CYBER VICTIMIZATION IN INDIA

A Baseline Survey Report

Prepared by

Debarati Halder & K. Jaishankar

Centre for
Cyber Victim Counselling
"Helping Cyber Crime Victims"

http://www.cybervictims.org

TABLE OF CONTENTS

Part - I: INTRODUCTION

1.1. Introduction

1.2. Structure of the report

Part - 2. SURVEY DESIGN AND PROCEDURE

2.1. Objectives of the study

2.2. Research Tool, Samples and Data Collection

2. 3. Limitations

Part - 3: RESULTS AND DISCUSSION

2.1. Awareness of cyber culture

2.2. Frequency in cyber networking

2.3. Knowledge of being victimized

2.4. Knowledge of common legal rights

2.5. Cyber victimization of women and awareness

Part – 4: MAJOR FINDINGS AND RECOMMENDATIONS

Disclaimer: This survey does not include any case study, emails, details of any victim who have contacted "Centre for Cyber Victim Counseling" (CCVC) for help and advice.

INTRODUCTION

1.1 Introduction:

In India, cyber crime and victimization in the cyber space had remained a subject of great trepidation, but lacks awareness. Bizarre combination of nature of attacks; ever changing trends of the victimization, limited knowledge about direct laws which address cyber crimes in India and rights of victims in cases of cyber attacks, contribute greatly towards forming a weird approach to cyber victimization scenario. There are millions of internet users in India now who are frequenting the cyber space on a regular basis for professional, commercial, socializing and educational purposes. Since the IT sector in India have seen a boom in the 1990's, (which still continues), almost every household falling in the economic zone of moderate income groups to high income groups, have internet access at home and people from the age group of 13 to 70 years, belonging to these clusters, are regularly using the internet either at home, or at work places, or at educational institutes, or at cyber cafes. But along with internet-dependency, victimization of 'cyber citizens' and also of those who are not in the 'internet', have grown in an alarming rate, in spite, India has an exclusive legislation dedicated for information technology, e-governance, e-commerce and also e-socialization to a certain extent; this has hardly helped in curbing the ever increasing victimization of individuals in the cyber space in India.

Sadly enough, less awareness brings in more victimization and cyber space victimization is no exception. In India, awareness of cyber victimization has remained limited to several informative and useful tips on how to save one's personal computer and personal data from identity-frauds, emotional blackmailers etc. A comprehensive empirical survey on this issue is the need of the hour.

This base-line survey on awareness of cyber victimization among Indian internet users is a first level activity of CCVC's future project on prevention of cyber victimization in India. The next step on the basis of this report would be a bigger project with a large number of samples.

The goals of the present survey are as follows:

- To examine the level of awareness of adult internet users of modern cyber cultures, trends of victimization and of common legal rights;
- To spread awareness about various trends of cyber victimization of adult internet users including men and women.

1.2. Structure of the report:

The report is divided into three sections. The first section outlines the basic problems that this survey covers; the second section reports the findings with observation and the third section recommends some suggestions. The findings of this report are divided into five parts.

The first part deals with awareness of cyber culture. It is often noted that cyber culture and ethics are misunderstood, misused and misjudged from many aspects by internet users. Once an individual gets internet connection and thereby starts socializing with others through social networking sites, mails and chartrooms, he / she is often lead into trouble either due to his / her own wrong steps or the undue advantage taken by his / her virtual friend(s) or others. This part aims to cover various aspects of cyber cultures and ethics.

The second part deals with frequency of individuals in social networking sites, chat rooms, and emails etc.

The third part deals with 'knowledge of being victimized'. In this segment we have analyzed awareness of respondents of several sorts of victimization; including financial, sexual and non sexual such as bullying and abusing, hacking, impersonating, stalking attacks, defamation, and personal data mining and misuse of the same.

The fourth part deals with 'awareness of legal rights and laws'. This segment aims to research on the general knowledge of common legalities and illegalities of several cyber behaviors and cultures in the cyber space.

The fifth part assesses awareness of victimization as well as trends of victimization of women.

PART II SURVEY DESIGN AND PROCEDURE

2.1. Objectives of the study:

- To examine the trends of individual victimization.
- To analyze the level of awareness about the victimization that occur in the cyber space;
- To know about the respondents' awareness about common legal principles and legal rights regarding internet crimes.

2.2. Research Tool, Samples and Data Collection:

The Research Tool used for this study is a structured questionnaire. This survey is designed with a purpose that sample selection should closely represent the characteristics of the target population, i.e., the general adult internet users of India, who may or may not be aware of the nature of their victimization in the cyber space.

The target population consists of 73 respondents (including 13 male and 60 female) from different regions of India, who are computer literate, internet savvy and also use social networking websites for virtual hanging outs. These respondents belong to different economic and social strata and they may or may not have personal computers at homes. 100 respondents were contacted by emails by the researchers and only 73 of them responded. Several of these 73 respondents have also given specific feedbacks which helped us to frame our observations more accurately.

2. 3. Limitations:

This survey does not intend to cover cyber generated or cyber assisted attacks on governments and corporate bodies and child sexual harassment through internet. This survey is meant to analyze only individual victimization of adults and awareness among adult internet users about cyber victimization. Due to time limitation, purposive sampling method was adopted. This study is only a preliminary study; a full fledged study is planned and no generalizations should be inferred on the findings of this baseline report.

PART III RESULTS AND DISCUSSION

3.1. Awareness of cyber culture:

Cyber culture could be defined as a compact term which expresses norms and cultures that are followed in the cyber space, or internet. Often the word cyber culture is used in context with varied meanings ranging from the culture of hacking or even computer revolution or even cyber cultural issues like cyber topics, cyber organization (see Macek, 2005)* etc. According to Wikipedia, cyber culture means *"the culture that has emerged, or is emerging, from the use of computer networks for communication, entertainment and business. It is also the study of various social phenomena associated with the Internet and other new forms of network communication, such as online communities, online multi-player gaming, and email usage"* (Cyberculture, Wikipedia, 2010, June 29)**.

Clarke (1997)^ has significantly associated the term cyber culture with authorities in cyber space by ISPs, e-news groups, cyber communities etc. For the purpose of this research report, we construe the term *"cyber culture" "as a conglomeration of cyber rules, norms and culture and principles generally provided by the Internet service providers (inclusive of website hosts, chat line providers, email providers etc) and those rules and cultures which may or may not have legal sanction, but which are generally expected to be followed by the common internet users"*.

Hence in this context, cyber culture may mean the followings:

1. Knowledge of minimum age to join any cyber community;
2. Personal information sharing activities;
3. Usage of freedom of speech;

---

* For more information, see Jakub Macek (2005) Defining Cyber culture (V.2), (translated by Translated by Monika Metyková and Jakub Macek), available at http://macek.czechian.net/defining_cyberculture.htm#_edn2, retrieved on 02.07.2010.

**Cyberculture. (2010, June 29). In *Wikipedia, The Free Encyclopedia*. Retrieved 08:04, July 3, 2010, from http://en.wikipedia.org/w/index.php?title=Cyberculture&oldid=370711935

^Roger Clarke, Encouraging cyber culture, available at http://www.rogerclarke.com/II/EncoCyberCulture.html, retrieved on 02.07.2010

Table 1: Awareness of cyber culture among Indian internet users

Awareness of cyber culture among Indian internet users	Yes	No
1. Knowledge of minimum age to join cyber communities like Facebook, Orkut, Myspace etc	56.2%	43.8%
2. Allow others to use one's own email id / profile id /passwords etc	46.6%	53.4%
3. Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc;	69.9%	30.1%
4. Mail back to unknown senders of spam / pornographic / erotic /phishing mails	37.0%	63.0%
5. Share personal information / emotions with virtual friends / chat room partners etc whom you don't know in real life	74.0%	26.0%
6. Believe in controlling free speech while communicating in the cyber space	37.0%	63.0%
7. Read policy guidelines of social networking sites, ISPs etc;	28.8%	71.1%
8. Use pseudo names	45.2%	54.8%

DISCUSSION

1. Knowledge of minimum age:

It is evident from the above table that among a total of 73 respondents, 56.2% are aware of the basic age limit for joining any cyber community/groups/social networking sites. It is to be noted that these 73 respondents are adults and majority of them are 'internetting' for more than 5 years. This particular assessment was necessary as many of these respondents have children who are either in pre-teens or teenagers or even young adults. Most of the respondents felt that the cyber communities or social networking sites or chat rooms etc should be only used by matured users. These respondents are also aware that impersonating as a child (when the user is an adult or a young adult and camouflages as a pre-teen or teenager to groom women and children for cyber nuisances including sexual crimes) in the chat rooms or social networking sites and trapping other children or women especially, are ethically wrong and this can lead to severe legal problems as well.

2. Allowing others to use one's own id and password:

46.6% of the respondents allow others like spouse, children, intimate partners etc to use their own id and passwords. Strangely enough, this 46.6% also includes a fraction of those who belong to those 56.2% of the respondents who are aware of minimum age for joining cyber networking communities. These respondents primarily allow their spouses or intimate partners to use their ids and passwords to check any mails or messages that they may have received during their absence from the cyber space. They feel comfortable to know about such 'vacation messages' from their spouses or intimate partners and they trust that their spouses or intimate partners will not misuse these ids. When asked about children who use their parent's ids, these respondents gave a cumulative answer that either the children use parent's ids for communicating with their parents who stay away from them or with friends of their own age (who probably are using their parent's ids in the same fashion) and this is done under strict vigilance of the parents.

3. Using safety tools and mailing back to unknown senders:

69.9% of the respondents are aware of various self protection tools in the internet like filtering emails, blocking unwanted persons, locking one's personal walls, albums and information in the social networking sites etc. These individuals have used these options either by learning from their own mistakes or from various safety tips available in the internet. 30.1% do not believe in restricting their emails / chat boxes / social networking sites only to known friends and they do not use these safety options. 37.0% respondents mail / message back to any mails / messages that they receive from unknown sources including strangers, spammers etc. These respondents communicate with such strangers more out of curiosity than necessity. 74.0% respondents share their personal information such as actual residential place, telephone numbers, personal favorites, personal pictures, mood swings, opinions about other friends, political parties, non political events, cinemas, holiday-places, children's school details and Information of spouses' workplace and other related information with virtual friends in social networking comminutes, chat partners etc whom they have never seen before in real life, but are in regular contact through mails / messages / phone calls etc.

4. On exercising free speech for communicating in the cyber space:

Awareness of cyber culture also includes the typical way of exercising the right to 'free speech' for cyber communications. These communications may include emails, chats, language used for writing on other's message board, writings on community walls or bulletin boards etc. We found out that only 37.0% respondents believe in exercising right to speech in a controlled and measured way. Some of these respondents also exercise similar communicative languages when they express their feelings through blogs. Many of these respondents felt that informal communications should be limited only between those whom they know very well even in real life since long and who are closely related, such as siblings, cousins etc. This is to note that the concept of free speech in India* differs from that in the US# and other countries. This stands true even for cyber communications also. What could be a 'free speech' in the US# may not be a 'decent', 'wanted' speech and way of expression in India. However, it should be noted, that, 63.0% respondents felt that there is no need to be formal or control speech or expressions in the written form, while in the cyber social networking sites or chat rooms or even in the emails. Some felt that this is an extended version of friendship and growing relationship and hence the communication should be as informal as in real life between two friends or group of close friends even if they do not know each other in real life. Some felt using harsh / teasing / rude criticizing words will never arise any issues of wounding sentiments of the recipient(s).

---

*As has been guaranteed under Article 19(1) (a) of the Constitution of India; Article 19(2) of the Indian constitution lays down the grounds of restrictions on freedom of speech and expressions which are as follows: sovereignty and integrity of India, security of the State; friendly relations with foreign nations, public order, decency of morality, contempt of court, defamation and incitement of an offence.

Freedom of speech is guaranteed by the First amendment to the constitution of the USA, which says "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." For more information see http://topics.law.cornell.edu/constitution/first_amendment

5. Reading the policy guidelines:

The policy guidelines of various cyber communities and ISPs (Internet Service Providers) form an important source for developing cyber culture. Many of these cyber communities have adopted their own policy guidelines to prevent hacking and related economic and sexual crimes, verbal abuse through cyber communications, child abuse etc. Majority of these cyber communities have followed the US laws and may take successful precautionary actions when any abuse is complained. In India several of such US based and some Indian ISPs and cyber communities have become highly popular. Most of the respondents of this study have indicated ISPs such as Yahoo, Gmail, Rediff, Hotmail and networking communities like Orkut, Facebook, Myspace, Yahoo groups, Twitter, Zorpia, etc as their favorite cyber hangout spaces. Notably, 71.1% respondents do not read any policy guidelines before joining cyber networking communities. It is interesting to note that many of the 71.1% respondents belong to the group of those 63.0% respondents who feel that communication and speech need not be restricted in the cyber space. On the contrary, 28.8% have read the policy guidelines and they feel these policy guidelines are enough to create awareness about cyber crimes, cultures and norms.

6. Using pseudo names:

45.2% respondents prefer to use pseudo names especially when socializing through social networking comminutes or chatting for various reasons including protecting his/her own identity. 54.8% do not use pseudo names and they do not feel that protecting privacy or identity by using pseudo names is needed.

2.2 Frequency in cyber networking:

The second part of these findings includes research on frequency in cyber networking among Indian internet users. Some of these responses may be included as part of the first Part, namely, awareness of cyber culture. But we intend to enlist it under the title 'frequencies' to show how often individuals hang around in these web hubs and how frequently they befriend other chatroom / social networking site partners. Table 2 describes the frequency of cyber networking.

Table 2: Frequency in Cyber Networking

Frequency in Cyber Networking	High	Moderate	Low
1. Frequency in the cyber space (including emailing, socializing through social net working sites, cyber communities etc)	83.6%	15.1%	1.3%
2. Frequency in the chat rooms	71.2%	28.8%	-
3. Frequency in interacting with unknown chat partners	27.4%	71.2%	1%

DISCUSSION

The above statistical data would show that among 73 respondents, 83.6% are highly active in networking through emails and social networking sites like Orkut, Facebook etc. 15.1% respondents are moderately active in socializing through mails and networking sites and 1.4% are least active in cyber socializing. We found out that these two groups of respondents (moderate and low) use emails and social networking sites mainly for business / academic / professional purpose and do not feel comfortable to socialize through cyber space as those who form the first category (highest). 71.2% respondents are highly active in chat rooms, whereas, 28.8% are moderately active in their preferred chat rooms. These respondents prefer to chat through chat rooms provided by ISPs such as Gmail, Yahoo, Rediff, AOL etc, and also through online chats available in social networking sites like Facebook, Orkut etc. However, we found that only 27.4% take the risk of chatting with unknown chat-room participants. 71.2% respondents feel it is risky to chat with unknown people and they often give cold to lukewarm response to unknown persons when he /she starts conversation with the said respondent. These respondents however feel comfortable to chat

with already known chat-room participants, whom they may have known either in real life or through social networking sites previously; many of them prefer to chat only when such 'virtual friends' through social networking sites are known for minimum 2 to maximum 5 months period, and these virtual friends have already shared their thoughts, information etc in community walls, previous email introductions etc. 1.4% respondents do not chat with unknown persons.

3.3. Knowledge of being victimized:

We preferred the title 'knowledge of being victimized' to illustrate how far these respondents are aware that they have become victimized. However, this particular title may not concentrate more on quantity of the cyber crime rates as our main aim was to cover the awareness of being victimized. The following table (3) describes the knowledge of victims on their own victimization.

Table 3: Frequency in Cyber Networking

Knowledge of being Victimized	Yes	No	No awareness
Had bad experience in the social networking sites	61.6%	38.4%	-
Received abusive / dirty mails in inboxes from known / unknown sources	78.1%	21.9%	-
Has experienced hacking (either directly / indirectly)	46.6%	43.8%	9.6%
Has experienced cyber stalking	37.0%	49.3%	13.7%
Has experienced phishing attacks	50.7%	42.5%	6.8%
Has been impersonated by email account / social networking profiles /websites etc	28.3%	60.3%	11.4%
Has seen his/her 'cloned' profile/email ids	41.1%	46.6%	12.3%
Has been a victim of defamatory statements/activities involving him/herself in the cyber space	68.5%	23.3%	8.2%
Has received hate messages in their inboxes/message boards	42.5%	47.9%	9.6%
Has seen his/her morphed pictures	31.5%	57.5%	11.0%
Has been bullied	39.7%	50.7%	9.6%
Has experienced flaming words from others	43.8%	46.6%	9.6%
Victimized by their own virtual friends	45.2%	53.4%	1.4%
Has reported to authorities	37.8%	47.3%	14.9%
Feels women are prone to cyber attacks	74.0%	26.0%	-

DISCUSSION

The Table 3 may show a mixed response on awareness of cyber victimization. The survey aimed to cover victimization in the emails, social networking sites, chat rooms, blogs and the search engines as a whole. It could be seen that 61.6% respondents had bad experiences in social networking sites where they regularly visit to hang around and 78.1% had received dirty / abusive mails from known / unknown senders. These groups of respondents had opined that even if they used filters and safety measures, some how they had been attacked in their emails or social networking sites; they also feel that they had become accustomed with the idea that cyber space is a vulnerable place and users are prone to be attacked.

a. Hacking/stalking/phishing etc:

Table 3 shows that 46.6% had experienced hacking and they understand that their profile / email id / web page etc had been hacked; 43.8% had never experienced hacking as they continuously take precautionary measures to prevent hacking. 9.6% are not aware whether their account got hacked or how their accounts can be hacked. 37.0% felt that they have experienced cyber stalking, 49.3% has never experienced cyber stalking and 13.7% are not aware of cyber stalking. Notably, those who are grouped under these 13.7% failed to understand the true nature of stalking. Indian laws do not describe cyber stalking. It is unfortunate that the term cyber stalking has remained neglected in the laws of India. Neither the Indian penal code, nor the Information technology Act defines or explains this particular term. Many respondents construed the term as harassment like pornography. This misleading conception about cyber stalking arose because in few reported cases on cyber stalking in India, the accused were booked under section 509 of the Indian Penal Code (Duggal, 2009)#. The section speaks mainly on harm on women's modesty and privacy and related harassments. But stalking is not necessarily harassment alone and cyber stalking does not happen only to women; even though women may form major part of victims of cyber staking. Duggal (2009) rightly pointed out that the said section does not cover cyber stalking fully. If we analyze the US laws on stalking, the nearest explanation of cyber stalking could be found in Violence Against Women and Department of Justice Reauthorization Act of 2005 which amended

Pavan Duggal, India's first cyber stalking case, available at http://cyberlaws.net/cyberindia/2CYBER27.htm, retrieved on 07.07.10

Communications Act of 1934 (47 U.S.C. 223(h)(1)) through Section 113 to include *the use of* any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet for the purpose of 'stalking', annoying and harassing others as penal offence. This U.S. provision attempts to explain cyber stalking as follows;

Cyber stalking = following the victim's internet activities + using digital device, software to create harassing, threatening, abusing mails/messages etc + transmitting the said mail to the victim's inbox and / or victim's friends or relative's inboxes + successfully creating fear, annoyance, irritation harassed feeling in the victim.

We feel that those who never understood how stalking may have happened or whether stalking have at all happened or not, perhaps feel confused with the whole component parts of the stalking. In one word, when 'following' is added by *Mens rea* to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened. Further, this study shows that 50.7% have understood that they had phishing attacks, 42.5% says they have never been victims of phishing attacks and 6.8% stated that they are not aware. These 50.7% respondents have seen phishing attacks through emails. Most common method is asking them to help for acquiring a lump some of money of a deceased customer / relative, or lottery prize money. The other method is sending fake 'Google / Yahoo warnings' where by the recipient is asked to provide his / her name, date of birth, password, country of residence etc, with a warning that if these are not sent, their Gmail / Yahoo account will be closed. Apparently these sorts of mails had arrived in their inboxes and the respondents had opened it for further clarifications. But this study does not show how many had been victims of phishing attack and thereby have lost their money. The respondents, who were never aware of such phishing attacks, had not communicated with the sender once they checked the originality of these mails from internet and also from friends and acquaintances. 42.5% respondents were already aware of such phishing mails and they marked them as 'spams' whenever they received such mails. These 42.5% never opened these mails and from the subject header they understood that these mails are nothing but 'phishing mails'. 6.8% respondents are never aware of these phishing mails and they claimed that they had neither received such mails nor know anything of phishing.

Impersonation and related attacks:

The table 3 would show that 28.3% respondents are aware of being victimized by impersonated profiles. Impersonated profiles are fake profiles made by an individual using the screen name, personal information or even picture of another. The impersonator may use this profile to cheat others. Our respondents have encountered such impersonated profiles through emails and social networking websites either themselves or have heard about it from their friends and acquaintances. The respondents in their feedbacks stated that these impersonated profiles came up either in the course of socializing through public chat rooms, social networking forums or even in the guise of fake email ids where by the creator of the impersonated email account had taken name of his / her friend or even the name of the respondents' friends also. 60.3% respondents have not encountered such impersonated profiles, (even though they know such pranks could be played by others) either because they are very irregular in the cyber space, or they do not use chat options or they use cyber space only for professional purposes and do not allow any one to chat or send any private emails / messages, neither entertain any unknown person in his / her personal mailing list. 11.4% have never heard of impersonated profile attacks.

Also we had surveyed on the awareness of 'cloned profiles' of the respondents. While in the above paragraph, we intended to note the awareness about impersonated profiles of others, this particular statistics show how many respondents have seen their own impersonated or cloned profiles whereby the harasser misuses the victim's personal information and contacts. 41.1% respondents have seen their own cloned profiles either in the form of social networking profiles or email id profile or chat room id profile. Apparently these profiles may have been made either simply creating fake profiles or using the original screen names or even sometimes by data mining from social networking sites. These respondents got to see their cloned profiles either by themselves or came to know of it through friends or acquaintances. In many of their feedbacks, these respondents have also indicated that they had mails from cloned email ids. Apparently these are proxy email ids which are often received by email users with obscene advertisements etc. But these respondents felt uncomfortable when they first received or seen it. 46.6% respondents have never seen or encountered any such cloned or proxy profiles and 12.3% are never aware of such occurences in the internet.

Defamatory statements / Bullying and flaming messages / Hate messages / Morphed images:

68.5% respondents had seen defamatory statements either in some email messages or in community discussions or in pubic chats etc about themselves. 23.3% had not seen such defamatory messages and 8.2% responded that they are never aware of such messages. Interestingly, many of these respondents' responses were affirmative in receiving bullying and flaming messages, hate messages in their public profiles or community discussion boards about themselves and as such they felt this also added to defamatory activities against them. 39.7% have received bullying messages and 43.8% have received flaming words from others either in their inboxes or in their public profiles; 42.5% have seen hate messages either in their inboxes or in their public profiles and 31.5% had seen their morphed pictures. 23.3% respondents indicated that they have not received or seen any such defamatory messages and neither they bother about such occurrences and 8.2% indicated that they are not aware of any such occurrences. We presume that those who were negative in their response of receiving or seeing such messages / images etc are well aware of cyber space culture and they feel this is normal in cyber life and hence do not worry about such cyber generated disturbances.

Victimized by virtual friends:

45.2% respondents felt that they have been victimized by their virtual friends by either or all of above mentioned ways**.** These respondents may had befriended these friends turned harassers without knowing them in real life or may be these 'friends' had never bothered to abide by cyber ethics and disturbed the respondents in one or many ways. 53.4% indicated that they were not victimized by their virtual friends and 1.4% indicated they do not know about this. We noted that many of those who indicated that they were not victimized by their virtual friends had practiced safe cyber practices like not accepting everybody as friend and accepting only those who are recommended by his / her already existing friends; keeping a safe distance from virtual friends; and not exhibiting too much personal information.

Reporting to authorities:

Among these respondents who are aware of cyber attacks or who had been victims themselves, 37.8% have reported the incidences to the authorities of Gmail, Yahoo, Orkut or Facebook etc; 47.3% are never bothered to report such incidences and 14.9% indicated that they do not know how to report and where to report. We understand that those who reported and those who have not bothered to report may have read the 'how to report' columns and other policy guidelines of service providers and those who indicated that they do not know, may have never read any policy guidelines regarding reporting. 74% of these respondents think that women are prone to attack in the cyber space and 26% feel that they are not. We have discussed victimization of women in the cyber space in the later segment.

2.4. Awareness of legal rights and reporting behavior:

In this part, we will cover the legal awareness and the reporting behavior of the respondents. The table below will show the data on legal awareness of the respondents:

Table 4: Awareness of rights and reporting behavior

Awareness of rights and reporting behavior	Yes	No
Aware that hacking, creation of pornography/distributing the same, distribution obscene materials etc are criminal offences	80.8%	19.2%
Aware of his / her legal right to protect privacy in the cyber space	78.1%	21.9%
Aware that cyber bullying, cyber stalking, sending annoying, defaming messages etc can be penalized	19.2%	80.8%
Has reported incidences of cyber victimization to police / lawyers / courts	9.6%	90.4%

As this section deals with awareness on cyber laws, we need to expand a little on the Indian cyber laws. India is governed by Information technology Act 2000 (which is amended in 2008) for cyber space related issues including several cyber crimes such as hacking, computer related offences, offensive communication, violation of privacy, cheating by impersonation, identity theft, cyber terrorism, obscenity, child pornography, transmitting or publishing sexually explicit materials, breach of confidentiality etc. ; and also Indian Penal Code.

Our aim in this section is to establish how far laypersons are aware of certain cyber behaviors which are termed as illegal both by Indian laws and also by international covenants / rules and regulations and general cyber ethics.

Table 4 shows that 80.8% respondents are aware that hacking, creation of pornographic material and distribution of the same is illegal and 78.1% respondents are aware that they have right to privacy in the cyber space. Only 19.2% are aware that cyber bullying, stalking, sending annoying messages etc can be penalized. This gives an impression that as hacking and pornography related cyber crimes are often spoken about in the news papers, news channels and also audio visual media including modern IT related cinemas and daily soaps, many have become aware of these sorts of illegalities. On the other hand, stalking, adult bullying, sending offensive messages etc are not that much spoken about in public and hence awareness about illegalities of these sorts of cyber behaviors is comparatively poor. This survey also shows that 9.6% of the respondents had opted for going for police reports when cyber crime happens. We noted that reporting to the police for cyber pornography, hacking, phishing or impersonation related matters has especially become more 'opted for' after cyber crime police stations have become functional in almost all the major cities of India. However, 90.4% respondents still feel that reporting to the police may bring more victimization and hence they prefer not report to the Police.

2.5. Cyber victimization of women and awareness:

This particular segment is dedicated to research on cyber victimization and awareness of the same on women respondents. Table 5 will elaborate the findings.

Table 5: Cyber Victimization of Women and reporting behavior

Cyber Victimization of Women and Reporting behavior	Yes	No	Not aware of
Experienced bad incidences in the internet	11.7%	88.3%	-
Received abusive mails with sexual images and dirty messages etc from known / unknown senders in her email	85%	15.0%	
Received repeated mails from the same individual/s asking to befriend him/them	16.7%	83.3%	
Received threatening mails from ex boyfriends / husbands	50%	50%	
Received sexually teasing remarks / images in her social networking profile / associated mail / message box	75.0%	25.0%	
Has been victim of hacking	48.3%	41.7%	10.0%
Has been victim of cyber stalking	40.0%	46.7%	13.3%
Has experienced phishing attacks	43.8%	48.3%	7.9%
Has been victim of impersonation	61.7%	26.7%	11.6%
Defamed in the cyber space / in the real space due to cyber activities of others	71.7%	18.3%	10.0%
Has received hate messages	41.7%	46.7%	11.6%
Has been targeted because of her sexuality/feministic ideologies	45.0%	53.3%	1.7%
Victim of morphing	33.3%	58.3%	8.4%
Has been bullied	33.3%	56.7%	10%
Victimized by her virtual friend / s	40.0%	58.3%	1.7%
Has seen her cloned profile	50.0%	40.%	10.%
Feels women are prone to victimization in the cyber space	76.7%	23.3%	-
Feels women's communities/groups etc are safe to discuss feminine issues	38.3%	60.0%	1.7%
Reported victimization	35.0%	46.7%	18.3%
Reported to police / lawyers	8.3%	91.7%	-

The above table would show that among the 60 female respondents of the total 73 respondents, 11.7% had experienced bad incidences in the cyber space in various ways; 85% have received abusive, obscene, dirty messages from known or unknown senders and 16.7% had received repeated mails from same individual / s asking to befriend him / them.

50% of the respondents have received threat mails / messages from ex partners / husbands; and 75% has received sexually teasing remarks in their social networking, profiles and / or associated email in boxes. 48.3% has been victims of hacking; 40% had been victims of stalking and 43.8% had experienced phishing attack. The survey further shows that 61.7% respondents had been victims of impersonation; 50% had seen their cloned profiles; 71.7% had been defamed in the cyber space and also in offline due to cyber defamation; 41.7% has received hate messages from various persons and 45.5% had been targeted because of her sexuality and /or feminine ideologies. 33.3% had been bullied and 33.3% had seen their morphed images; 40% had been victimized by their virtual friends; 76.7% feels that women are prone to victimization in the cyber space and 38.3% feel online women's communities are safe for discussing women related issues. 35% had reported cyber victimization to ISPs etc and 8.3% preferred to report to Police.

Part-3

Major Findings and recommendations

- Majority of the respondents do not feel it is necessary to read the policy guidelines, terms and conditions of ISPs and social networking websites before entering into contract with these sites and thereby opening their accounts;
- Most of the respondents do not mind to share their profile /account and password with their spouses or children;
- Most of respondents like to participate in virtual socializing, however, many are not aware of spams / phishing mails etc and often out of curiosity reply to these mails.
- Many respondents do not prefer to chat with completely unknown persons in public chat rooms and they are aware that such chat-friends may be fradulent; many do not prefer to share their personal secrets with chat friends. But they would prefer to chat with people whom they have met and already accustomed in the social networking sites and followed their responses in various posts. No matter whether these people have met in real life or not; such chat partners may even exchange their personal emails for professional as well as personal purposes.
- Several internet users feel that in the cyber space they need not follow a strict formal rule of communication when in a group / forum; many such internet users are unaware of basic cyber ethics.
- Indian social value system differs from that of the U. S. or European countries. Maximum problems in the cyber space arise when Indian users try to adopt western cyber culture in Indian social value system; glaring examples are the attack on modesty of women in typical cyber ways, use of abusive / harsh language in groups or forums attacking core social / religious sentiments of other users etc and the treatment of the same by Indian laws.
- Cyber defamation, sending threat messages etc are rampant in India. Sexual crimes in the internet are growing.
- Using bullying words in the cyber space by Indian internet users is becoming rampant.

- Social networking sites like Orkut (maximum) and also Facebook are used to harass women by putting up fake profiles with / without morphed pictures, obscene descriptions etc.
- Majority of the respondents do not understand true nature of stalking.
- Majority of respondents are aware of hacking but few know how to protect themselves from hacking.
- Impersonation, emotional and financial cheating, victimizing by making cloned profiles in the cyber space, taking revenge through cyber space for breach of romantic commitments etc are growing in India.
- Many are aware that hacking, sexual crimes in the internet, economic scams, sending threat messages etc can invite legal problems; but maximum Indian internet users are not aware that stalking can also invite penal actions. Similarly bullying, sending annoying messages, impersonating and cheating, posting defamatory messages etc can also attract penal actions.
- Many Indian users are aware that they have a right to protect their privacy in the cyber space. But we understand that this 'privacy' may indicate their personal lives, financial information etc and this may not include the awareness of right to privacy and right to protection against misuse of already exhibited information in their profiles etc.
- Very few respondents, especially women prefer to report the victimization to the police as they feel this may bring in future victimization; however, many are aware of reporting options provided by ISPs or social networking websites and some users also use these options.
- Women are more prone to victimization than men in the cyber space;
- Most women receive mails from unknown men with disturbing contents, requests for friendship etc and such mails may be the results of data mining.
- Many women are victims of several types of harassment meted out by their former partners including former boyfriends.

- Most women receive hate messages sexual / nonsexual teasing remarks, offensive comments etc due to their feministic perceptions expressed both in blogs / forum walls etc; and also for marital status, profile pictures, profile statements etc exhibited in the main profile page.

Based on the above findings, we suggest some recommendations:

1. Awareness campaign must be arranged from grassroots levels such as schools and colleges about cyber ethics and probable cyber crimes like economic cheatings, stalking activities, defamatory activities, misusing email and social net working web sites etc.
2. Police, social workers, lawyers and NGOs must be invited to educational institutes, corporate offices, clubs, social awareness - campaigns, workshops and seminars to talk about legalities and illegalities of cyber conduct among adults inclusive of both the genders. Reporting of cyber victimization must be encouraged at all levels directly to police and also to NGOs working for the cause.
3. More stringent laws must be brought in to curb individual victimization in the cyber space. The present Information Technology Act includes only few sections for cyber crimes, hence a separate law on cyber crimes should be created.
4. Seminars and workshops must be arranged for police personnel for better understanding of such sorts of victimization and prompt responses towards the complainants. Legal and academic experts, NGOs working for this cause etc must be brought in for such seminars and workshops.

Conclusion:

The scenario of cyber victimization in India needs to be studied in detail. It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. Most ISPs and social networking sites adhere to western cyber cultures and cyber rules and regulations which may give rise to opportunities to experiment with the personal freedoms, especially freedom of speech and expression and right to privacy. In the Indian social value system, some of such cyber cultures may give rise to severe abuse of fundamental rights guaranteed by our constitution. Matured adult internet users must understand that what is offensive in the real space, must be maintained as offensive in the cyber space also. Cyber socializing has opened the gateway to a global village which may form its own culture, rules and ethics. But that in no way should encourage abuse of personal rights and freedom.

Centre for
Cyber Victim Counselling
"Helping Cyber Crime Victims"

Centre for Cyber Victim Counselling (CCVC)
28, State Bank Officers Colony,
Maharaja Nagar, Tirunelveli 627 011
Tamil Nadu, India
Emails: ccvcindia@cybervictims.org, ccvcindia@gmail.com
URL: http://www.cybervictims.org