Information Technology Miseries: Cyber Molestations Against Women & Children

Reena Hooda

Abstract: Developments in information technology greet the life with everything in hand, world within range of body area network and make the life fast, creative & efficient. Technology saves time & cost, connects the people, brings office at home. Automated tools for instance, robots work intelligently like a human being work in various circumstances, do home tasks, provide services in hospitals, work as a guide, help us & saves our life in hazards. We can pay bills online, feel forms online and do shopping online. However every good thing has a dark side also so the technology, specifically while using Internet that arise the question of privacy, security, threats, fears and still unanswered. All these are fall under the category of Cyber Crime specially target the women and children in age of 10 or above. Children generally abused online indulged through game playing, non-consensual pornography or blackmailing and many more. Wherever women attacked while looking for work opportunities, social-networking, hangouts, uploading personal images and get victimized easily in form of cyber stalking, harassments, frauds. Therefore, the present paper highlights the types of Cyber Crime, Cyber Attack, target victims, Indian laws and suggestions to handle such situation and conclusive the feasibility in Indian scenario.

Index Terms: Cyber Crime, Types, Threat for Women, Indian Acts.

1 Introduction

Cyber means anything relating to computers or electronic systems, information technology, Internet and virtual reality. It's a landscape with no boundaries, unknown linkage, no physical addresses and dynamic nature. Cyber Crimes means a crime that is performed on computers, through computers and even targets the computers that involve systems, networks for transferring data or targeting the victims. It is the technological attack that is so fast that never give chance to escape and seen only after being victimized. Example may contain the hacking personal information with any bad intention/ Goal, denial of services repeatedly, upload private information and make it public. According to CERT-IN (Computer Emergency Response Team, 27482 cases of Cyber Crime reported from January to June and reported after every 10 minutes in India. India has seen 1.71 lakh Cyber Crimes in past three and half years. According to Norton, 113 million Indians victim of Cyber Crime lost Rs. 16,000 on average. [1] [2] [3] [5] [6] The problem of Cyber Crime in India is more serious as here; handle birth rate of girl child is a big problem as Cyber Crime again adding the problem causes the violence, disrespect against women. So Cyber Crime is a big hurdle in women progress. India is a developing nation, women are less educated comparatively and less informed so get easily victimized. The distress is more than the physical violence against women. Same in case of the kids, they play on the systems like computers or phones, download the Apps, games while just accepting the conditions, don't know about the effects, thus get victimized through leakage of information or fall in to bad activities or harassed, brain washed without the knowledge of guardians. [1] [2]

2 Types of Cyber Crime

First is cyber stalking or bullying: when target is continuously followed by a person. Access all the information about the victim's online activities or send the messages continuously to the victim are fall under this category. Next is computer stalking that means unauthorized control over the system or accounts like email. Third is the pornography that involves the unauthorized display of pictures on social media. The list of the crimes is very vast and unpredicted. There are many more crimes that are listed as below. [3] [5] Morphing of Images: It is the technique of changing the original picture using sophisticated image editors. Some people do it for fun, some misuse the techniques of morphing and try to harm or defame the target. In morphing the picture or an image can be cut or other picture or subpart of the picture can be added that change the overall appearance or the meaning of the picture.

1 Shopping Frauds: Online shopping is the biggest target of the shopping frauds, in which your id are hacked, bank information stolen and cash withdrawal or the information can even be used to purchase by your id with intended address. Or moreover, you order is traced and replaced and you got the defected or unexpected items.

2 Dating Frauds: Youngsters are the highest target. They tagged into online dating, posting personal photos and later you found all the personalized information is public and you are spoiled.

3 Email Frauds: Now a day's email contains everything, your synchronized contacts from phone, bank account information, aadhar card information and other personal data. Though two step securities are provided by the service providers like Google offer, Google message the user if login from different user, if new mail or any changes made, even than email can be hacked through sending the hacker link. Unauthorized messages can send from the mail or may be dangled in cyber bullying.

4 Discount Coupons or Lottery Frauds: We tangled in the free schemes but nothing is free in this world, you are stirred to put your online money transfer id on the link and you will be bared.

- *Dr. Reena Hooda, Assistant Professor. Indira Gandhi University Meerpur (Rewari). Haryana (India), E-mail: reenah2013@gmail.com*

5 Information theft: It is also fall under the category of cybercrimes, unauthorized access to someone's information, or chasing anyone, collecting information regarding the activities on the network, links he or she open, friend list or any type of attempts revealing the privacy is the type of cybercrime.

6 Taking unauthorized picture of body parts, revealing the privacy moods are the biggest crime that is done by hidden cameras connected with the networks.

7 Cyber Attack are new methods for crashing the country's economy that doesn't need any army or arms and done in seconds. [3] [5] Now days with the advent of ICT (Information Communication Technology), everything in advanced economy is connected via network that can be penetrated and make the whole economic system down, that generally make the electricity cuts, create problems in healthcare while doing critical operations, or preservation of biomaterials like stem cell or other organs will be spoiled with even a few minutes crash. Military services can be stopped, or security data can be hacked without any use of physical or biological attacks.

3 Role of Information Communications technology in Cyber Crime

Technology is not an entity that can affect anyone itself. It is up to the user of the technology the way he or she is employing it. Information communications technologies connect us with the universe; provide lots of information which can enhance over knowledge and life styles. Communication network have the major threats of leakage of information over the networks by the intruders or the hackers. We personalize data while on social networking sites, if hacked and misused; caused lots of tensions, fear, demoralize, negativity, doubts and loose of confidence in personal relationships. So there should be common ethics about the use of ICT and standard must be formed to secure the faith of ICT users. [6] Laws are not enough to trace the crimes or protect the victims. The attackers of the Cyber Crime are anonyms means the address or identity even location of attack cannot be easily identified. Cybercrime is one of the biggest crimes evoked due to enhancements and extreme use of ICT. The potential for child pornography, prostitution, scams, hacking and theft of data, burglary by the bank account fraudsters, terrorist activities, government check and monitoring on the various sites, companies for hidden data analytics and more over human trafficking specially children involvement in drugs dealing; are at growth with the growth of ICT in developing countries or backward areas. All these ICT based crimes are due to absence of proper laws against crime, government insufficient provisions, lack of basic knowledge among the users of ICT and money grid for sudden richness. [8] [9] [10] The basic cybercrimes due to ICT are by cyber criminals for stealing information, second is the spying for gaining intellectual property rights and other is the Cyber war that is military or politically moved. [8] Making faster payments, daily use of ATM, credit cards are also targeting by the criminals and terrorist for illegal transfer of money from unauthorized bank accounts or across the economic boundaries. [9] [10] ICT help in education, acquiring more knowledge about the topics without spending money on books or going physically to the library, everything including libraries are on system. However, also increasing chance of indulging kids in cybercrime as an attacker or as a victim and risking them by permitting them to sit on net, a regular check is must to ensure the safety and prevent the cyber risks. Use of mobile phones, smart watches help kids to be connected every time also charted them to connect to unsafe network, they are more chased by the trespassers than parents and inversely motivated as compared to parents. In largely populated areas, individuals are more targeted than the computer system, after getting background knowledge about individual, criminals make attempts to force them to be involved in crimes and other social ills and intimidations. [10]

3.1 Reasons for growth of Cyber Crimes against Women & Children

Development of society is dependent on the growth of women and their safety as she is the building block of the family and reputation in the society. Children are the future of the family and country, they are innocent, uninformed thus an easy and key target of the criminals. Developing country like India, where the technology and development in growing stage, there is more chance of menaces with fewer provisions to tackle with the problems, following are the reasons for the growth of Cyber Crime against women and children.

1 Decreasing cost of equipments and universal nature of Cyber that is mysterious, unsolved, boundary less, unknown and changing frequently.

2 In metro cities in India, the prime cause of become internet edict and get victimized of Cyber Crime is the Loneliness as students and working staff live away from family and work for long hours on the computers. Thereby computer and Internet becomes their trusted mate.

3 Discounts are favorites of female shoppers; new trends watching and being unique and fashionable icon thus go for free trials, online discounts and schemes and lost privacy in ignored transactions.

4 Online work Opportunities (grid for Young Girls)

5 Watching online videos, Uploading personal videos on YouTube.

6 Use Drive or Cloud for storing personal data or photos

7 Jealous

8 Google Hangouts and Synchronization with email or social networking accounts like Facebook.

9 Changing definition of advance

10 Official Victims (especially in companies)

11 Increased use of Internet of things.

4 Discussions and Suggestions

It's not feasible to survive in a world of isolation and without information technology and advance tools for different tasks. Social networking is vital for information sharing and gathering and to involve in group of intellectuals and for different social benefits. It's the human nature, attitude & behavior to use beautiful gazette for different motives. Such hazards can never be removed from the society; however can minimize the potential of victimized of unknown threats like cybercrime. Government always tries to minimize the risks of such crime through different campaigns, police force and various awareness schemes for women and children safety, even various private telecommunication companies start offering different apps for female securities free of cost. Besides these to prevent such crimes or to tackle with such problems if occurred, following are the suggestions:

1 Uploading of family pictures on computers or clouds should be avoided that are commonly used to connect and with different profiles on Internet.
2 While in hotel or in changing rooms of malls, ensure to check for a hidden online spy cameras or instruments.
3 Ensure there is no hidden camera in room where you sittings or there is no webcam on in your room or mobiles video on while you discussing something private even if web cam is not in use. Check your friend phone also when talking personal that is not on recording or try to switch off the phone.
4 Putting personal details on Facebook, Google+, LinkedIn, or other social networking should be avoided as it might get misused. Personal details like hobbies, work place, educations and friend circle on public platform may increase your problem.
5 Always make two kinds of online presence i.e. a professional presence for your colleagues and a private presence. Use dummy profile photo and details while connecting social media that is not secure enough.
6 Install filters in your computer in order to prevent children from insecure accesses.
7 Do not become edict of online shopping or payments online. It is better to be social and go to the branch for payments. It will be good enough to select cash payment options in place of online payments.
8 Put the spy software to track the kids or activities performed on your systems.
9 Most of the Cyber Crimes are listed under the Information Technology Act (IT Act), 2000, which was amended in 2008. The various sections of the act specify the types of the crimes and their punishment in form of money or imprisonment etc. so contact to local Cyber Crime cell that will take necessary action like blockage of site or filing case against the liable. [4]

5 Conclusions

Though the law helps a lot but it is a solution after the problem. Try to prevent the problem by getting aware and awaking the friends or family circles. Don't feel shy of discussing the things or afraid of revealing the personal information. The Panchayat system or honor killing however make the problem bigger and some crimes are not get revealed because of fear of society. Awareness camp should be organized to teach children in the schools or people in villages or in women colleges about the Cyber Crime and possible hazards and suggestions for handling such problems.

References

[1] https://en.wikipedia.org/wiki/Cybercrime

[2] https://www.techopedia.com/definition/2387/cybercrime

[3] https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html

[4] http://www.cyberlawsindia.net/

[5] http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html

[6] https://www.osce.org/secretariat/cyber-ict-security

[7] https://www.sipri.org/yearbook/2016/10

[8] Barry B. Hughes, David Bohl, Mohammod Irfan, Eli Margolese-Malin and José R.Solórzano (2017). "ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance". Technological Forecasting and Social Change. Volume 115, February 2017, Pages 117-130. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0040162516303560

[9] Olumide Longe, Oneurine Ngwa, Friday Wada, and Victor Mbarika (2009). "Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives". Journal of Information Technology Impact. Vol. 9, No. 3, pp. 155-172, 2009. Retrieved from: https://www.researchgate.net/publication/228876250_Criminal_Uses_of_Information_Communication_Technologies_in_Sub-Saharan_Africa_Trends_Concerns_and_Perspectives

[10] University of Twente (2013). "ICT plays an increasing part in criminal activities". Retrieved from: https://phys.org/news/2013-04-ict-criminal.html