International Journal of Internet of Things 2012, 1(1): 9-15
DOI: 10.5923/j.ijit.20120101.02

Impact of Cyber Crimes on Social Networking Pattern of Girls

M. Neela Malar

Dept of Media Sciences, Anna University, Chennai

Abatract Social networking sites have become an integral part of the lives of most of the youth today. It has encouraged new ways to communicate and share information. The relative freedom afforded by social networking sites has caused concern regarding the potential of its misuse by individual patrons. This questions the safety and security of the users, especially girls who are more preyed upon particularly in relation to online sexual predators. These sorts of cyber crimes leave an everlasting scar in the minds of the users and change the way in which they communicate in the social networking sites and sometimes even force them to completely opt out of the social networking sites. This study deals with how girls are affected by cyber crimes in social networking sites and how those crimes impact their social networking pattern.

Keywords Cyber Crimes, Social Networking, Users, Safety, Online Communities

1. Introduction

A social networking site focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.

Social networking has encouraged new ways to communicate and share information. Social networking websites are being used regularly by millions of people. Although the features of social networking sites differ, they all allow users to provide information about themselves and offer some type of communication mechanism (forums, chat rooms, email, instant messenger) that enables them to connect with other users. On some sites, we can browse for people based on certain criteria, while other sites require that we be "introduced" to new people through a connection we share. Many of the sites have communities or subgroups that may be based on a particular interest.

Cyber Crimes

Cyber or Electronic Crime is where a computer is the target of a crime or is the means adopted to commit a crime. Most of these crimes are not new. Criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery, and embezzlement using the new medium, often involving the Internet (Seth, 2007).

Cyber Crimes in India

India is one of the very few countries to enact IT Act 2000 to combat cyber crimes. The Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data etc as punishable offences (Halder, 2006). However, there is lack of clarity and jurisdiction to keep pace with new forms of cyber crimes and lack of international treaties on cyber crimes to track the sources of crime originating in other countries. There is also lack of cyber army and cyber savvy policy makers including judges and finally there is lack of awareness among the net users.

As per the National Crime Records Bureau statistics, 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006) thereby reporting an increase of 52.8% in 2007 over 2006. 22.3% cases (49 out of 217 cases) were reported from Maharastra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each). 45.6% (99 cases) of the total 217 cases registered under IT Act 2000 were related to obscene publication / transmission in electronic form, normally known as cyber pornography. The age-wise profile of persons arrested in cyber crimes cases under IT Act, 2000 showed that 63.0% of the offenders were in the age group 18 – 30 year (97 out of 154) and 29.9% of the offenders were in the age group 30 – 45 years (46 out of 154). Crime-wise and age group wise profile of the offenders arrested under IT Act, 2000 revealed that 55.8% (86 out of 154) of the offenders were arrested under 'Obscene publication / transmission in electronic form' of which 70.9% (61 out of 86) were in the age-group 18 – 30 years. 50% (24 out of 48) of the total persons arrested for 'Hacking with Computer System' were in the age-group of 18 – 30 years.

Most victims, especially women hesitate to report the crime for fear of personal and social backlash. According to

* Corresponding author:
nmalar@yahoo.com (M. Neela Malar)

Published online at http://journal.sapub.org/ijit

one of the cyber law experts in India Na. Vijayashankar (popularly known as Naavi), it is difficult to measure the growth of Cyber crimes in India by any statistics, the reason being that a majority of cyber crimes go unreported. Cyber lawyers Pavan Duggal, advocate with the Supreme Court of India, points out to the result of a survey he conducted in early 2006 on the extent of under-reporting. For every 500 instances of cyber crimes that take place in India, only fifty are reported and out of that fifty, only one is registered as an FIR or criminal case. So, the ratio effectively is 1:500 and this, he points out, are conservative estimates. Giving an insight into the reasons for low reporting, Nandkumar Sarvade, Director, Cyber Security and Compliance at Nasscom, points out that very often, people are not aware whether an incident is a cyber crime; there is also lack of awareness on where to lodge a complaint or whether the police will be able to understand.

2. Review of Literature

The distribution of malware on social networking sites first occurred in small amounts towards the end of 2007, but that trend appears to be on the rise.

According to a report from MessageLabs Intelligence, which specializes in the analysis of messaging security issues and threats, a popular tactic in 2008 among cyber criminals involved the creation of fictitious accounts on social networking sites. These fake accounts were then used to post malicious links, which usually led to a phishing site, to legitimate users (www.messagelabs.com)

Scammers would then make use of the phished personal information, such as usernames and passwords, to gain access to legitimate accounts. This access would be used to post blog comments on their pages of their friends, and send messages from the phished accounts to other contacts. These messages usually contained spam, including links to spam sites such as online pharmacies.

"Web 2.0 offers endless opportunities to scammers for distributing their malware--from creating bogus social networking accounts to spoofed videos--and in 2008, the threats targeting social networking environments became very real," said Richard Bowman, regional manager, MessageLabs South Asia.

Another report from security expert Symantec, which owns MessageLabs, showed this trend does not look to be slowing down.The report, which analyzed Web threats for the month of January 2009, said social networking sites continue to be popular premises for cyber criminals seeking potential victims.

According to the Symantec report, January saw the emergence of e-mail spam which closely mimicked legitimate notification e-mails of two major social networking sites. These spam messages, which invited users to join a group on the social networking site, contained a link to a virtual group created on the site by the spammers.

Table 1. Some Popular Social Networking Sites

Name	Description/Focus	Registration
Bebo	General	Open to people 13 and older
Bigadda	Indian Social Networking Site.	Open to people 16 and older
Classmates.com	School, college, work and the military	Open to people 18 and older
Facebook	General.	Open to people 13 and older
Flixster	Movies	Open to people 13 and older
Flickr	Photo sharing, commenting, photography related networking, worldwide	Open to people 13 and older
Google Buzz	General	Open
hi5	General. Popular in India, Portugal, Mongolia, Thailand, Romania, Jamaica, Central Africa and Latin America. Not popular in the USA.	Open to people 13 and older. No children allowed
LinkedIn	Business and professional networking	Open to people 18 and older
MouthShut.com	Social Network, social media, consumer reviews	Open
My Opera	Blogging, mobile blogging, sharing photos, connecting with friends. Global	Open
MySpace	General. HTML based site.	Open to ages 13 and up.
Netlog	General. Popular in Europe, Turkey, the Arab World and Canada's Québec province. Formerly known as Facebox and Redbox.	Open to people 13 and older
Orkut	General. Owned by Google Inc. Popular in Brazil and decreasingly, in India.	Open to people 18 and older, (Google login)
Tagged	General. Subject to quite some controversy about its e-mail marketing and privacy policy	Open
Twitter	General. Micro-blogging, RSS, updates	Open
WAYN	Travel and lifestyle	Open to people 18 and older

This virtual group would be linked to a free blogging site before redirecting the user to the destination URL. Upon clicking this URL, users would be faced with the request to fill out a form collecting personal information. Information collected could then be sold to marketing companies or used for other malicious purposes.

In the realm of computer security, the term social engineering is used to describe the malicious intent of people who are trying to gain access to sensitive data and information through illegal means. The process of obtaining information through social engineering techniques implies a lack of technical skills but places a strong emphasis on social skills. However, a skilled social engineer can spend a lot of time gathering publicly available information about the targeted data and talking to eventual victims before directly requesting access to the desired information.

Bagyavati (2009) states in ‘Social engineering’ that “Commonly used modes of social engineering are via the telephone or through the Internet, although face-to-face conversations also form part of the social engineer’s repertoire of techniques. Social engineering attacks rely on the victim’s natural human tendency to trust rather than rigidly following security policies. In general, security professionals agree that human beings are the weakest link in computer and network security; social engineers confirm this fact through their exploits.”

Brenner (2009) states in the article ‘Social networking dangers exposed” that through a variety of easy tricks, attackers can hijack a person's social network account to use as a launching pad for additional attacks against other users, other Web 2.0-based applications, and so on. Social networks can also be incorporated into micro botnets and, by rummaging through a page of misfired direct messages on Twitter, a motivated attacker can unearth the cell phone numbers of prominent people.

Willard (2007) in the article ‘Social networking: Are cyber teens in danger?’ says the hottest new craze among teens and young adults on the Internet is social networking. But concerns related to teen use of social networking sites include unsafe disclosure of personal information, risky sexual behaviour, 'cyber bullying', involvement with dangerous communities and groups, and posting 'cyber threats'. Recent news coverage has raised significant concerns about interactions with strangers, especially sexual predators, on these sites. Many teens spend little time, if any, interacting with online strangers. The vast majority of teens are using social networking sites to engage with known friends and acquaintances from within their school and community. For some, their friendship network may expand to include others they meet in discussion groups. These friends likely are ones with whom they share mutual interests.

Bradley (2009) in the article ‘Predators on Social Networks’ reveals social networking in all the rage. Various web sites have sprung up for the sole purpose of providing a place for users to express themselves, share with like-minded individuals, discover new things, and communicate with others. There have been numerous instances of sexual predators and child molesters posing as children to network with young victims on MySpace.com. MySpace was also recently discovered to be compromised by attackers spreading malware on exploited profile sites. MySpace has taken steps and implemented security measures to minimize this problem, but users should still be cautious and aware. While not directly related to a social network, Craigslist, the popular regional classified listings site, was recently used by a predator to lure a victim to her death. After listing a job opening for a babysitter / nanny, and arranging a meeting with the potential nanny, the killer then murdered the prospective nanny. Photo sharing sites are used by thousands of families to post and share family photos. It is possible to restrict access and only let users you identify view the pictures, but many users are proud of their kids and their photographic skills and allow the general public to view the photos as well. Child molesters and sexual deviants can search through these sites and bookmark their favorite photos of young boys and girls.

Tan (2008) in the article ‘social networking: Danger - Warning for Teens’ says to parents: ‘One of the first things that you may want to discuss with your child is who they are talking with online. Although they may not want to give you an answer, you need to emphasize the importance of knowing who they are talking to. Since social networks work to connect individuals who do not physically know each other it may seem impossible, but it can be done. Your child should fully read and try to understand the content of their friend’s online profiles. This will enable them to watch out for inconsistent stories or any inaccurate information.

Collier & Magid (2009) in the article ‘Social networking dangers in perspective- Social-networking sites may not be as dangerous as some officials claim’

state that there has been a flurry of media coverage of North Carolina Attorney General Roy Cooper's announcement that MySpace had found more than 29,000 registered sex offenders' profiles on its site. As shocking as this news may seem, parents of teen social networkers deserve some perspective. Finding and expelling sexual predators from social Web sites - something MySpace says *it* now does routinely - is a good thing. Other social sites are similarly cooperating with law enforcement. But this announcement from North Carolina Attorney General Roy Cooper (see General Cooper's "Protecting Children from MySpace," a link under "What's New" on his page) was only possible because MySpace took the initiative to develop a law- enforcement tool the federal government called for in a recently passed law- but failed to create a national sex offender database that MySpace then donated to the National Center for Missing & Exploited Children for broader use.

Bharkavi and Sheeba (2009) in their study ‘Safety issues in Orkut for Girls’ found out that most girls do not take much precautionary steps to stay safe on Orkut until they were affected, they were not very suspicious about strangers sending them friend requests until they were affected, they were not much aware of the different types of cyber crimes and cyber laws and they were not aware of the different types of cyber crimes and cyber laws.

San Diego News (2007) in the article tilted ‘Social Networking Sites Could Open Doors to Danger’ reports that these sites are considered great ways to communicate and spread the personal message but the regular users might be surprised to find their information is not as private as they think and that could be dangerous.

Satyanarayana (2009) in the article ‘Five Security Risks of Social Networking Websites’ finds that social networking is big but at the same time it is a big threat for the small businesses and enterprises. He says that companies all over the world bear with the fact that over 45% of the employee’s productive time goes wasted on these sites.

Gonsalves (2009) in the article ‘Social Networkers Risk More Than Privacy’ quotes a U.K. study and suggests that Facebook and Twitter users post personal information that could be used by professional home burglars looking for targets. He says that people who use social networks are posting personal information that could be used by professional home burglars looking for potential targets.

Everett (2009) in the article ‘Social networking - a risk to information security?’ reports as the popularity of social networking sites continues to mount, it becomes increasingly important to consider the information security risks posed in the context of a wider data loss prevention and reputation management strategy. Many organisations, notes Everett, are less concerned about the potential information security implications of using social networking tools and more worried about the potential for time-wasting and reduced productivity. That does not mean to say, however, that such information security risks do not exist.

Leyden (2006) in the article ‘Social networkers risk losing their identities’ says many adult users of social network sites such as MySpace and Facebook expose themselves to risk from identity thieves and hackers. He points out that the focus of concerns over social networking sites has so far focused on incidents where online predators have used the sites to "groom" potential child victims for abuse

Muthalay (2007) in the article ‘Orkut users livid over demands for ban’ states that a ban on the social networking site Orkut has kicked off a debate in cyberspace. He says that a storm is brewing in the virtual world over the popular social networking site Orkut.com, India's second most visited portal. Derogatory remarks about Maratha icon Shivaji posted by certain communities on the site has triggered shrill cries to ban the portal. But as the Indian Computer Emergency Response Team (CERT-In) decides whether to make the site inaccessible to everyone in the country, Orkut users are up against the latest attempt at "Internet regulation".

The Hindu Business Line (2007) states in the article ‘Google in India’s fast lane: Orkut fast rising search query’ that Indian netizens continued to swoon over Aishwarya Rai, making her the most searched for Bollywood celebrity on search engine Google in 2007, even as newcomer Deepika Padukone — who made her Bollywood debut with *Om Shanti Om* in November — earned a spot in the top 10 list in the category. According to the first-ever annual ‘Google Zeitgeist’ report for India (indicating the fastest rising and highest volume search terms submitted to Google in the country), the poster girl of Indian tennis Sania Mirza, was the top Sportstar on Google search, and Mahatma Gandhi the ‘most searched for political leader’.

Zechariah (2009) in the article ‘Man held for defaming woman on Orkut’ states that one person was arrested by the Kolkata Police’s Detective Department for creating a woman’s profile with obscene photographs and putting up her mobile number on social networking site Orkut. The police received a complaint from a person that his wife was receiving lewd phone calls from strangers. An investigation led to the discovery of a profile on Orkut in his wife’s name, with her phone number. Investigators found that the profile was created by a person named Hazra on February 23 2009. He had met the woman when they were students at Technoindia Engineering College in Salt Lake.

Joseph (2009) in the article ‘Man arrested for posting obscene profile of ex-boss on Orkut’ says a former call centre employee landed in jail after he took to cyber crime to avenge alleged harassment at the hands of his boss, a woman. Annoyed over “non-payment of dues”, Vikram Singh, a resident of Gobind Pura in Manimajra in Chandigarh, allegedly created an obscene profile of the manager of the call centre firm on Orkut, a popular networking site. He was arrested on Wednesday under Section 67 of the IT Act and Section 292 of the Indian Penal Code.

Kumar (2008) says that an inter-state gang operating from Mumbai and Visakhapatnam (in Andhra Pradesh) used the social networking website Orkut to buy airline tickets with stolen credit card data. The tickets were sold at a discount to unsuspecting buyers, mostly employees of the Vizag and Bokaro steel plants who were availing their leave travel concession. The city Central Crime Station (CCS) police busted the gang following a complaint from a Hyderabad-based person who found that the gang had fraudulently used his credit card data to purchase the tickets. The CCS police have arrested one Umapathi Thakur alias Vikas Kumar alias Praveen, 22, of Jharkhand, from Visakhapatnam for the gang, saying he was a key operative. The Mumbai-based scamsters who booked the tickets with stolen credit card data are still at large. Umapathi’s office, Ganga Ticket Solutions, was located near the Visakhapatnam Steel Plant. The scam started unravelling when one Ravinder Reddy of Kalyannagar in Dilshuknagar received an SMS from ICICI Bank on May 6 stating that he had purchased an air ticket from Kolkata to Guwahati.

Krishnan (2009) in the article ‘Mumbai Police tie up with Orkut to nail offenders’ finds that Anti-Shivaji forums or anti-Ambedkar postings or “hate India” campaigns on Google’s social networking site, Orkut, have been confounding authorities for quite some time now. Other than blocking the objectionable forums, the Mumbai Police could do little, except wait for the next one to pop up on the web, say, a “fan club” of wanted underworld dons. The Mumbai Police is finally equipped to track down such offenders and bring them to book. A single e-mail between the DCP in charge of the Enforcement Branch and the California-based company will now nail such persons. Following a meeting between representatives of the site and the Enforcement Directorate last month, the Mumbai Police and Orkut have entered into an agreement to seal such cooperation in matters of objectionable material on the web.

Nappinai (2010) in "Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study says that.India was shocked out of its complacent conservatism due to the widespread circulation of a MMS clip shot by a Delhi schoolboy17. This case took an unexpected twist when this clip was circulated on Bazee.com and its Chief Executive Officer of American origin was arrested. S.66E has now been introduced under the ITA, 2008 for the protection of physical or personal privacy of an individual. This section makes intentional capturing of the images of a person's private parts without his or her consent in any medium and publishing or transmitting such images through electronic medium, a violation of such person's privacy punishable with imprisonment of up to three years or with fine up to Rupees Two Lakhs, or both. A case of posting of the personal information and obscene material on a Yahoo! Site was touted as the fastest trial and conviction of a cyber crime case in Chennai18. It appears that this conviction has recently been reversed. S.72 A of the ITA, 2008 now explicitly provides recourse against dissemination of personal information obtained without the individual's consent through an intermediary or under a services contract, with intent to cause wrongful loss or wrongful gain. The maximum punishment prescribed for this offence is three years imprisonment, or fine up to Rupees Five Lakhs or both. Service providers on the Internet, social networking sites, Companies, firms, individuals and other intermediaries ought to now be careful in the collection, retention and dissemination of personal data. Interactive websites and P2P site operators also have to be extremely careful to ensure that the provisions of S.66E & S.72 A are not violated.

3. Social Networking Sites and Indian Youth

The Indian youth have immediately taken to social networking sites, much in the same way they took up internet as a technology. Some of them have gone to the extent of getting addicted to the social networking sites. And some others have met up with serious psychological implications, due to their utmost concentration in the interactions through social networking sites. Above all, there definitely is an increase in the percentage of cyber crimes in India after the invent of social networking sites. As has happened in so many other crimes, girls and young women happen to be the target of attack for cyber criminals too. The details of girls and women displayed in Orkut are (mis)used by the miscreants, raising serious security problems for the youing women aspiring to find friends through Orkut.

Orkut – one of the most famous social networking sites in India

Orkut is a free-access social networking service owned and operated by Google. The service is designed to help users meet new friends and maintain existing relationships. The website is named after its creator, Google employee Orkut Büyükkökten.

Although Orkut is less popular in the United States than competitors Facebook and MySpace, it is one of the most visited websites in India and Brazil. In fact, as of May 2009, 49.83% of Orkut's users are from Brazil, followed by India with 17.51%.

4. History

Orkut was launched on January 22, 2004 by Google as an independent project of Orkut Büyükkökten, a Turkish software engineer. The community membership was originally by invitation only. At first year, United States had the largest user base. By word of mouth, various Brazilians began adopting and inviting more friends, in a viral driven by the blogosphere. Soon after, Brazil surpassed U.S. in number of users and Orkut started becoming heavily popular in Brazil. Americans then started leaving the service and switching to other similar sites such as MySpace and Friendster. This phenomenon was covered by the English blogosphere with some criticism towards Brazilians because they communicate among themselves using their native language Portuguese and not English.

From that time, orkut growth was driven by Brazilian users, first being opened to everyone by registration and becoming one of the most popular websites in Brazil. The creator Orkut Büyükkökten visited Brazil in 2007, in an attempt to understand the success in that country. In 2007 Orkut began attracting large amount of Indians who were not intimidated by the number of Brazilians on the site. As for now, orkut also has a simplified site for mobile users.

5. Case Studies

Case studies were conducted with girls belonging to Chennai. Chennai is one of the metros of India and hence possess people belonging to various backgrounds and people all over India could be spotted in Chennai and hence has been taken as the place for study. Girls belonging to the age group of 16-22 share their experiences in Orkut and tell how the cyber crimes have made them more cautious in net and also how it changed their social networking.

Priya *22 years, final year, MA travel and tourism

Priya had nearly 500 friends in her orkut profile, many of them she already knew and some of them she came to know through orkut, and one such guy who called himself Shiva sent her a friend request, he was one of the members in her cute community'(She owns the community). He sent her a request saying that he would like to be her good friend and hence she accepted his request. He gradually started scrapping her everyday, he started to ask her very personal questions-which she did not like and so she took him out of her friends' list to avoid any further mishaps. In return he started posting bad and illicit comments about her in her own community, at first she did not notice it but later one of the members in her community, who is also her friend scrapped her about it. She was shocked to hear it first, she went to the community and deleted all his posts and banned him from the community.

*Names Changed

Before the incident, she did not follow any safety mechanism when she was interacting in social networking sites, and her knowledge of cyber laws in India was quite negligible. After the incident, she says that she has learnt that she should keep strangers at bay. She stopped accepting unknown friend requests and has started suggesting the same to her friends.

But, still she has not taken efforts to equip herself with the knowledge of cyber laws!

Koushika (20 years, final year, B.Com)

She calls herself an Orkut fan, she logs into Orkut at least 3-4 times per day. Once she had to scrap all people in her friends' list and invited them for some programme. To do the 'scrap all' thing, one has to join one of the many 'scrap all' communities out there and copy paste the code they give. Once it is done, it is possible to scrap all friends in the list in one go. One such of those communities asked her email id and password of her orkut account and she typed it down. The next time when she logged into the Orkut, to her shock she found out that her entire profile has been changed and illicit website URLs were posted in her profile page! For a minute she did not know what to do, later she changed her password and deleted all that was posted in her profile.

She did not take any special action, she just handled it herself, but she made all her friends aware of it. She says that she knows cyber laws are existent but she feels that they are not stringent enough in India as in other countries.

After the incident she learnt that she should not give her email id or password to anyone on the net, no matter how confidential they claim themselves to be and she started suggesting the same to her friends.

Tina: (22 years, currently undergoing air hostess training)

She has her orkut account for more than 4 years now and she used to post pictures in her profile. One day when she was browsing the net, she got a call from one of her friends saying that she had seen Tina's picture in a man's profile and asked her to view it immediately. She was stunned and immediately went to that profile. There in his album he had posted her picture stating that she is his girlfriend. She was shocked for a moment because she did not even know who this guy was. She did not know what to do and so she called one of her friends and asked her what could be done. Then, many of which specializes in the her friends scrapped him asking him to remove the picture immediately and cautioned that otherwise they would go to the police. That guy next day apologized to her through scrap and removed her picture.

Since she did not want to make a big issue out of it, she preferred not going to the police. Instead, she took the aid of her friends to resolve the issue! She knows about cyber laws but her scant knowledge made her thik it was only for very severe cases like hacking, phishing etc.

After the incident, her parents had insisted that she should not post her pictures and she also follows that safety mechanism in Orkut.

Rashmi: 22 years, final year, mass communication

About a year ago, her orkut profile was hacked by somebody and that person started sending obscene scraps to all her friends in the list. She did not know about it first and later one of her friends told her that she was receiving obscene scraps from her profile. She was shocked and immediately after going home she tried logging into her profile and was unable to do so. She then realized that her profile has been hacked and she immediately created a new account and scrapped all her friends about the incident and asked them to report abuse. After many abuse reports were filed, the profile was removed by Orkut.

She did not know about the cyber laws when the incident happened but now she says she is well aware of it. As a result, she stopped joining too many communities and stopped posting any personal information in her profile. She suggests the same to the girls who want to safeguard themselves on Orkut.

Gowri: (19 years, 2nd year, BE, ECE)

About 6 months ago when she was in college, her friend received a SMS in her mobile saying that she had received a scrap from Gayathri from orkut mobile services. At that time, she was sitting just beside that friend. Gayathri was shocked and did not know what to do. She went home and immediately checked her account and her whole profile was changed. It was alarming to her and she did not know what to do, so she deleted her account in Orkut. Later after a week she reopened a new account in Orkut.

She did not take any steps; the only thing she did was informing all her friends and asking them to be careful! She came to know about cyber laws only very recently.

She says that she really did not have any reason to get her account hacked because she did not post personal information or photos or videos but still got her account hacked. Hence she says the same can happen to anyone else. Now A days she is always on the alert and also suggests to others to be alert and monitor their profiles regularly! And she believes that a sound knowledge of cyber laws is needed to safeguard oneself on net!

Roshini: (22 years, completed B. Sc., Visual Communication)

Her scrapbook was available to public until that particular incident happened. Some two guys in Orkut suddenly one day started scrapping her obscene messages. She did not even know who they are. More over their scraps were in Tamil and she does not know Tamil. She got it translated from one of her friends. It was scandalizing to hear them and she felt bad of herself. She immediately put her scrap book to private, and deleted those obscene scraps. She sought her friend's help to track down who those people were; the friend lodged a complaint with the cyber crime officials. The officials tracked down the people who were doing this. They got to know that these people were doing this as a hobby with many girls' profile. They had them arrested and they were made to pay some amount of fine.

After the incident, she locked her scrap book, photos, videos and testimonials only allowing her name to be displayed. She also learnt that her safety is in her hands and she needs to monitor and control it herself without allowing anybody to disturb her!

6. Conclusions

The case studies reveal that the cyber crimes those girls have encountered in their interaction through social networking websites have made them more cautious and alert on net. But it is really saddening to know that only their own bitter experiences in Orkut have made them alert. They have not learnt from others' experiences or from whatever is portrayed in the media. Also, it is evident that Orkut has immediately come to their rescue whenever security problems were taken to their notice.

There exist so many other girls who were more affected by cyber criminals and who have undergone severe mental agony. They are not even in a position to share their cyber problems with others! Hence, the need of the hour is proper propagation of awareness to all the youth who interact through social networking sites, especially to the girls who are the most affected in Indian context. And this could be achieved only through a perfect co-ordination between the parents, teachers (who essentially need to guide the teen-agers on safety-related issues) and law-enforcement agencies. Both the cyber laws and cyber crime cells in India need to be scrutinized and strengthened further. The knowledge of cyber crimes and the means to escape from them should be strongly imparted to girls. Successful implementation of all these would definitely enable safeguarding girls in social networking sites such as Orkut.

REFERENCES

[1] Bagyavati (2009) 'Social Engineering' in Lech J.Janczewski and Andrew M.Colarik Cyber warefare and cyber terrorism pg: 182

[2] Bargavi and Sheeba (2009 November) 'Safety Issues in Orkut for Girls', Unpublished.

[3] Bradley (2009) 'Predators on Social Networks' http://netsecurity.about.com/od/newsandeditoria2/a/socialpredators.htm

[4] Brenner (2009), 'Social networking dangers exposed' http://www.networkworld.com/news/2009/020909-slapped-in-the-facebook-social.html

[5] Collier and Magid (2009), 'Social networking dangers in perspective', http://www.connectsafely.org/Commentaries-Staff/social-networking-dangers-in-perspective.html

[6] Everett (2009), 'Social networking - a risk to information security?' http://www.infosecurity-magazine.com/view/2503/social-networking-a-risk-to-information-security/

[7] Gonsalves (2009), 'Social Networkers Risk More Than Privacy' http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=219500360

[8] Joseph A L (2009, April 23) 'Man arrested for posting obscene profile of ex-boss on Orkut', The Indian express

[9] Krishnan. S (2009, March 21) 'Mumbai Police tie up with Orkut to nail offenders'. The Indian Express

[10] Kumar A (2008, May 19) 'Orkut used in credit card scam to buy airline tickets', The Deccan Chronicle

[11] Leyden (2006), 'Social networkers risk losing their identities' http://www.theregister.co.uk/2006/10/04/social_networking_security_survey/

[12] Muthalaly, (2007, June 12) Orkut users livid over demands for ban, The Hindu

[13] Nappinai (2010), 'Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study.in Journal of International Commercial Law and Technology Vol. 5, Issue 1 (2010)

[14] San Diego News (2007), 'Social Networking Sites Could Open Doors to Danger' http://www.10news.com/news/14557347/detail.html

[15] Satyanarayana (2009), 'Security Risks of Social Networking websites' http://www.brighthub.com/computing/enterprise-security/articles/9732.aspx

[16] Tan N (2008), 'Social networking: Danger - Warning for Teens'

[17] http://www.articlesbase.com/internet-articles/social-networking-danger-warning-for-teens-654816.html

[18] The Hindu Business Line (2007, Dec 19) Google in India's fast lane; Orkut fast rising search query

[19] Willard N E (2007) 'Social networking: are cyber teens in danger?' http://www.ivillage.co.uk/parenting/teens/teencon/articles/0,,186632_712646,00.html

[20] Zechariah, (2009, June 27), 'Man held for defaming woman on Orkut', The Indian Express