNALITIES

Reasons	Initial	Extraction
To use E-mail	1.000	.880
To use Face Book	1.000	.852
To View Photo	1.000	.742
To Read News	1.000	.897
To Search for Job related Information	1.000	.739
To Play Games	1.000	.857
To Listen or Download Music	1.000	.748
To Search for Study related Information	1.000	.931
To use Banking Facilities	1.000	.834
For Online Shopping	1.000	.757

To get day to day Information's	1.000	.894

Source: Estimation based on Field Survey

Extraction method: Principal Component Analysis

The table 4.13 enlists the Eigen values, their relative explanatory powers and the factor loadings for 11 components identified within the data set. The Eigen values greater than one alone was considered for inclusion in the analysis.

TABLE 4.13

ROTATED COMPONENT MATRIX

S.No	Reasons	Components			
		1	2	3	4
1	To use E-mail			.866	
2	To use Face Book	.888			
3	To View Photo	.832			
4	To use other Social Media Sites		.942		
5	To Read News		.702		
6	To Search for Job related Information		.924		
7	To Play Games				.857
8	To Listen or download Music			.869	
9	To Search for Study related Information	.870			
10	To use Banking Facilities	.829			
11	For Online Shopping	.940			
Eigen values		4.950	2.636	1.061	1.021

Percentage of variance	41.253	21.963	8.844	8.507
Cumulative percentage	41.253	8.844	72.059	80.566

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization,

Rotation converged in 6 iterations.

Source: Estimation based on Field Survey

The results indicates that for the sample data, Eigen value of the first four factors alone was greater than one for reasons for using internet and that these factors alone were appropriate for inclusion in the analysis. For reasons for using internet four factors together accounted for nearly 81 percent of the variations in the factors.

Reasons for using Internet, factor 1 has significant loadings for five dimensions namely “To use Face Book”, “To view Photo”, “To search for Study Materials”, “To use Banking Facilities” and “For Online Shopping”. These Five dimensions together explained nearly 41 percent of the variance. Factor 2 has significant loadings for three dimensions namely “To use other social media sites”, “To read news”, “To search for job related information’s” and explained nearly 22 percent of the variance. Factor 3 has significant loading for two dimensions namely “To use mail” and “To listen or download music” and explained nearly 9 percent of the variance. Factor 4 has significant loading for one dimension namely “To play games” and explained nearly 9 percent of the variance. To sum up, the major reasons sited by sample respondents for using Internet were to use social media sites, for online shopping, to search job related information’s, to search study related information’s, to use Face Book, etc.

Details on Cyber Crime

These days a worst fear in teenager’s eyes is Cyber Crime. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Crime as per inspection. It is becoming an alarming trend in our society. (Sumanjit Das and Tapaswini Nayak, 2013). Following table and figure shows that respondents victimized by Cyber Crime, types of Cyber crime and Perpetrator of Cyber Crime against Women in Coimbatore City.

TABLE 4.14

DETAILS ON CYBER CRIME VICTIMIZATION

S.No	Details on Cyber Crime	Victimized	Non-Victimized	Total
1	**Victimized by Cyber Crimes**			
	Yes	65(65.0)	0(0.0)	65(65.0)
	No	0(0.0)	35(35.0)	35(35.0)
2	**Types of Cyber Crimes**			
	Harassment via E-mail	19 (29.2)	0 (0.0)	19 (19.0)
	Cyber Stalking	3 (4.6)	0 (0.0)	3 (3.0)
	Cyber Pornography	2 (3.1)	0 (0.0)	2 (2.0)
	Hacking	34 (52.3)	0 (0.0)	34 (34.0)
	E-mail Spoofing	7 (10.8)	0 (0.0)	7 (7.0)
	Non-victimized	0 (0.0)	35 (100.0)	35 (35.0)
3	**Perpetrator**			
	Stranger	18(18.0)	0 (0.0)	18(18.0)
	Acquaintance	10(10.0)	0 (0.0)	10(10.0)
	Girlfriend	12(12.0)	0 (0.0)	12(12.0)
	Boyfriend	13(13.0)	0 (0.0)	13(13.0)
	Family Members	11(11.0)	0 (0.0)	11(11.0)
	Co-Workers	14(14.0)	0 (0.0)	14(14.0)

	Stranger, Girlfriend, Boyfriend, Family Members and Co-Workers	22(22.0)	35 (100.0)	22(22.0)

Source: Estimation based on Field Survey

Victimized and Non-Victimized

Data pertaining to the Victimized and Non-victimized respondents by Cyber Crime unravel that majority of them were victimized by Cyber Crime (65 percent) and the remaining 35 percent of them were Non-victimized by Cyber Crimes. The present study found that majority of the sample respondents were victimized by Cyber crime.

Types of Cyber Crimes

Data pertaining to the types of Cyber Crimes, most of the Victimized respondents were affected by the Hacking (34 percent); 19 percent of them were affected by Harassment via E-mails; 7 percent of them were affected by E-mail Spoofing; 2 percent of them were affected by Cyber Pornography and the remaining 35 percent of them were Non-victimized by. The study found that majority of them Victimized affected by Hacking.

Perpetrator of Cyber Crimes

In the table, Majority (22 percent) of the respondents were victimized by Strangers, Girlfriend, Boyfriend, Family Members and Co-workers; 18 percent of them were victimized by Strangers; 14 percent of them were victimized by Co-workers; 13 percent of them were victimized by Boyfriends; 12 percent of them were victimized by Girlfriends; 11 percent of them were victimized by Family Members and 10 percent of them were victimized by Acquaintance. The study found that there is no much difference in perpetrator of Cyber Crimes against Women and the major perpetrator of Cyber Crime were Strangers, Relatives and Co-workers.

HARASSMENTS IN ONLINE

Chi- Square Analysis

In order to investigate the relationship between Harassments in Online and Victimized and Non-victimized respondents of Cyber Crime, Pearson's Chi-square test was done. The null hypothesis framed was:

Inference

H_o: There is no significant association between Victimized and Non-victimized respondents by Cyber Crime and Harassments in Online.

H_a: There is significant difference between Victimized and Non-victimized respondents by Cyber Crime and Harassments in Online.

The calculated Chi-square value are shown in table

TABLE 4.15

ASSOCIATION BETWEEN VICTIMIZED AND NON-VICTIMIZED BY CYBER CRIME AND HARASSMENTS IN ONLINE

Variables	Chi-square Value	Degrees of freedom	Asymptotic Significance	Inference
Verbally abused	63.912	3	**.000**	**Reject H_o**
Physically Threatened	83.727	3	**.000**	**Reject H_o**
Intentionally tried to embarrass others	87.729	4	**.000**	**Reject H_o**
Stalked	60.045	3	**.000**	**Reject H_o**
Sexually Harassed	95.971	4	**.000**	**Reject H_o**

Source: Estimation based on Field Survey

The above table shows, the Pearson Chi-square value is 63.912, finding the association with the variables and Harassments in Online. The P value with respect to the Chi-Square value is 0.000 at the 0.01 level of significant which lies below the 0.05, and hence there is association between the Victimized and Non-victimized respondents by Cyber Crime and Verbally abused harassment in Online and following the Pearson Chi- Square values are like 83.727, 87.729, 60.045 and 95.971 have respective of Physically threatened, Intentionally tried to embarrass others, Stalked and Sexually harassed and Victimized and Non-victimized respondents by Cyber Crime with respect to the P values .000, .000, .000 and .000) are also lies below the 0.05, hence there is an

association between the Verbally abused, Physically threatened, Intentionally tried to embarrass other, Stalked and Sexually harassed.

LOCATION OF ONLINE ABUSE

Garrets' Rating scale

In the present study, the respondents were asked to rank the major Location of Online Abuse and ranks were converted into percent position by using the formula:

$$\text{Percent position} = \frac{100\ (R_j - 0.5)}{N}$$

where R_j is the rank of the i^{th} item and N refers to the number of items ranked. The percent position was converted into score by using Garrets' Rating scale and the average score obtained for differential reasons are tabulated and presented in table 4.16.

TABLE 4.16

LOCATION OF ONLINE ABUSE

S.No	Location	Scores under different age group					
		Victimized		Non-Victimized		All	
		Score	Rank	Score	Rank	Score	Rank
1	Face Book	63.68	1	63.63	2	63.66	1
2	Instagram	52.63	3	48.60	3	51.22	3
3	Twitter	50.34	4	47.49	4	49.34	4
4	Chat Groups	60.89	2	63.71	1	61.88	2
5	Comments section of Websites	41.80	7	42.80	7	42.15	7
6	Online Dating Sites	44.75	6	46.11	6	45.23	6
7	Personal E-mails	47.32	5	47.11	5	47.25	5
8	Online Gaming Sites	34.88	8	37.23	8	35.70	8

Source: Estimation based on field survey

Victimized respondents have stated that 'Face Book" (1st rank) and 'Chat groups' (2nd rank) as a prime location of Online abuse. In contrast, the ranking for the Non-victimized respondents were stated that 'Chat groups" (1st rank) and the 'Face Book' (2nd

rank) as a prime location of Online abuse. Irrespective of Victimized and Non-victimized respondents were stated as 'Instagram' (3rd rank), 'Twitter' (4th rank), 'Personal E-mail' (5th rank), Online Dating Sites (6th rank) and Comments Section of Websites (7th rank). The location of Online abuse which was of least priority were given on 'Online Gaming Sites' (8th rank) for both Victimized and Non-victimized respondents.

PROBLEMS FACED BY WOMEN IN CYBER SPACE

ANOVA Test

ANOVA was done to determine whether the Problems faced by Women in Cyber Space differed across Victimized and Non-victimized respondents. The hypothesis framed was:

H_o: There were no significant differences in the Problems faced by Women in Cyber Space across Victimized and Non-victimized respondents of Cyber Crime.

H_a: There were significant differences in the Problems faced by Women in Cyber Space Users across Victimized and Non-victimized respondents of Cyber Crime.

The results are presented in table .4.17

TABLE 4.17
PROBLEMS FACED BY WOMEN IN CYBER SPACE

S.No	Variables	F Value	Significance
1	Experienced Hacking (either directly/indirectly)	324.020	.000
2	Reported to authorities	305.609	.000
3	Feels Woman are Phone to Cyber Attacks	296.143	.000
4	Received hate message in their inboxes/message boards	287.245	.000
5	Victim of Defamatory statement/activities involving him/herself in the cyber space	277.245	.000
6	Experienced Cyber Stalking	271.559	.000
7	'Cloned' Profile/email id's	193.211	.000
8	Victimized by their own friends	180.225	.000
9	Received abusive/dirty mails in inboxes from known/unknown sources	164.616	.000
10	Experienced bad in the Social Networking Sites	60.420	.000
11	Experienced flaming words from others	51.412	.000

12	Impersonated by E-mail account/social networking Profiles/Websites, etc	37.901	.000
13	Bullied	2.347	.129
14	Experienced Phishing Attacks	.794	.375
15	Seen her Morphed pictures	.005	.944

Source: Estimation based on field survey

The results reveal that there is significant differences across the Victimized and Non-victimized respondents of Cyber Crime with respect to Experienced Hacking (either directly/indirectly), Reported to authorities, Feels Woman are Phone to Cyber Attacks, Received hate message in their inboxes/message boards, Victim of Defamatory statement/activities involving him/herself in the cyber space, Experienced Cyber Stalking, 'Cloned' Profile/email id's, Victimized by their own friends, Received abusive/dirty mails in inboxes from known/unknown sources, Experienced bad in the social networking sites, Experienced flaming words from others, Impersonated by email account/social networking Profiles/Websites, etc.

With regard to other pattern of Problems like Bullied, Experienced Phishing Attacks and Seen her Morphed pictures had no difference across Victimized and Non-victimized respondents of Cyber Crime. Thus, Victimized women deferred from the Non-victimized women in terms of Experienced Hacking (either directly/indirectly), Reported to authorities, Feels Woman are Phone to Cyber attacks, Received hate message in their inboxes/message boards, Victim of defamatory statement/activities involving him/herself in the cyber space, Experienced Cyber Stalking, 'Cloned' Profile/email id's, Victimized by their own friends, Received abusive/dirty mails in inboxes from known/unknown sources, Experienced bad in the social networking sites, Experienced flaming words from others, Impersonated by email account/social networking profiles/websites, etc.

AWARENESS OF CYBER CULTURE AMONG INDIAN INTERNET USERS

ANOVA Test

ANOVA was done to determine whether the awareness on Cyber Culture among Indian Internet Users differed across Victimized and Non-victimized respondents of Cyber Crime.

The hypothesis framed was:

H_o: There were no significant differences in the awareness on Cyber Culture among Indian Internet Users across Victimized and Non-victimized respondents of Cyber Crime.

H_a: There were significant differences in the awareness on Cyber culture among Indian Internet Users across Victimized and Non-victimized respondents of Cyber Crime.

The results are presented in table .4.18

TABLE 4.18

AWARENESS OF CYBER CULTURE AMONG INDIAN INTERNET USERS

S.No	Variables	F Value	Significance
1	Do not allow others to use one's own mail id/ profile id/ password, etc	52.753	.000
2	Share personal information with virtual friends/chat room partner etc whom you don't know in real life	34.062	.000
3	Mail back to unknown senders of spam/ pornographic/ erotic/ phishing mails	31.689	.000
4	Use pseudo names	7.779	.006
5	Read policy guidelines of social networking sites, etc	7.666	.007
6	Knowledge of minimum age to join Cyber communities.	3.181	.078
7	Use safety tips filtering emails, locking personal albums and information, personal walls of social networking sites, etc	.630	.429
8	Believe in controlling free speech while communicating in the Cyber Space	.024	.877

Source: Estimation based on field survey

The results reveal that there were significant differences across the Victimized and Non-victimized respondents of Cyber Crime with respect to Awareness of Cyber Culture among Indian Internet Users on 'Do not allow others to use one's own mail id/ profile id/ password, etc, Share personal information with virtual friends/ chat room partner etc whom you don't know in real life, Mail back to unknown senders of spam/ pornographic/ erotic/ phishing mails, Use pseudo names, Read policy guidelines of social networking sites, etc'.

With regard to other pattern of awareness like, 'Knowledge of minimum age to join Cyber communities, Use safety tips filtering emails, locking personal albums and information and Believe in controlling free speech while communicating in the Cyber Space' there was no difference across Victimized and Non-victimized respondents of Cyber Crime. Thus, Victimized respondents deferred from the non-victimized respondents with respect to Allow others to use one's own mail id/ profile id/ password, etc, Share personal information with virtual friends/chat room partner etc whom you don't know in real life, Mail back to unknown senders of spam/ pornographic/ erotic/ phishing mails.

SUGGESTIONS FOR CYBER CRIME

Factor Analysis

There are many things to like about Internet: the convenience, the functionality, even the fashion component. But there are also aspects that users dislike. Beyond obvious issues such as Harassments via e-mail, Cyber Stalking, Cyber Pornography, Hacking, Cyber Defamation, Morphing, E-mail Spoofing, Cyber Flirting, Cyber Bullying and Cyber Sexual Defamation all of these concerns constitute what we might call the "dark side" of Internet. An attempt was made to gauge attitude of the respondents on the Suggestions for using Internet to avoid Cyber Crimes the various statements were listed relating to the suggestions for Cyber Crimes against women in India and the respondents were asked to rate the statement on a five point scale, with maximum point five given most favourable statement and a minimum of one given to least favourable statement. Factor analysis was used to identify the underlying dimensions among the factors on suggestions for Cyber Crimes against Women in India. To determine the reliability of applying factor analysis the Cronbach's alpha test was applied and was estimated to be 0.879, which was greater than 0.7 indicating the reliability of the constructs. To determine the appropriateness of applying factor analysis the KMO and Bartlett's test measures were computed and the results are presented in table.4.19.

TABLE 4.19

KMO AND BARTLETT'S TEST MEASURES

Kaiser-Meyer-Olkin Measures of Sampling	.860
Bartlett's test of Sphericity approx: chi-square	450.338
Degrees of freedom	55
Significance	.000

Source: Estimation based on Field survey

The KMO statistics for all respondents was 0.860, signifying higher than acceptable adequacy of sampling. The Bartlett's test of sphericity was also found to be significant at 1 percent level providing evidence of the presence of relationship between the variables to apply factor analysis.

The communalities for variable were computed to determine the amount of variance accounted by the variable to be included in the factor rotation and the results are shown in table.4.20

TABLE 4.20

COMMUNALITIES

Suggestions	Initial	Extraction
Constantly Update Password and Login Details	1.000	.915
Report Suspicious Activities	1.000	.790
Use Anti-Virus Software's	1.000	.727
Ignore Pop-Ups	1.000	.793
Two-Step Verification	1.000	.741
Only Use Secure Sites	1.000	.748

Avoid Being Scammed	1.000	.815
Avoid Unknown requests	1.000	.711
Be Social Media Savvy	1.000	.787

Source: Estimation based on Field Survey

Extraction method: Principal Component Analysis

The table 4.21 enlists the Eigen values, their relative explanatory powers and the factor loadings for 9 components identified within the data set. The Eigen values greater than one alone was considered for inclusion in the analysis.

TABLE 4.21

ROTATED COMPONENT MATRIX

S.No	Suggestions	Components		
		1	**2**	**3**
1	Constantly Update Password and Login Details			.945
2	Report Suspicious Activities		.853	
3	Use Anti-Virus Software's	.791		
4	Ignore Pop-ups		.809	
5	Two-steps Verification	.854		
6	Only use Secure Sites		.778	
7	Different Sites, Different Passwords	.771		
8	Be aware while using Public Wi-Fi Hotspots	.728		
9	Avoid Being Scammed	.864		
10	Avoid Unknown requests	.708		

11	Be social Media Savvy	.823		
Eigen values		5.899	1.372	1.030
Percentage of variance		53.624	12.468	9.362
Cumulative percentage		53.624	66.092	75.454

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization,

Rotation converged in 5 iterations.

Source: Estimation based on Field Survey

The results indicates that for the sample data, Eigen value of the first three factors alone was greater than one for Victimized and Non-victimized respondents by Cyber Crime and Suggestion for Cyber Crimes, that these factors alone were appropriate for inclusion in the analysis. For Suggestions for Cyber Crimes three factors together accounted for nearly 75 percent of the variations in the factors.

For Suggestions for Cyber Crimes, factor 1 has significant loadings for seven dimensions namely 'Use Anti-Virus Software's', 'Two-step Verifications', 'Different Sites, Different Passwords', 'Be aware while using Public Wi-Fi Hotspots', 'Avoid Being Scammed', 'Avoid Unknown Requests', 'Be Social Media Savvy'. These Seven dimensions together explained nearly 54 percent of the variance. Factor 2 has significant loadings for three dimensions namely 'Report Suspicious Activities', 'Ignore Pop-Ups', 'Only use Secure Sites' and explained nearly 12 percent of the variance. Factor 3 has significant loading for one dimensions namely 'Constantly Update Password and Login Details' and explained nearly 9 percent of the variance. To sum up, the major suggestions sited by sample respondents for reducing Cyber crimes against Women in Coimbatore City were Update Password Constantly, using Two-step Verification, Reporting Suspicious Activities, Ignoring Pop-ups, Avoid Being Scammed and Be social Media Savvy.

CHAPTER V

SUMMARY AND CONCLUSION

Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

The different types of Internet crime vary in their design and how easily they are able to be committed. Internet crimes can be separated into two different categories. There are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. The typical crimes in criminal history are now being brought to a whole different level of innovation and ingenuity. People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers.

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Therefore, a study on perception of women internet users on cyber-crime against women in Coimbatore city was undertaken with the following Objectives

The specific objectives of the study are:

(a) To study the characteristics of women internet users in Coimbatore City.

(b) To examine the reasons and types of Cyber Crime against Women.

(c) To elucidate the problems faced by women on Cyber Crime.

(d) To analyze the awareness about Cyber Crimes among Internet Users.

(e) To give suggestions to curb the Cyber Crime against Women.

HYPOTHESES

In the course of the study the following hypotheses were examined.

- Inter users are young and highly educated.
- The opinions of respondents regarding Internet services do not differ significantly.
- There were no significant differences in the Harassments in Online across Victimized and Non-victimized respondents of Cyber Crime.
- The respondents did not differ in the ranking of the Location of Online Abuse of Cyber Crimes.
- The problems in Cyber space are the same for the victimized and non-victimized respondents
- There is no association between Awareness on Cyber Culture among Indian Internet users among the Victimized and Non-victimized respondents.
- The strategies suggested by the internet users for reducing crimes on internet are the same for victims and non-victims respondents.

METHODOLOGY

The population of the study consisted of Women Internet Users in Coimbatore city. From these selected areas 100 samples were selected by adopting incidental purposive sampling technique. The term incidental sampling is applied to those samples that are taken because they are most readily available. The basic assumption behind purposive sampling is that with good judgment and an appropriate strategy one can handpick the cases to be included in the sample and thus develop samples that are satisfactory in relation to one's needs (Guilford, 1978). A common strategy of purposive sampling is to pick up cases that are judged to be typical of the population, in which one is interested, assuming that errors of judgment in selection will tend to counter balance each other if sufficiently large sample is taken. Questionnaire was administered to Women Internet users within the selected area of the city. Women Internet users were asked to complete

the questionnaire. A total of 100 Women Internet Users were contacted. Hence, the investigator approached only those peoples were willing to cooperate and supply the needed information. Relevant and required data for the present study were collected from the primary source by administering an interview schedule to the selected women Internet users. The interview schedule was first pre-tested to check for clarity and specificity and the necessary modifications were made on the basis of the experience gained during pre-testing. The field investigation and data collection for the study was carried out during the period December- March (2017).

TECHNIQUES OF ANALYSIS

Besides averages, percentages and graphs, techniques like Chi-square Test, Garrett's Rating Scale, Likert's Summated Scale, One-way ANOVA, Factor Analysis and Cronbach's Alpha were used.

EMPIRICAL FINDINGS

The major findings of the study are summarized below:

Socio-economic profile of the selected respondents

- The surveyed samples were Women Internet Users in Coimbatore City.
- Most of the surveyed samples were in the age group of 20-30 years, categorised as Young Adults and the general Education Status of the sample respondents was Under-Graduation level.
- There was equal proportion of Employed and Students. Of the employed respondents, 44 per cent were working in Private Concerns and 9 per cent in Public Sector. In the non-working group, 47 per cent were Students.
- Most of the surveyed samples were Unmarried (52 percent) and majorly (46 percent) had three members in their family.
- The analysis of the total Income of the respondents reveals that 27 per cent of the respondents had monthly income of ₹.10,000- ₹.20,000, 15 per cent were earning ₹.20,000- ₹.30,000, 5 per cent were earning ₹.30,000- ₹.40,000 and less than ₹.10,000 as monthly income, 1 per cent of the respondents were earning above ₹.40,000 as their monthly income and 47 per cent of the respondents were students.

Details on Internet Usage:

- Analysis of the Places of Internet usage by the sample respondents showed that majority of them uses Internet Daily at Home (59 percent), Majority of them uses Internet at other places Weekly (65 percent), Majority of the uses Internet at Cyber Cafe Sometimes (59 percent).
- The analysis of the Other Internet Users in home other than sample respondents reveal 45 per cent and 28 per cent of them were Siblings (Brother and Sister), followed by Parents (Father (6 per cent) and Mother (8 per cent)), followed by Grandparents by 2 per cent, Children's by 4 per cent and All persons by 5 per cent and the remaining 2 per cent shows that no one uses the Internet in home other than the sample respondents.
- Data pertaining to the mail account usage shows that majority (88 per cent) of the respondents were had mail account and 12 per cent of the respondents were do not use mail account.
- The perception of the respondents for having Privacy locks for Social Media shows that majority of them had privacy locks for their Social media by 62 percent).
- The perception of the respondents on the usage of Social Network shows that majority of the respondents uses Face Book by (36 per cent) and another 36 per cent of the respondents uses Face Book and Other Social Network, followed by 10 per cent of the respondents uses other Social Network, 9 per cent of the respondents uses Orkut, 8 per cent of the respondents uses Twitter and the remaining 1 per cent of the respondents uses Blog's. That the sample respondents majorly used Face Book and Other Social Network.
- Downloading data over Internet would be Legal and Illegal, majority (72 per cent) of the respondents were said that downloading data over Internet were Legal and the remaining 28 per cent of the respondents were said that downloading data over Internet is Illegal.
- The data pertaining to the major downloads from Internet shows that majority (42 per cent) of the respondents downloads Movies, Songs, Applications, Study Materials and Government Documents, other 18 per cent of the respondents

downloads Movies, Songs, Applications and Government Documents, 2 per cent of the sample respondents downloads only Applications, 1 per cent of the respondents downloads only Movies, another 1 per cent of the respondents downloads only Songs, another 1 per cent of the respondents downloads only Study materials and the remaining 25 per cent of the respondents were downloads Movies, Songs, Applications, Study materials, Software's and Government Documents.

- Data pertaining to the Internet Browser used by the sample respondents shows that majority of them using Google chrome, Internet Explorer, Mozilla Firefox, Opera Mini as their Browser, 28 percent of them use only Google chrome and 16 percent of them use Internet Explorer, Google Chrome and Mozilla Firefox.
- Changing the Password for their personal accounts was important to protect the personal information's. Study shows that 48 percent of the respondents change their password by Monthly, 40 percent of them changes fortunately and respondents change their passwords Weekly and Daily by 11 percent and 1 percent respectively.
- In the present study majority 37 percent of the respondents got aware to Internet by their Siblings, 33 percent of them were aware by their Friends, another 18 percent of them were aware by their Relatives and 7 percent, 4 percent and 1 percent of them were aware by Media, Schools/Colleges and Parents respectively.
- Factor analysis was used to identify the underlying dimensions among the factors on reasons for using Internet. To determine the reliability of applying factor analysis the Cronbach's alpha test was applied and was estimated to be 0.835, which was greater than 0.7 indicating the reliability of the constructs.
- The KMO statistics for all respondents was 0.720, signifying higher than acceptable adequacy of sampling. The Bartlett's test of sphericity was also found to be significant at 1 percent level providing evidence of the presence of relationship between the variables to apply factor analysis.
- The results of factor analysis indicate the major factors sited by sample respondents for using Internet were To use social media sites, For online

shopping, To search job related information's, To search study related information's, To use Face Book, etc. These factors together accounted for 80 percent of the variations.

Details on Cyber Crime Victimization

- In the present study 65 percent of the respondents were Victimized by Cyber Crime and 35 percent of them were Non-Victimized by Cyber Crime.
- The study shows the types of victimized Cyber Crimes most of the Victimized respondents were affected by the Hacking (34 percent); 19 percent of them were affected by Harassment via E-mails; 7 percent of them were affected by E-mail Spoofing; 2 percent of them were affected by Cyber Pornography and the remaining 35 percent of them were Non-victimized by. The study found that majority of them Victimized affected by Hacking.
- Majority (22 percent) of the respondents were victimized by Strangers, Girlfriend, Boyfriend, Family Members and Co-workers; 18 percent of them were victimized by Strangers; 14 percent of them were victimized by Co-workers; 13 percent of them were victimized by Boyfriends; 12 percent of them were victimized by Girlfriends; 11 percent of them were victimized by Family Members and 10 percent of them were victimized by Acquaintance. The study found that there is no much difference in perpetrator of Cyber Crimes against Women and the major perpetrator of Cyber Crime were Strangers, Relatives and Co-workers.

Location of Online Abuse

- Victimized respondents have stated that 'Face Book" (1st rank) and 'Chat groups' (2nd rank) as a prime location of Online abuse. In contrast, the ranking for the Non-victimized respondents were stated that 'Chat groups" (1st rank) and the 'Face Book' (2nd rank) as a prime location of Online abuse. Irrespective of Victimized and Non-victimized respondents were stated as 'Instagram' (3rd rank), 'Twitter' (4th rank), 'Personal E-mail' (5th rank), Online Dating Sites (6th rank) and Comments Section of Websites (7th rank). The location of online abuse which was of least priority were given on 'Online Gaming Sites' (8th rank) for both Victimized and Non-victimized respondents.

- To guage attitue of the respondents on the suggestions for using Internet to avoid Cyber Crimes factor analysis was done. The KMO statistics for all respondents was .860 signifying higher than acceptable adequacy of sampling. Bartlett's test of sphericity was also found to be significant at 1 percent level providing evidence of the presence of relationship between the variables to apply factor analysis.

Abuse or Harassments in Online

- The Chi-square analysis revealed that Verbally Abused, Physically Threatened, Intentionally tried to embarrass others, Stalked and Sexually Harassed were found to have significant association with the Victimized and Non-victimized respondents by Cyber Crime. This implies that harassments in online against women were higher.

Problems of Women in Cyber Space

- ANOVA was done to determine whether the Problems of Women in Cyber Space differed across Victimized and Non-victimized respondents of Cyber Crime. The results reveal that there is significant differences across the Victimized and Non-victimized respondents of Cyber Crime with respect to Experienced Hacking (either directly/indirectly), Reported to authorities, Feels Woman are Phone to Cyber Attacks, Received hate message in their inboxes/message boards, Victim of Defamatory statement/activities involving him/herself in the cyber space, Experienced Cyber Stalking, 'Cloned' Profile/email id's, Victimized by their own friends, Received abusive/dirty mails in inboxes from known/unknown sources, Experienced bad in the social networking sites, Experienced flaming words from others, Impersonated by email account/social networking Profiles/Websites, etc. With regard to other pattern of Problems like Bullied, Experienced Phishing Attacks and Seen her Morphed pictures had no difference across Victimized and Non-victimized respondents of Cyber Crime.

Awareness on Cyber Culture among Indian Internet Users

- ANOVA was done to determine whether the awareness on Cyber culture among Indian Internet Users differed across Victimized and Non-victimized respondents of Cyber Crime. The results reveal that there were significant differences across

the Victimized and Non-victimized respondents of Cyber Crime with respect to Awareness of Cyber Culture among Indian Internet Users on 'Do not allow others to use one's own mail id/ profile id/ password, etc, Share personal information with virtual friends/ chat room partner etc whom you don't know in real life, Mail back to unknown senders of spam/ pornographic/ erotic/ phishing mails, Use pseudo names, Read policy guidelines of social networking sites, etc'. With regard to other pattern of awareness like, 'Knowledge of minimum age to join Cyber communities, Use safety tips filtering emails, locking personal albums and information and Believe in controlling free speech while communicating in the Cyber Space' there was no difference across Victimized and Non-victimized respondents of Cyber Crime.

Suggestions for Cyber Crimes against Women

- Factor analysis was used to identify the underlying dimensions among the factors on suggestions for Cyber Crimes against Women in Coimbatore City. To determine the reliability of applying factor analysis the Cronbach's alpha test was applied and was estimated to be 0.879, which was greater than 0.7 indicating the reliability of the constructs.
- The KMO statistics for all respondents was 0.860, signifying higher than acceptable adequacy of sampling. The Bartlett's test of sphericity was also found to be significant at 1 percent level providing evidence of the presence of relationship between the variables to apply factor analysis.
- The results of factor analysis indicate the major factors sited by sample respondents for reducing Cyber crimes against Women in Coimbatore City are Update Password Constantly, using Two-step Verification, Reporting Suspicious activities, Ignoring Pop-ups, Avoid being Scammed and Be social media savvy.

CONCLUSION

Roots of cybercrime are lies in technology and critical infrastructure. Number of internet users is continuously increasing and with this growth risk of several types of crimes is also amplified. Cybercrimes are varying in its nature due to enhancement in technologies. (kothawade and Agarwal 2016) While women benefit from using new digital

and Internet technologies for self-expression, networking, and professional activities, cyber victimization remains an underexplored barrier to their participation. Women often outnumber men in surveys on cyber victimization. Based on the findings of the study it is concluded that the young Women (students) were more addicted to Internet. The major factor attracting young women to Internet was Social Media, Entertainment Service, Banking Facilities, Study related Information's and Job related information's. Most of the Women Internet users were affected by Cyber Crime like Hacking, Harassment via E-mail, sexually harassed and physically threatened in Cyber space. The major problems faced by them were women Hacking, Defamation, Stalking, security issues, etc.

RECOMMENDATIONS

As technology continues to move forward, making our lives easier and more connected, cyber criminals are developing more sophisticated techniques to exploit technology for their benefit. No country, industry, community, or individual is immune to cyber risks, and no one government agency, company, or individual can thwart the risks alone. We all have a role to play in stopping cybercrime. Capacity of human mind is profound. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and to guard ourselves so that crime has no effect on us. The main suggestions to prevent Women from Cyber Crimes were noted below:

- Create passwords with eight characters or more and that use a combination of letters, numbers, and symbols.
- Keep social security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name and date of birth.
- Lock the computer and smart phones when not in use.
- Be cautious about opening attachments or clicking on links in emails and remember that free apps (games, ringtones, screen savers) can hide viruses or spam.
- Always use privacy settings on social networking websites.

- Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor.
- Report online fraud to the respective.
- Never disclose the personal information publicly on websites.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and updated Antivirus software to guard against virus attacks.
- To prevent loss of data due to virus attacks, always keep back up of your data.

Bibliography

Books

- Garrett Henry, E (2005), “Statistics in Psychology and Education”, New Delhi, Paragon International Publishing.
- Guliford, J.P (1978), “Psychometric Methods”, New Delhi, Tata McGraw Hill.
- Halder, D., & Jaishankar, K. (2011), “Cybercrime and the Victimization of Women: Laws, Rights, and Regulation”, Hershey, PA, USA: IGI Global.
- Nunnally, J .C. (1978), Psychometric Theory, New York, McGraw-Hill Series in Psychology.

Journals

- Ahmad and Aminah (2007), “Work-family conflict, Life-cycle stage, Social support and coping strategies among Women Employees”, The journal resource and adult learning, Vol: 3, No.1, pp: 70.
- Alison Marganski and Lisa Melander (2015), “Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association with In-Person Dating Violence”, Journal of Interpersonal Violence, pp: 1–25.
- Anjana Kumari, Kapil Sharma and Manju Sharma (2015), “Predictive Analysis of Cyber Crime Against Women in India and Laws Prohibiting Them”, International Journal of Innovations & Advancement in Computer Science IJIACS, Vol: 4, No: 3.
- Anna Leppanen, Timo Kiravuo and Sari Kajantie (2016), “Policing the cyber-physical space”, The Police Journal: Theory, Practice and Principles, Vol: 89, No: 4, pp: 290–310.
- Brandon Valeriano and Ryan C Maness (2014), “The dynamics of cyber conflict between rival antagonists, 2001–11”, Journal of Peace Research, Vol. 51, Issue No: 3, pp: 347–360.
- Chandan Mukherjee, Preet Rustagi and Krishnaji, N (2001), "Crimes against Women in India: Analysis of Official Statistics", Economic and Political Weekly, Vol: 36, No: 43, pp: 4070-4080.

- Christine Zhen-wei Qiang (2009), “Broadband Infrastructure Investment in Stimulius Packages: Relevance for developing Countries”, Vol. 12, Issue.2.
- Harvey, C (1992), “Culture, Human Development and Economic Growth”, Aldershot: Gower.
- Hemraj Saini, Yerra Shankar Rao and T.C.Panda (2012), “Cyber-Crimes and their Impacts: A Review”, International Journal of Engineering Research and Applications, Vol: 2, No: 2, pp: 202-209.
- Ibrahim Baggili and Marcus Rogers (2009), "Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity", International Journal of Cyber Criminology, Vol : 3, No: 2, pp: 550-565.
- Jackson T.C.B Jack and Robert W.Ene (2016), “Cybercrime and the Challenges of Socio-Economic Development in Nigeria”, Journal Of Research In National Development, Vol: 14, No: 2, pp: 42-47.
- Janhavi J Deshmukh and Surbhi R Chaudhari (2014), “Cyber crime in India scenario-a literature snapshot”, International Journal of Conceptions on Computing and Information Technology, Vol: 2, No: 2, pp: 24-29.
- Jaspreet Singh (2015), "Violence against Women in Cyber World: A Special Reference to India", International Journal of Advanced Research in Management and Social Science, Vol: 4, No: 1, pp: 60-76.
- Jock Collins (2007), “Immigrants as Victims of Crime and Criminal Justice Discourse In Australia”, International Review of Victimology, Vol: 14, No: 7, pp: 57-79.
- Jongyeon Tark and Gary Kleck (2004), “Resisting Crime: The Effects of Victim Action on the Outcomes of Crimes”, Criminology, Criminal Justice Periodicals, Vol: 42, No: 4, pg: 861.
- Kamini Dashora (2011), “Cyber crime in the Society: Problems and Preventions”, Journal of Alternative Perspectives in the Social Sciences, Vol: 3, No: 1, pp: 240-259.
- Kenny, G (1995), “The Missing Link-Information”, Information Technology for Development, Vol.6, pp. 33-38.

- Lewis Herrington and Richard Aldrich (2013), “The Future of Cyber-Resilience in an Age of Global Complexity”, POLITICS, Vol: 33, No: 4, pp: 299–310.
- Lorena Montoya (2014), "Modelling Urban Crime through workforce size: a test of the activity support concept", Environment and Planning: Planning and Design, Vol: 42, pp: 399-414.
- M.Alexis Kennedy and Melanie A. Taylor (2010), “Online Harassment and Victimization of College Students”, Justice Policy Journal, Vol: 7, No: 7.
- Manisha M. More, Meenakshi P.Jadhav and K.M.Nalawade (2015), “Online Banking and Cyber Attacks: The Current Scenario”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol: 5, No: 12, pp: 743-749.
- Mayank R. Kothawade and Preeti Agarwal (2016), “Cybercrimes An Indian perspective”, International Journal of Engineering Science and Computing, Vol: 6, No: 4, pp: 3863-3870.
- Mansell, R and Wenn.U (1998), “Knowledge Societies: Information Technology for Sustainable Development”, Oxford, UK: Oxford University Press.
- Michelle F. Wright (2015), “Cyber Victimization and Perceived Stress: Linkages to Late Adolescents’ Cyber Aggression and Psychological Functioning”, Youth & Society, Vol: 47, No: 6, pp: 789–810.
- Michelle F. Wright (2016), “Cyber Victimization on College Campuses: Longitudinal Associations with Suicidal Ideation, Depression, and Anxiety”, Criminal Justice Review, Vol: 41, No: 2, pp: 190-203.
- Neelam Seam (2013), "Cyber crime against Women", My Research Journal, Vol :8, No: 2.
- Nidhi Agarwal and Neeraj Kasuhik (2014), “Cyber Crimes Against Women”, Global Journal of Research In Management, Vol: 4, No: 1, Pp: 37-49.
- Nithya N.R (2013), "High Literacy and Mounting Violence: A Case of Women in Kerala, India", International Journal of Scientific and Research Publications, Vol: 3, No: 9.

- Odumesi and John Olayemi (2014), “Combating the Menace of Cybercrime”, International Journal of Computer Science and Mobile Computing, Vol: 3, No: 6, pp: 980-991.
- Pooja suman (2015), “Cyber-Crime Against Women and Unconstitutional Section 66-A of Information Technology Act 2000: A Brief Discussion”, International Journal of Research and Analysis, Vol: 3, No: 2.
- Press, L (1996, February), “The Role of Computer Networks in Development”, Communications of the ACM, Vol. 39, Issue.9.
- R.N Mangoli and Ganapati M.Tarase (2009), "Crime against Women in India: A Statistical Review", International Journal of Criminology and Sociological Theory, Vol: 2, No: 2, pp: 292-302.
- Ronald J. Burke, Mustafa Koyuncu and Lisa Fiksenbaum (2010), “Organisational practices supporting women’s career advancement and their satisfaction and well-being in Turkey”, Women in Management Review, Vol: 21, No: 8, pp: 610-624.
- Ryan C. Maness and Brandon Valeriano (2016), “The Impact of Cyber Conflict on International Interactions”, Armed Forces & Society, Vol: 42, No: 2, pp: 301-323.
- Shalini Kashmiria (2014), "Mapping Cyber Crimes Against Women in India", International Research Journal of Commerce and Law, Vol: 1, No: 5, pp: 22-38.
- Sheryl A. Hemphill, Michelle Tollit, Aneta Kotevski and Jessica A. Heerde (2015), “Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of Australian Secondary School Students”, Journal of Interpersonal Violence, Vol: 30, No: 15, pp: 2567–2590.
- Shivani Grover (2015), “Cyber Security in Digital Economy”, International Journal of Business Management, Vol: 2, No: 2, pp: 1563-1569.
- Shobhna Jeet (2012), “Cyber crimes against women in India: Information Technology Act, 2000”, Elixir International Journal Criminal Law 47, Vol: 47, No: 4, pp: 8891-8895.
- Shubham Kumar, Santanu Koley and Uday Kumar (2015), “Present Scenario of cybercrime in INDIA and its preventions”, International Journal of Scientific and Engineering Research, Vol: 6, No: 4, pp: 1971-1976.

- Sophia J.Ali (2011), “Challenges Facing Women Employees in Career Development: A Focus on Kapsabet Municipality, Kenya”, International Journal of Current Research, Vol: 3, No: 8, pp: 196-203.
- Sudershan Pasupuleti, Eric G. Lambert, Shanhe Jiang, Jagadish V. Bhimarasetty and K. Jaishankar (2009), “Crime, Criminals, Treatment, and Punishment An Exploratory Study of Views Among College Students in India and the United States”, Journal of Contemporary Criminal Justice, Sage Publications, Vol: 25, No: 2, pp: 131-147.
- Sumanjit Das and Tapas Wini Nayak (2013), “Impact of Cyber Crime:Issues and Challenges”, International Journal of Engineering Science and Emerging Technologies, Vol: 6, No: 2, pp: 142-153.
- Tanaya Saha and Akancha Srivastava (2014), "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization", International Journal of Cyber Criminology, Vol: 8, No: 1, pp: 57-67.
- Yougal Joshi and Anand Singh (2013), “A study on Cyber Crime and Security in INDIA”, International Journal of Engineering and Management Research, Vol: 3, No: 3, pp: 13-18.

Thesis

- Madan Mohan Oberoi (2002), “Regulatory and Enforcement Issues of E-Commerce and Cyber Crime in India Context”, Department of Management Studies, submitted for doctorate thesis programme, Indian Institute of Technology, New Delhi, India.
- Malarvizhi.V, (2011), “Perception on E-Banking Services Among Users and Non-users in Coimbatore City”, Department of Economics, submitted for Doctorate thesis program, Avinashilingam University, India.

Working Paper

- Adithya Kumari, H, MahadevaMurthy, M and Ali, H (2013), "Awareness and Use of Internet Facilities by the Students of VidyaVikas Institute of Management Studies in Mysore city: A study", Paper presented at the National Conference on Inspiring Library Services, Tumkur.
- Dhanaraj Thakur, Lyoyd Waller, Shinique Walters and Stephen Johnson (2015), "Violence against Women and the use of Information and Communication Technologies in Jamaica", Research Project, Regional Fund for Digital Innovation in Latin America and the Caribbean, Centre of Leadership and Governance, The University of the West Indies, Mona.
- Duygu Solak and Murat Topaloglu (2014), "The Perception Analysis of Cyber Crimes in View of Computer Science Students", Procedia - Social and Behavioral Science Pp: 590-595.
- Sheela Saravanan (2000), "Violence against Women in India A Literature Review", Institute of Social Studies Trust, India.
- Teena Jose, Y.Vijayalakshmi and Suvanam Sasidhar Babu (2016), Cyber crimes in Kerala: A Study", 6th International Conference on Advances in Computing & Communications, Cochin, India, Procedia Computer Science, Science Direct.

Reports

- The World's Women (2010), the report of the United Nations Organization in 2010, Pp: 127-139.
- World Health Organization, "Global and regional estimates of violence against women: Prevalence and health effects of intimate partner violence and non-partner sexual violence". (Geneva: WHO, 2013).

Websites

- Census of India, 2011 http://www.censusindia.gov.in
- CYBERLAWSINDIA.net, Internet Crime, http://www.cyberlawsindia.net/internet-crime.html.
- http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html

- INTERPOLE, Connecting Police for a Safer World, https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
- Japleen Pasricha (2016), **"Violence Online in India: Cybercrimes against Women & Minorities on Social Media",** FEMINISM IN INDIA.COM.
- Marco Gercke (2012), "Understanding cybercrime: Phenomena, challenges and legal response", ITU Telecommunication Development Bureau, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
- National Cyber security Awareness Month 2014, National Crime Prevention Council, http://ncpc.typepad.com/prevention_works_blog/2014/10/7-tips-to-protect-yourself-from-cybercrime.html.
- Moore, A (2009) "Cyberstalking and Women - Facts and Statistics" available on http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm
- Muthukumaran, B (2008) "CYBER CRIME SCENARIO IN INDIA" avaialable on http://www.gcl.in/downloads/bm_cybercrime.pdf
- Simhan, R "India ranks third in cyber bullying" Business Line available on http://www.thehindubusinessline.com/industry-and-economy/infotech/india-ranks-third-in-cyber-bullying/article3573592.ece
- Kumar, M (2010) "Cyber stalking : Online harassment or Online abuses" available on http://www.cyberarmy.in/2010/12/cyber-stalking-online- harassment-or.html
- "Email Harassment in Business" available on http://www.icsworld.com/Private_Investigation_Case_Studies/Email_Harassment_in_Business.aspx
- Duggal, P "Cybercrime" available on http://cyberlaws.net/cyberindia/cybercrime.html
- Childnet International "Cyberbullying: A whole-school community issue" available on http://digizen.org/downloads/cyberbullyingOverview.pdf
- Cyber stalking (2011) "Cyber stalking: A growing problem" available on http://womenslawproject.wordpress.com/2011/06/13/cyberstalking-a- growing-problem/

- The Times of India, March 18 (2013) “Cyber stalkers leave residents in web of trouble” available on http://articles.timesofindia.indiatimes.com/2013-03-18/ludhiana/37813762_1_cyber-stalkers-cyber-cell-e-mail-account
- Cyber Times, National News Paper 25.07.2017, http://cybertimes.in/?q=node/540.

Dissertation

- Adam C.Tagert (2010), “Cybersecurity Challenges in Developing Nations”, Carnegie Mellon University, Research Showcase @ CMU, Paper: 22.

Interview Schedule to Elicit Information on Perception of Women Internet Users on Cyber Crime Against Women in Coimbatore city

Personal Details

Name :

Age :

Education :

Designation :

Monthly Income Level :

Marital Status : Married ☐ Unmarried ☐ Widow ☐ Separated (Please Tick)

Family Members :

1. Place and frequently usage of internet?

	Daily	Weekly	Fortunately	Monthly
At Home				
At Office				
At Cyber Café				
At Public Place				
Any other place				

2. If at home, who uses the Internet other than you?

   Father ☐ Mother ☐ Brother ☐ Sister ☐ Grandparents ☐ Children's ☐ No one ☐ All ☐ (Multiple Ticking Option)

3. Do you have e-mail account? **Yes** ☐ **No** ☐
4. Which of the Social Network do you use Orkut ☐ Facebook ☐ Twitter ☐ Blog ☐ Any other social network site ☐ (Multiple Ticking Option)

5. What do you download from Internet?
   Movies ☐ Songs ☐ Application ☐ Study Material ☐ Software's ☐ Government Documents ☐ (Multiple Ticking Option)
6. Do you think downloading data over Internet is legal or not? **Yes** ☐ **No** ☐
7. Which Internet browser you use regularly?
   Internet Explorer ☐ Chrome ☐ Mozilla Firefox ☐ Opera Mini ☐ Any Other ☐ (Multiple Ticking Option)
8. Do you use password for Social Media security? **Yes** ☐ **No** ☐
9. How regularly you change the Social Media / mail password?
   Daily ☐ Weekly ☐ Monthly ☐ Yearly ☐ (Please tick)
10. Who created awareness to use Internet?
    Friends ☐ Relatives ☐ blings ☐ dia Pa☐nts In ☐ool / Colleges (Multiple ☐king Option)
11. **Reasons for Using Internet**

S.No	Particulars	Always	Sometimes	In a while	Rarely	Not at all
1.	To use E-mail					
2.	To use Face book					
3.	To View photo					
4.	To use other social media sites					
5.	To Read news					

6.	To Search for job related information					
7.	To Play games					
8.	To Listen or down load music					
9.	To Search for Study related information					
10.	To use Banking Facilities					
11.	For online shopping					
12.	To get day to day information's					

12. Do you aware about Cyber Crime? Yes ☐ No ☐

13. If yes, what type of cyber do you face while using Internet?

Harassment via e-mail ☐ Cyber Stalking ☐ Cyber Pornography ☐ Hacking ☐ Cyber Defamation ☐ Morphing ☐ Email Spoofing ☐ Cyber Flirting ☐ Cyber Bullying ☐ Cyber Sexual Defamation ☐ (Multiple Ticking Option)

14. Relationship with perpetrator of online abuse? (Multiple Ticking Option)

S.No	Particulars	Tick
1	Stranger	☐
2	Acquaintance	☐
3	Girlfriend	☐
4	Boyfriend	☐
5	Family member	☐
6	Co-worker	☐

15. Observing abuse or harassment online of others?

S.No	Particulars	Always	Sometimes	In a while	Rarely	Not at all
1	verbally abused					
2	physically threatened					
3	intentionally tried to embarrass another					
4	Stalked					
5	Sexually harassed					

16. Location of online abuse?

S.No	Particulars	Rank
1	Face book	
2	Instagram	
3	Twitter	
4	Chat groups	
5	Comments section of websites	
6	Online dating sites	

7	Personal E-mail	
8	Online gaming sites	

17. **Problems faced by women's in Cyber Crime**

S.No	Particulars	SA	A	N	D	SD
1	Experienced bad in the social networking sites					
2	Received abusive / dirty mails in inboxes from known / unknown sources					
3	Experienced hacking (either directly / indirectly)					
4	Experienced Cyber stalking					
5	Experienced phishing attacks					
6	Impersonated by email account / social networking profiles / websites etc					
7	'cloned' profile / email ids					
8	Victim of defamatory statement / activities involving him / herself in the cyber space					
9	Received hate message in their inboxes / message boards					
10	Seen his / her morphed pictures					
11	Bullied					
12	Experienced flaming words from others					
13	Victimized by their own virtual friends					
14	Reported to authorities					

15	Feels woman are phone to cyber attacks					

(SA – Strongly Agree, A- Agree, N-Neutral, D-Disagree, SD- Strongly Disagree)

18. Awareness of Cyber culture among Indian Internet users?

S.No	Particulars	Fully	Partially	Not at all
1	Knowledge of minimum age to join cyber communities like Face book, Orkut, telegram, etc			
2	Do not allow others to use one's own email id / profile id / password etc			
3	Use safety tips filtering emails, locking personal albums and information, personal walls of social networking sites etc			
4	Mail back to unknown senders of spam / pornographic / erotic / phishing mails			
5	Share personal information / emotions with virtual friends / chat room partners etc whom you don't know in real life			
6	Believe in controlling free speech while communicating in the cyber space			
7	Read policy guidelines of social networking sites etc			
8	Use pseudo names			

19. Suggestion for Cyber Crimes:

S.No	Particulars	Very much	Some what	Undecided	Not really	Not at all
1	Constantly Update Password and Login Details					
2	Report Suspicious Activities					
3	Use Anti-Virus Software's					
4	Ignore Pop-Ups					
5	Two-Step Verification					
6	Only use Secure Sites					
7	Different sites, Different Passwords					
8	Be aware while using Public Wi-Fi Hotspots					
9	Avoid Being Scammed					
10	Avoid Unknown requests					
11	Be social Media Savvy					