

CYBER CRIME AGAINST WOMEN- PRESENT SCENARIO

Ms.Ramandeep Kaur
Assistant Professor
PG Dept. of Computer Sc. & IT
Apeejay College of Fine Arts
Jalandhar

Abstract

The growing rate of usage of internet has helped individuals not only in betterment of livelihood, economical learning, entertainment etc. but at the same time this advancement in technology has led us to face the bitter side of it thereby introducing us to Cyber Crime. The objective of the study is to study growing rate of cyber crime against women in India and to analyze the reason of its growth. To authenticate the study, data from National Crime Report Bureau and World Bank for the year 2010-2013 has been used. The data available was only till 2013. The tool of SPSS has been used to show the association between internet users and cyber crime cases registered.

Key words: Cyber Crime, women , cyber stalking, cyber flirting , morphing.

Ms.Perna Pratham Singh, a final year M.A.(Political Sc.) Delhi University student, posted the screenshot (May,2015) ,on her Facebook page, of a lewd and abusive message posted to her by accused Raushan Kumar. With this screenshot, she posted a message too- which sent a straight message to not only the accused but to his alikes too. Within hours after Perna posted this message on her timeline, the accused tried to escape the situation by declaring that his Facebook account has been hacked and has been used by somebody else to send offensive messages.

Although Perna took a brave step to teach lesson to the culprit, but does every women have this much courage to fight against "Cyber Crime".

Introduction

In this age of technology, it is difficult to realize or conceptualize that whether this 'daily changing' face of technology is a boon or bane for us. With new software's, IT-enabled gadgets, Internet-enabled-easy to use-Applications, the technology is becoming an important part of our lives. Few years back, internet could be accessed only in few parts of country and only on desktop computers. Within a decade the scenario has changed completely. Now the internet is accessible on a tiny Smartphone or any handheld device. This has affected the growth of active internet users in an unexpected way. According to Internet Live Statistics 2014, around 40% of the world population has an internet connection today. In 1995, it was less than 1% which increased to ten folds from 1999 to 2013. The first billion was reached in 2005, the second in 2010 and the third in 2014. With around 200+ million active internet users, India has become one of the top three internet users in the world.

According to Singapore based Digital Agency (known for its APAC reports) out of 243 million active internet users 118 million are active on social media with 100 million active on social media via mobile. This mind boggling increase in the internet usage can be credited to availability of cheap handheld digital devices (laptop, tablets and smart phones), accessibility of internet (through WiFi or affordable data plans for mobiles) and awareness about social networking. The percentage of mobile internet users has grown more rapidly than traditional broadband users and it has led to increase in number of cybercrime cases.

Number of internet users and cybercrime cases registered in India

It is imperative to study the association between internet users and cyber crime cases registered under IT Act and IPC in India.

Table: Internet users per 100 people and cyber crime cases under IT Act and IPC in India

Year	Internet users per 100 people	Cybercrime cases under IT Act and IPC
2010	7.5	1765
2011	10.1	2975
2012	12.6	4398
2013	15.1	6454

Source: National Crime Report Bureau, World Bank

By using the tool of SPSS, the association between internet users and cyber crime cases registered under IT Act and IPC in India can be established.

Correlations		Internet users	cybercrime cases
Internet users	Pearson Correlation	1	0.991
	Sig. (2-tailed)		0.009
	N	4	4
cybercrime cases	Pearson Correlation	.991**	1
	Sig. (2-tailed)	.009	
	N	4	4

Correlation is significant at the 0.01 level (2-tailed).

There is positive and high correlation between internet users and cyber crime cases under IT Act and IPC in India. Since significant value 0.009 is less than level of significance 0.01 which means the association between internet users and cyber crime cases under IT Act and IPC in India is significant.

Moreover, the dependence of cybercrime cases on internet users can be analyzed through regression.

Coefficients ^a					
Model		Unstandardized Coefficients		Standardized Coefficients	Sig.
		B	Std. Error	Beta	
1	(Constant)	-3028.375	672.045		.046
	internet users	611.600	57.573	.991	0.009

a. Dependent Variable: cybercrime cases

The regression equation is $Y = -3028.375 + 611.600X$ in which regression coefficient is 611.600. Since significant value 0.009 is less than level of significance 0.01 which means the regression coefficient of cybercrime cases on internet users in India is significant.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.991 ^a	0.983	.974	325.720

a. Predictors: (Constant), Internet users

R square is 0.983 which is very high indicating that around 98% of the changes in cybercrime cases are due to changes in internet users and rest 2% changes are unexplained. Clearly data show that there is high dependence of cybercrime cases on internet users.

The impact of this increase in usage of internet has been both positive and negative. Where on one side it has helped individuals in better decision making, improved livelihood, entertainment, easy and

affordable learning, development of e commerce etc., on the other side it has also given birth to crime in the virtual world.

Online shopping, web browsing and social networking is few main usages of internet in India. Out of these three, social networking sites are a major factor which has prompted us to reconsider the implication of usage of these technologies in our daily lives. Facebook, Twitter, Google+, LinkedIn, Instagram, whatsapp, wechat etc. are influencing the way users maintain and cultivate a range of social relationships from close friendships to casual acquaintances. These social networking sites are used for making friends, chatting, sharing pictures and videos and read news etc. the usage of technology in this form has given birth to the ugly side of internet- the "Cyber Crime".

Cyber crime comes from the terms "Cyber" means internet and "Crime" which means harmful act. Therefore the cybercrime refers to any crime that involves a computer and a network. Criminal activities that specifically target a computer or network for damage or infiltration are known as cybercrime. In simple words, cybercrime refers to illegal activity committed on the internet. Cybercrimes have risen so dramatically in recent years that they are grabbing more attention worldwide as compared to conventional old fashioned organized crime. When the technology is on the side of cyber space offender and motivation is high, it seems difficult to put an end to such a crime.

Cybercrime includes (but are not limited to) email espionage, software piracy, hacking, frauds, spying, phishing, stalking etc. The study here has been limited to the various types of cyber crimes against women in India.

Cyber crime against women can be defined as any form of gender based and sexual-violence expressed through the use of internet and computer. Violence against women is being committed through the use of the media such as email, texting, Facebook, Twitter, LinkedIn, Youtube, chatting, Instagram etc. Although these platforms were designed for sharing information and communicating but miscreants are using them as a tool to humiliate shame or silence women with devastating consequences.

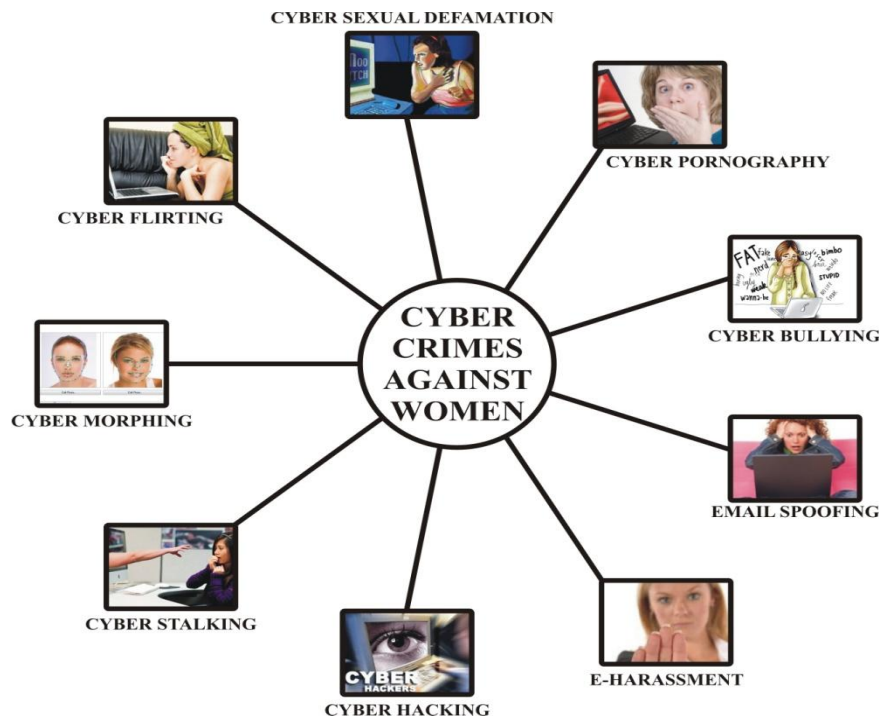
Reasons for growth of Cyber Crime against Women

1. The ease of access to internet, availability of cheap gadgets like Smartphone's etc, affordable internet data plans feed up the growth of Cyber Crime in India. This ease of access has increased peoples interest in using social networking and chatting etc. Also as stated earlier number of users using internet through mobiles has also grown rapidly and this results in their spending time more on "on-line" activities and thereby increasing the rate of cyber crime.
2. Apart from using internet at home or on handheld device, users at times use internet at Cyber Café's. These café's are at times not equipped with proper computer security software's (firewalls etc). The miscreants at times save passwords or hack emails of the users through these café's.
3. Women by and large shy away from reporting their complaints against cyber criminals as they fear negative media publicity and impact on family reputation. This is why cyber crime against women is on rise.
4. The law against cyber crime especially cyber crime against women is still in making. When India started framing India Information Technology Act it basically focused on need to protect ecommerce and related communications (and not crime related to socialization). The Act resulted in half baked law which manages commercial crimes and economic crimes but it did not focus on prevention of cyber crime against individuals. By the time Indian Parliament focused on cyber crime against individuals, the 'virtual world' had already created lawless situation. The

laws that were created to combat cyber crime especially against women created negative impact on women victims. Immediate media attention and attitude of the government reporting agencies made women victims helpless and traumatized. This hugely discouraged the reporting of crimes thereby worsening the Indian cyber crime scenario.

5. The recent increase in cyber crime against women can also be credited to busy life styles and loneliness. With changing life styles, women fall prey to social networking sites or chatting. They make accounts and profiles on these websites or chatting applications and start making friends. They tend to spend more time online without being aware of pitfalls of the cyber space. This makes them more vulnerable to targeted online attacks.
6. There is lack of 'cyber ethics'. Majority of individuals does not bother about policy guidelines (terms and conditions) to open accounts or for sharing data on various websites or applications. Without taking much precaution (like setting proper security settings for social networking sites) they start sharing personal information, sharing profiles, passwords, photographs etc. this makes them an easy prey to cyber criminals.
7. Majority of women are sensitive and emotional. They tend to share their passwords, photographs or personal data with their friends, boyfriends or partners. This also makes them more vulnerable to increasing crime in 'cyber space'.
8. At times, feministic perception and expressions on internet by women also pull them in to the dirty world of cyber crime. Hate messages, sexual or non-sexual teasing remarks, offensive comments by women are unacceptable by few people who then plunge into criminal activities against women.
9. Not only are criminals making or developing their own tools but they also use legitimate or publicly available software's such as to copy files, to share vulgar images, to morph photographs or to hack passwords etc.

Various types of Cyber Crimes against Women are:



Cyber-Flirting:

Cyber flirting generally starts when miscreant sends the victim obscene songs, videos or messages. This may later result in cyber sexual defamation.

In a recent Crime News¹ (Mid-Day, May 2015) a Mumbai cop is facing a complaint from an air-hostess for flirting with her on Whatsapp. A 21-yr old air-hostess complained against police sub-inspector of Nalasopora police station for flirting with her even after the victim objected over it. The victim had met the sub-inspector when she went to police station with her mother to register a complaint against a builder. It was around this time that the victim also applied for her passport and had given her contact number to the sub-inspector. The sub-inspector started messaging her on Whatsapp. He offered her coffee and kept on messaging her even after the victim had asked him to stop messaging her. Then the victim's mother has filed the complaint against him and investigation is going on.

Cyber Morphing:

Editing original picture by unauthorized or fake identity is Morphing. Cyber criminals download female's pictures (from social networking sites etc.) and again upload it after morphing. Most common victims to this crime are famous movie stars or famous celebrities.

Cyber Stalking:

This is one of the most common cyber crimes against women in India. In this miscreant follows victim's movements across the internet. Stalking social networking site of victim, or entering chat-rooms frequented by the victim, constantly sending disturbing emails to the victim are few examples of cyber stalking.

One such case (source IndiaForensic.com) has been of Seema Khanna (name changed) an employee with an embassy at New Delhi. She received a series of emails from a man asking her to either pose nude for him or pay him Rs. One lakh. The accused threatened that he would put her morphed pictures at sex websites along with her telephone number and address. After repeated threats through emails and letters, she was forced to report the matter to the police. It was later found that the accused had hacked her email account which enabled him to access her pictures and data.

Cyber Hacking:

Unauthorized access to one's data, profile, personal information, passwords or any such online activity is known as hacking. Criminals can change passwords or use this personal information for morphing or defamation.

E-Harassment:

Harassment via social networking site: in the latest case of harassment via a social networking site, a person has been nabbed by Mumbai police for blackmailing and money laundering from a female victim. As per Mid-Day Crime News (posted on 15 May, 2015), 27 year old Madan Prasad alias Amit Rai of UP befriended the married woman by sending her a friend request over Facebook. The woman accepted the request and began chatting on the website. Soon they became close friends and started seeing each other daily. During one of their meetings, Prasad shot a cellphone video of them in a compromising

position. The Blackmail began when women once refused to meet him. It was then Prasad told her about the video and threatened to send it to her husband or upload it on Facebook if she disobeyed him. Afraid of the repercussions, the woman gave in and gave him the money he asked for. This continued till her husband questioned about her fast-depleting bank balance. Then the victim revealed everything. A police complaint was lodged by the victim and the criminal was traced and arrested.

Email Spoofing:

This type of cyber crime occurs when the criminal sends a fake or fraudulent email to the victim. This email has pretentious details of sender so that the victim thinks that the email has been generated from a different source.

Cyber Bullying:

Harassing or harming other people in a deliberate manner is called cyber bullying. It includes posting rumors or gossips about a person on the internet bringing about hatred in other's mind thereby bringing defamation and humiliation to the victim. Many a times girls are cyber bullied by giving statements like "You are fat or you are ugly" on social media sites. This results in mental depression or anxiety, fear, loss of self esteem and isolation thereby at times leading the victims to commit suicide.

Cyber Pornography:

According to IndiaForensic.com, cyber pornography would include pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the internet (to download and transmit pornographic pictures, photos, videos, writing etc.).

One of the famous incidents of cyber pornography has been of the student of Air Force Bal Bharti School where a 16-yr old boy student created a website and hosted it on free web space. It was dedicated to Airforce BalBharti School and contained text material. On this site lucid, explicit, sexual details were given about various girls and teachers of the school. This continued till one day one of the boys told a girl featured on the site about it. The father of the girl, an Air Force officer, registered a case under section 67 of the IT Act 2000 with Delhi Police Cyber Crime.

Cyber Sexual Defamation:

According to Debarati Halder (an advocate and working as legal researcher) Cyber sexual defamation occurs when defamation takes place with the help of computers and / or the internet. Example someone publishes defamatory matter about someone on a website or sends emails containing defamatory information to that person's entire friends.

In a latest case of Cyber sexual defamation(source The Tribune,21 May,2015), a girl student of class XII of Kupwara (J&K) committed suicide after her classmate allegedly uploaded her obscene photograph on Facebook. The police has registered a case against accused under section 306(abetment to suicide).

Measures to be taken to avoid being victim of Cyber Crime:

Now days, cyber criminals indulge in cyber crime not only for expertise but for various other reasons like ego, hatred, money laundering, exploitation, betrayal in love etc. Although law enforcement agencies are trying to tackle this problem but growing and changing face of technology and our love for social networking makes it difficult for them to control it. To avoid being victim, women need to take measures to be safe in “Cyber World”.

1. One of the best ways to be safe is by making appropriate use of impenetrable security for your personal information and your devices (laptops, smart phones, tablets etc.). Anti-virus and security software's should be used for the same.
2. Technical solutions need to be developed which help in dealing with cyber crime. Applications for tracking cyber criminals, creating awareness of the issue among the women and cyber security methods to protect themselves should be developed.
3. Cyber criminals should be dealt with strictly. These cases should be highlighted in media thereby sending strong message that cyber crime is illegal and punishable act.
4. Government should frame and enforce strict laws against cyber crime especially against women.
5. Basic security methods like filtering emails, locking/hiding personal information, blocking miscreants etc. should be implemented by every woman while using emails or social networking sites.
6. Policy guidelines, terms and conditions should be read carefully.
7. Passwords should never be shared – not even to close friends/family.
8. Strict regulations should be maintained for cyber cafes. Proper records of the customers should be maintained.
9. In case of any suspicious activity, proper complaint should be lodged with the concerned authorities without any delay or fear.

Conclusion:

There is no denying fact that the impact of increase in usage of internet has been both positive and negative. On one side it has helped individuals in better decision making, improved livelihood, entertainment, easy and affordable learning, development of e commerce etc., and on the other side it has also given birth to crime in the virtual world. The association between internet users and cyber crime cases is significant. All over the world the usage of internet is ever increasing therefore the incidence of cybercrime inevitable. Women being soft-hearted, under stress and tend to trust others easily property – makes them more vulnerable to cyber crime. The need of the hour is that by taking various preventive measures we can reduce the increasing incidence of cyber crime against women. Although there are stringent laws against cybercrime but the problem is of implementation of these laws due to one or the other reason.

References:

- Nappinai N.S., *"Cyber Crime Law in India: Has Law Kept Pace With Emerging Trends"*, Journal of International commercial Law And Technology Vol.5 ,Issue 1 (2010).
- Malhotra Reema,Bhola,Gopal Chandra Mahakud, *"A qualitative analysis of social networking usage"*,International journal of Research & Development of Health: Vol 2(1):34-44,March 2014.
- Singh Jaspreet, *"Violence against women in cyber world:A special reference to India"*,International Journal of Advanced Research in Management and Social Sciences,Vol.4,No.1,January 2015.
- Agarwal Nidhi & Dr.Neeraj Kaushik, *"Cyber Crimes Against Women"*, GJRM Vol.4, No.1,June 2014.
- Shobhna Jeet, *"Cyber Crimes against women in India:Informatio Technology Act,2000"* , Elixir ISSN:2229-712X.
- Halder Debarati , Jaishankar K., *"Cyber Victimization in India- Survey Report"*.
- Iris Reyachav,Shraga Sukenik, *"Cyber bullying: Keeping our children safe in the 21st century"*.