IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"A Study of the awareness level on Increasing Cyber Crime against Adolescents in Delhi Govt. DIETs"

Ms.Neha Sharma, Lecturer

DIET Daryaganj

Abstract:

Cyber-crime is a global phenomenon. With the advent of technology, cyber-crime and victimization among teenagers are on the high and it poses as a major threat to the security of a person as a whole. Even though Information Technology Act 2000 is functional in few countries including India in order to combat Cybercrime, issues regarding Cybercrime against adolescents still remain untouched. The cyber-crime pose a great threat to individuals. Cyber-crime is a global phenomenon and young teenagers are the soft targets of this new form of crime. Being a victim of cybercrime could be the most traumatic experience as many individuals especially teenagers feels uncomfortable to report such issues. This paper will deal with the meaning of Cybercrime, reasons of cyber-crime and the suggestions to overcome such issues.

Introduction:

Technological advancements in the field of communication is growing at a faster pace that is developing a communion among the people. Internet has become an urgent need in today's world that many of the people are totally dependent on it by it using it for some informative purpose or be it in creating a network of social well-being in the virtual world. As the human civilization progressed or the worlds of technologies like information revolution leads to some challenges in the form of Cybercrime. It is understood as a crime committed via computer (hacking, phishing, spamming, child pornography, hate crimes). Criminals may use computer technology to target personal information, business trade secrets or use the internet for exploitative or malicious intensions. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime. Cybercrime is often intended to be performed in order to target people especially the Females with a general motive to intentionally harm the victim while using modern telecommunication networks like Internet through Chat-Rooms, E-Mail, and Social Networking Sites etc. and even through Mobile Forms in the form of SMS / MMS.

It is also done via voicing showing to be genuine organization like of banks asking to dial a number and enter your account detail. So there has to be a caution which is not to disclose secrets to anyone. To this banks are reporting from time to time the advisory in the form of caution. So this can be preventable if proper awareness is spread among the masses. One has to be smart to not to get trapped in the virtual world of crime.

In this modernized world the perpetrators are gradually misusing the cyber platform in order to harass and abuse women and children for voyeuristic pleasures. At young ages there is an increase in reports of intimidation, harassment, intrusion, fear, and violence experienced through Information Technologies (IT). Hacking, spamming, identity theft, child pornography, cyber bullying, and cyber stalking are just few examples of cyber-crimes.

Today's teens form part of Gen Z, young people who were born and raised in the new technology era, who cannot envisage an offline world with no access to the Internet or social media. From an early age, they have juggled with computers, tablets and smartphones, accessories they use in their daily lives. In tandem, data also evidence that cybercrime is increasingly attracting and engaging with the teen population.

Categories of Cybercrime:

Broadly classifying the various categories of cybercrime that are being prevalent are:

- Harassment
- Hacking
- Phishing
- Identity Theft
- Password theft
- Stalking
- Spamming etc.

Harassment: Internet harassment, also referred to as "cyberbullying", is the term used to describe the use of the Internet to harass, threaten, or maliciously embarrass. It can involve behaviors such as:

- Sending unsolicited and/or threatening e-mail.
- Encouraging others to send the victim unsolicited and/or threatening e-mail or to overwhelm the victim with e-mail messages.
- Sending viruses by e-mail (electronic sabotage).
- Spreading rumors.
- Making defamatory comments about the victim online.
- Sending negative messages directly to the victim.
- Impersonating the victim online by sending an inflammatory, controversial or enticing message which causes others to respond negatively to the victim.

- Harassing the victim during a live chat.
- Leaving abusive messages online, including social media sites.
- Sending the victim pornography or other graphic material that is knowingly offensive.
- Creating online content that depicts the victim in negative ways.

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. With the prevalence of social media and digital forums, comments, photos, posts, and content shared by individuals can often be viewed by strangers as well as acquaintances.

Cyberbullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it. Cyberbullying has unique concerns in that it can be:

- Persistent – Digital devices offer an ability to immediately and continuously communicate 24 hours a day, so it can be difficult for children experiencing cyberbullying to find relief.
- Permanent – Most information communicated electronically is permanent and public, if not reported and removed. A negative online reputation, including for those who bully, can impact college admissions, employment, and other areas of life.
- Hard to Notice – Because teachers and parents may not overhear or see cyberbullying taking place, it is harder to recognize.

Hacking: In this computer data is exploited without the knowledge or permission of user. These people are good at computer programming and knowledge and they do it for the wrong reasons. Having good skill on computers to show off about their expertise they manipulate with the program and may inadvertently cause destruction. Greed and voyeuristic tendency make them to do this.

Password theft: This is to tamper with website to find out concealed information. The thief search the FTP information passes it top their system to be exploited later on.

Cross site scripting: Another way to interfere in the security system via infecting website with malicious Client side script. It is against HTML, Java or flash. Against this a firewall has to be installed in order to prevent unwanted network.

Virus: These are programs that attack file and damage them and have the tendency to spread to other computers. Thus computer operation is affected. Worms are self-replication malware jamming the computer processor system. Some the well known viruses are like Trojan horses. This comes along with games download. It can hamper the working of the computers. In fact this virus is put in the chain of commands unused for the specific purposes. Sometimes it is

added in the startup of the computer. This is a virus infecting the files and folders. The two types of virus are mentioned herewith- Those only disseminate and do not cause damage and those which can disseminate and caused damage. Thus memory space is also engulfed and computer becomes slow down. For that anti-virus are created to take care of them to prevent economic fallout.

Stalking: It is following a person online following his/her on line activities to get some personal information and harass him and make threats. It happens through internet and other electronic means. Most victims are woman and children who are not aware of internet safety. These people are sometimes stranger and sometimes known to you. The stalker harasses their victims via mail, chat. The free e-mail and the anonymity provided are the reasons of increase of crime rate. The information available online about a person can be misused. It is of two types either internet or computer. It has now gone further to social networking such as face book, twitter and you tubes photo and status updated. Giving personal information on social media could be the point of problems which are exploited. Thus too much of interactive habits allowing the crime to flourish.

Spamming: It is sending huge volume of emails leading to server crash. The message is meaningless and long sent for consuming the network resources. This happens when security is compromised by malware. This difficulty is to be checked as they are sent from different sources. By not responding to these one can limit this otherwise it may spread like anything. Sending spam is the violation of internet norms. If the system become slow suddenly it means that large chunk of material has come that is under process.. To avoid that is to block the particular incoming packets from that address.

Research Study:

A research study was conducted to know the general awareness of teacher trainees of District Institute of Education and training (DIET, Daryaganj,N.Delhi).

Sample of the study: 200 D.El.Ed. Teacher trainees of District Institute of Education and Training (DIET) Daryaganj. The Questionnaire was administered among girls and boys of D.El.Ed course of DIET.

Tool of the Study:

A Questionnaire was formed to know the awareness about cyber culture and crime. The questionnaire comprised of 3 Parts to check on various grounds.

Result Analysis:

Table-1: Analysis of Part-A

QUESTIONS	GIRLS		BOYS	
	YES %	NO %	YES %	NO %
Are you using social media	100	0	93.3	6.7
Should you opt for privacy option	91.8	8.2	73.35	26.6
Would you like to prefer for public from fringing the privacy and copyright while using social media	6.1	93.9	46.6	53.4
If you harassed by anyone on any means of social media, would you like to report to police?	89.7	10.3	73.3	33.3
Are you aware of Information technology Act 2000?	36.7	63.3	26.6	73.4
Are you aware of Criminal Intimidation and punishment for the same –Section 507 of Indian Penal Court	18.3	81.7	26.6	73.4

Table-2: Analysis of Part-B

QUESTION	GIRLS		BOYS	
	YES %	NO %	YES %	NO %
Knowledge of minimum age to join cyber communities like facebook, orkut, Myspace etc	77	23	86.6	13.4
Allow others to use one's own e-mail id/profile id/passwords etc	14.2	85.8	6.6	93.4
Use safety tips like filteringemails,locking personal albums,and information,personal wallsof social networking sites etc.	91.8	8.2	60	40
Mail back to unknown senders of spasm/pornographic/erotic/phising mails	10.2	89.8	86.6	13.4
Share personal information/emotionswith virtual friends/chatroom partners etc whom you don't know in real life	14.2	85.8	13.3	86.7
Believe in controlling free speech while communicating in the cyber space	42.8	57.2	60	40
Read policy guidelines of social networking sites,ISPs etc	55.1	44.9	33.3	66.7
Use psedo names	14.2	85.8	0	100

Table-3: Analysis of Part-C

QUESTION	GIRLS		BOYS	
	YES %	NO %	YES %	NO %
Aware that hacking,creation of pornography/distributing the same,distribution obscene materials are criminal offences	77.5	22.5	80	20
Aware that cyber bulling ,cyber stalking,sending annoying ,defaming messages etc can be panelized	79.5	20.4	66.6	33.3
Has reported incidences of cyber victimization to police/lawyers/courts	8.16	91.8	53.3	46.6
Aware of legal right to protect /privacy in the cyber space	61.2	38.7	73.3	26.7

It is evident from the study that:

- The biggest mistake that most of the Youngsters make is ignorance of the safety Tips that usually comes under various Heads as well as Pop-Up Windows.
- Many of the trainees were not aware of the Information Technology Act 2000 and that's why they are even not aware of the Punishment that the culprit has to undergo if arrested.
- Usually most of the youngsters mail back to the unknown mail senders without realizing that they may be a threat to their life as well.
- Virtual world has become an identity to the youngsters. In this virtual world of Technology, many of them share their personal information in one go without knowing the person at the other end.

Solution and Prevention:

From the study it is evident that the individuals do know about cybercrime but they are generally not aware of the different modes of conducting the crime via computers. Everyone in the age of technology and especially in the world of Social Networking uses a number of sites but due to their mere negligence becomes trapped against such monsters that are always ready to exploit the women. Awareness about the Information technology Act 2000 is much needed to be promoted in the society so that such victims are not been exploited by the invaders. The best part of the study was

that if anybody becomes victimized then they are ready to get the case reported in the Police and follow the legal formalities.

In response to this various solutions can be made functional which can put a stop to such a crime. Few suggestions of prevention which was felt are as follows:

Strict Laws: There should be strict laws for cybercrime against women. Laws are made for cybercrime such as information technology Act 2000(amendment 2008),Section 507 of IPC,S-509 punishment for harming the modesty of women,S-499 and 500- for defamation and punishment for the same,S354-D –punishment for stalking of the IPC may be used for posing intimidating, insulting, defamatory comments, stalking and creating threats. Some other sections are 66-punishment for computer related offences, 66-C punishment for fraudulently using password, 66-E-violation for cheating by impersonation, Section 67 for sexually explicit contents. Laws are made for cybercrimes however more strict laws should be made for crimes.

Awareness among Young Girls: One of the reasons of increasing of cybercrime is that laws are made but awareness amongst people are less. Many of the young girls and boys are not aware Prevention is better than cure is an old saying.

Strict Punishment: Strict actions need to be taken against the culprit in order to put a halt to such offenses in the society. If the society becomes fearless and reports the cases to the Judiciary on time, then the ones who are exploiting can be punished.

Strict Regulation of Cyber Café: Many of the offenses in the category are made in the Cybercafé whereby sometimes mere negligence at the part of the owner can put the life of the victim at risk. Many of the cybercafe owners don't take the Identity Proofs of the persons who are visiting and using the computers in the café and such persons are always in a look to overcome this situation.

Accompanying/Support the Victim: The victim needs support from the family and the society in order to overcome the situation that she is going through. It is really disgraceful that the society instead of supporting/ sympathesising the victim, always looks for a teasing situation to enjoy.

Mothers/Teachers Counsel Young Girls/Boys: Parents also needs to be aware about the cybercrime and counseling their children regularly so that they neither become the culprit nor becomes the victim.

Beware of Surveillance at Public Places: One needs to be more attentive in Public Places of being victimized. For example: It is being reported that in Metro most of the Girls are being filmed by certain type of intruders. They usually don't let anyone know that they are doing an offense as in public places most of the people are behaving casually and enjoying whereas the stalkers are in a move to take advantage of such soft target.

Capacity Building Workshop/ Online Short Term Courses: This step can be a boom in the field of cybercrime as the awareness among the youngsters as well as the Senior Citizens who are also on the verge of getting victimized must be oriented with certain kind of refresher/ short term courses in order to get equipped with the situation and getting themselves safe from this crime.

Cyber safety Awareness Camps: This step can be done in association with the various Resident Welfare Associations as well as various NGOs who work in the Slum Areas to make them aware of the situation.

References:

- Cyber stalking India, www.indianchild.com.
- Cybercrime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27 IST
- David Wall, "Cyber crimes and Internet", Crime and the Internet, by David S. Wall. ISBN 0-203-164504 ISBN 0-203-164504, Page no.1
- en.wikipedia.org/wiki/Crime
- en.wikipedia.org/wiki/Phishing
- Jain, Neelesh & Shrivastava, Vibhash & Professor, & Professor, Assistant. (2014). "Cyber Crime Changing Everything – An Empirical Study". 4.
- Kabay, M. E. (2000). Studies and Surveys of Computer Crime, Focus. http://securityportal.com/cover/coverstory2001211.html
- Sharma, Ushamary & Ghisingh, Seema & Ramdinmawii, Esther. (2014). A Study on the Cyber - Crime and Cyber Criminals: A Global Problem. International Journal of Web Technology. 3. 172-179. 10.20894/IJWT.104.004.001.003.
- https://shodhganga.inflibnet.ac.in
- The IT Act 2000.