IMPACT OF CYBERCRIME ON WOMEN, YOUNGSTERS AND CHILD

Kshama V. Basarkar (Dharmapuriwar)
B.A, LL.B., From Nagpur University,
MCLIT From Gondwana University, Gadchiroli

ABSTRACT:

Cybercrime is the newest and the most complicated problem in the cyber world. Cybercrime is basically an illegal act in which computer is either tool or target. After the development of internet, anybody can have easy access of data and information from all over the world. But instead of taking benefits of internet, some people are misusing of computers and internet for crime such as cyber pornography, cyber stalking, email bombing, virus attacks, web jacking etc. Other than these crimes, offenders use the cyber world for child abuse which is also a kind of cybercrime. Violence and harms against children and young people in cyberspace and in relation to new technologies include: The production, distribution and use of materials depicting child sexual abuse, Online solicitation or 'grooming' (securing a child's trust in order to draw them into a situation where they may be harmed), Exposure to materials that can cause psychological harm, lead to physical harm, or facilitate other detriment to a child, Harassment and intimidation, including bullying. Children are the newest victims of cybercrime. Offenders use illegal activities such as online grooming against the children to make their victim. The computer and internet are being used to commit crimes against the children such as child exploitation, production, distribution, and possession of child pornography; exposure to harmful content; grooming, harassment, and sexual abuse; and cyber bullying. Research papers discussed about the connection between a child and the cybercrime, how cyber offenders use the cyber world to abuse the children. Some preventive measures are also discussed at the end of the paper.

Keywords : *Cybercrime, child pornography, violation of priviacy,online sexual harassment, online child traficiking.*

INTRODUCTION :

Nowadays, email, websites, online applications are the means of communication for every individual. It helps us exchanging and circulating data, images and other variety of materials. It is altogether a helpful material but undesirable information also. These all start from inventions in information technology that, to increase new economic and social opportunities post difficulties to our security and prospects of privacy. These days all of us as individuals are already interconnected with the IT. Everybody uses devices and the smart digital gadgets. All the social systems are now fully connected as the "internet of things". In this generation, the quality of life is improving through Information Technology. The framework is getting automatic. Safety and privacy, these are the two major challenges. Interruption and the illegal connection can be made through attacks. In this current online generation of cyber threats, a giant number of cyber threats and its impact along with understanding is crucial to inhibit at the initial stage of the cyber-attacks. The United Nations, for analytical purposes, describes "youth", as those individuals between the age group of 15 and 24 years, without biasness to other definitions by member states almost 27.5% of the Indian population is comprised of the youth in the age group of 15–29 years. It is also seen that online risks such as addiction, cyber bullying, sexual solicitation is combine with negative result for the youth. It is very important issue to note that not all the children Information Technology users. Describing youth with the age group is one of the easiest ways in equally susceptible

and more research is necessary to find out the youth, most at risk as well as to develop effective interventions behavior. From last few years, it has been observed that there has been 53.5% rise in the Cyber Crime. According to a report many cyber criminals were arrested, who were mostly the young adults. Out of 324 people arrested under the IT Act, 215 were from the age group of 18–30 years. The major cause of increasing crime rates amongst youth is the 'easy money'. The greedy and attention-seeking behavior of today's youth leads them to commit heinous crimes. The more disturbing facts on the crime sheets are young and qualified teenagers even get involved in doing of such atrocious crimes. The rate of crime amongst youth has increased to 40% and almost 56% of the crimes are done by youngsters between age group 16–25. The traceable young and reasons are far from the obvious but majorly such worrying figures are contributed due to: 1. Easy Money 2. Unemployment 3. Fitting into the group 4. Lust for attention

But blaming the youth for all of it will clearly be wrong. Youth, at most times, in such cases are themselves victims. Many qualified young criminals are drawn to committing crimes due to scarcity of jobs. Also, peer pressure plays a negative role, which leads teenagers to earn money in easy ways, show-off and try to gain attention by buying expensive gadgets. The upbringing, lack of time provided to youngsters has led to most of the youngsters to be drawn towards the wrong path. There is not one but many ways to put a stop to let youth destroy their and nation's future.We are in dire need for a better education system, huge modi cations is called for in terms of upbringing and social awareness. Youngsters are a sensitive and tender group and need to be dealt with better care and protection. They need time and protection. They need time and behavior, need to be talked out with the help of love and care. It does not guarantee that no offending by youth will be considered or committed but reduces the risk to a minimal level. Stringent law enforcement, better judiciary setup can discourage youngsters from committing such crimes but why wait for others to better your world when you, yourself can take a step more and stop it from being.

What and how Much do We Know about Cyber Crime?

Cyber Crime is an international issue now, no country is exempt. The first Cyber Crime was committed in India, Japan and China in 1820. One of the most important problem is Pornography, under Section 67 of the Information Technology (IT) Act, 2000 making, transmitting and distribution of cyber pornography is an offence. However, browsing and viewing online pornography is not punishable. Making, distributing and even browsing Online Child Pornography is punishable under cyber laws. There are almost 1,00,000 websites that are offering illegal Child Pornography. In Bhopal, a youth was arrested for being a member of WhatsApp group that shared videos of child pornography, the crime branch found many messages sent in "code word" demanding child pornography content from the accused.Cyber Crime is the form of crime where internet connection or computer is used as instruments to commit this crime. Some of the causes which affected to commit a Cyber Crime like quantity to store the data in small space, easy to access, complexity to do work, negligence and loss of evidence. Some kinds of Cyber Crimes are mentioned below:

• Crackers are those individuals who are virus creator. Hackers are the one who explore others computer system for education. Pranksters are individuals who attempt tricks on other. Career criminals are individuals who earn their income crime. Harassment is the cyber bullying that occurs through the internet.

• Computer spams refers to unsolicited commercial advertisement distributed online via e-mails/which can sometimes carry viruses and other programs that harm computers. Restriction of Cyber Crime is dependent on proper analysis of their behavior and accepting their impacts over different levels of society. Therefore, Cyber Crimes understanding in the current era and their effects over society with the future trends of Cyber Crimes are explained.

• What and how Much do We Know about Cyber and accepting their impacts over different levels of society. Therefore, Cyber Crimes understanding in the current era and their effects over society with the future trends of Cyber Crimes are explained.

• One more type of cybercrime is Phishing. It is just one of the many frauds on the internet world. Phishing is an electronic fraud that is tactic in which individuals are tricked into revealing their personal nancial information to an unauthorized entity. A phishing attack can be handled by voice e-mail, or landline or cellular telephone. In Kolkata, the death of the young 17-year-old student due to cyber bullying might be an extreme case but Cyber Crimes are on the rise in this city that a recent TCS study has claimed is addicted to Facebook – an high of 85% of teens have an account there.

RESEARCH METHODOLOGY :

Whole research process is defined and delivered in a systematic order. It carries comprehensive literature view, survey-based research, from Ebsco, Emerald, Scopus, Jstor, Thomson Reuters and Google Scholars. This present paper is based both on primary data as well as secondary data and information. To get this primary data from the root source, the systematical questionnaires were prepared for offenders. The number of offenders were 1000 youth from different states of India. Social Networking Sites. The most popular social media sites like Facebook, Twitter, Instagram had

studied the views on trust and privacy concern regarding the sharing of information and new relationships. It is very clear that there is no much difference as privacy is concerned. It was found that most of the famous members were willing to share information. These views suggest us that given in any social media platform, privacy and trust do not matter when exchange of the information or relationship building between the members is concerned. Study shows that involving adults also use the social networking sites to connect with family and friends and the pattern disclose that they use online to reinforce their disconnected folks. According to one of the major factors, people join social networking sites. One of the top reason experiences to violence has an adverse effect on youth mental vigor, academic presentation, and interactions. They proved that youth violence, together with victimization, mob violence and self-directed violence, more and more occurs in the virtual space. Some methods of online violence are inadequate to internet-based relations; other are directly related to head-on acts of violence. In Bengaluru, College Principal's name misused in E-mail scam; A fraudster who created an e-mail account in the name of the principal of St. Joseph College autonomous, which was used to send a mail asking for a donation for a charitable cause.

What Motivates Some Young People to Become Cyber Criminals?

We all know that the cyber criminals are always searching for financial gain, but it looks that this is not generally what Young cyber criminals have in their mind when they take their first step over to the 'dark side 'For example: An appealing report by the National Crime Agency (NCA) UK found that many are not necessarily motivated by financial reward. Generally, perceptions from their peers, popularity in the forums they belong to, and a sense of success, are bigger influencing factors. "The sense of

OPEN ACCESS

achievement at completing a challenge, and justifying oneself to peers are the main motivation for those who involved in Cyber Criminalities. "This report includes the evidence given by an 18 year old who was arrested for an unauthorized access to a government website. At the same time of his arrest of the child he said, "I did it to impress the people in the hacking community, to show them I had the skills to pull it off… I wanted to prove myself."

Cyber Crimes and Its Impact on Youth, children's and woman's

Studies proved that more and more effective policies and plans can be established to policies and plans can be established to teach the youth and individuals about defending themselves while online. Youth should be careful of who they are communicating with online and refrain from as long as any type of personal information to persons they do not identify and trust. And more analysis of the access of social networking websites and the false action of the youths, as well as their knowledge with misleading internet practices, will spread awareness of the online activities and practices of teenagers. With this perspective, better safety and security measures and strategies can be established to keep the teenagers safe online. The study analyzed that Cyber Crime, which has grown into major issue within the last 2 decades. Youth societies are more likely to be the targets of the Cyber Crimes. In addition to age, the other aspects which includes Gender, Education, Financial status, and Forceful Victimization that relates with the Cyber Crimes victimization. Right offline social networks were a defending aspects against the Cyber Crime harassment among the females. The young Cyber Crimes games were more likely to be disturbed about the future harassment. In Delhi, Youth Flees With Iphone To Make Tiktok Videos; A call centre employee, who escaped with an Iphone to make the better quality Tiktok videos, was arrested during a

vehicle check at Vikas Marg, the police said. The complainant had posted an advertisement regarding sale of Iphone on an online site. He got a call from a potential buyer and he agreed to meet him near Preet Vihar Traffic Signal. After reaching the location, respondent borrowed the phone from the complainant, diverted his attention and sped away with the phone.

The internet has connected the world. Due to social media, happenings from every corner of the world reach us in just a few moments. Now this social media is trying to become a weapon of persecution. It mainly affects young women, children and men as well. Cyber crime is becoming a hot topic day by day. Street criminals have turned to cyber crimes as this sector has become more and more used in daily life. Social Media i.e. Facebook, WhatsApp, Instagram, Twitter is 4G…

Women and Children in Cybercrime is Open fields are becoming open for criminals. With all the crimes like banking fraud, fraud from marriage matching websites, sending fraudulent e-mails, social media as a whole is becoming a weapon of criminals. Among the social media, WhatsApp, Instagram and Facebook are being used more and more.

More than a quarter of the world's population is currently active on social media. It is considered as the easiest and most dynamic method of communication. However, where there are safe people, criminals also make their nests. The same has happened in the cyber world too. This is true by cyber hackers (criminals) harassing, cheating, defaming the common man through various means including altering the original photo or document.

By asserting this, in a way they create a new image of the person. Currently, this type has become common.

Let us first talk about cyber crime. It can be affected from a common man to a big company/bank of a country.

1) Phishing

For example, a crime called "phishing" is so widespread that it is really important for everyone who uses the Internet to know about it. But still, innocent people who are new to the Internet are constantly falling prey to this type of scam. In this type, cyber criminals on the Internet harm the common people by misleading, intimidating or deceiving them. For that Title

Harm them by intimidating or deceiving them. For that, they first send you a scary or creepy e-mail. For example, the e-mail reads 'Your internet banking password has been obtained by an attacker...change your password immediately to avoid the risk...' For this, a 'link' is provided in this e-mail. When you move your computer's mouse over that link and click on it, you feel that your bank's website is opened in front of you. Actually, this is not your bank's website at all. It is the cybercriminal's own website. But because it looks exactly like your bank's website, you think it's your bank! It says things like "Enter current password to change your password". This is from cybercriminals. Things are written. Since we don't know this work of cyber criminals, we secretly fill in the information and the new, changed password that we want. He also types there. Then because of "changed password" everything is fine, thank you' etc. we see on our computer screen and we feel good. But this is where all the scam happens. This e-mail is sent to you by the cyber criminals themselves in the name of your bank. He also writes the information in such a way that we believe it quickly. Also, this e-mail is sent by him from an e-mail id which he thinks belongs to his bank. So, we think it is really from our bank. Also, the 'link' given by those cyber criminals in that e-mail takes us to Our bank but Even if you think it takes you to your bank's website, it actually takes you to the cybercriminal's bogus website. Then when you type your bank user id and password there, it gets into the hands of that cybercriminal! Then the cybercriminal uses this information to go to the real website of your bank and transfer all the money from your account to his own account using your real user ID and password obtained from you. This is a form of cybercrime. Phishing shall be punished with imprisonment up to 3 yrs. and fine up to 1 lakh rupees. sec 66 (D) information technology act 2000

2) child pornography

India tops in child pornography. Shocking information has come to light that the number of children and teenagers uploading porn videos is high. This is why schoolgirls, teens and desi girls are the most used keywords. Child pornography refers to the sexual abuse of children below the age of 18 years and its filming is called child pornography. Children are sexually abused by luring them with food, toys, mobile games etc.

Child pornography sec 67 (B) shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

3) Cyber grouping

Intimacy is created through social media or messaging platforms for the purpose of sexually or otherwise exploiting children. Cyber groomers encourage intimacy by offering gifts, compliments, modeling jobs. Next they start sending obscene messages, photos or videos. Next ask to send your nude photos, videos with private photos. And that's how they can sexually abuse. Cyber grooping shall be punished with

imprisonment for a term which may extend to three years, or with fine which may extend to one lakh rupees, or with both.sec 66 (B) Information technology act.

4) Cyberbullying

Women, girls are threatened and mentally disturbed. Using the Internet or mobile technology to harass someone by sending obscene or harmful messages, comments and videos. Cyber criminals use texts, messages, e-mails, social media, websites, chat rooms, etc. This leads to severe emotional, physical, social and psychological consequences.

Cyber bullying shall be punishable with imprisonment for a term which may extend to three years and with fine. Section 66 - (A) of IT act.

5) Morphing

In cyber morphing, the original photograph of a person is changed. Fake profiles are created by downloading the pictures of women or young girls, morphing them in a derogatory manner and reposting or uploading them on websites.

Morphing shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees. only if you like it. (Section 67 in The Information Technology Act).

6) Cyber defamation

A person's social reputation is harmed by making a wrong statement. E-mails or posts on social media with defamatory intent.

Cyber defamation sec 77 (B) punishable with imprisonment of three years and above shall be cognizable and offence punishable with imprisonment of three years shall be bailable.

7) Cyber stalking

Tracking a person's online activities, constantly monitoring them and collecting their personal information and disseminating it on social media. By collecting such sensitive information, a cyber stalker enters the victim's daily routine based on name, family background, and mobile number. Also posts the information on the relevant website in the name of the victim.

Cyber stalking shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.(sec 72 of Information technology act).

8) Online gaming

Children play online games on social networks using mobiles, computers, portable gaming devices. For example:- Blue Whale, Pub G. But due to the excessive use of online gaming, children become victims of crimes like theft, suicide.should be careful. Do not share personal details like photos, information, contact numbers, addresses. This information is exploited by cyber criminals and based on which women are cheated or harassed. This is how social media can be misused.

- Infamy due to rejection of love.
- Fraud by luring marriage.
- Blackmail by making viral photos, blackmail.
- Slander to avenge a quarrel.
- Obscene photos, videos viral.
- Misuse by tampering with photos.

In this way, social media can be misused, so women, children and men should remember the following things while using social media carefully: -

Do not send 'friend requests' to strangers or

- Fraud by luring marriage
- Blackmail by making viral photos, blackmail
- Slander to avenge a quarrel
- Obscene photos, videos viral
- Misuse by tampering with photos.

Now if you are a Parent of Young Teen, and Concerned about His/her Well Being, Here are some ways to Protect your Child from Cyber Crimes

1. Recognize the fact that Cyber Crimes exists, and your child is the most vulnerable: Shake away your over confidence that nothing is going to happen with your child. Even the most intelligent Cyber Specialists have fallen into the honey trap. Whatever is shared online can make their way to data hackers, and malware specialists. There is nothing as a safe zone, where it comes to online platform, whether social media, e-commerce or P2P site.2. Report Cyber Crime however big or small. If your child has faced any issue of Cyber Bullying, for example, it is better to immediately inform the authorities, cyber bullies game on the fears and the insecurities of people to make sure that their crime is not reported. You can help arrest some of the biggest Cyber Criminals, with your alertness and ingenuity. 3. Educate your child to avoid visiting and sharing on sites that have a unreliable record: The peak of the interest is that it offers anonymity. Though, it can be a big disadvantage just because you do not know who is watching you and what they plan to do with it. Generally, students fall in to trap of Freebies, easy and free access to Files and Media, Torrent sharing, and the other heinous activities. To save up a little money, or simply to have fun, you may end up in a tangle of the Crime. 4. Educate your ward about Cyber Crime: As long as, most of the students are aware of the Cyber Crimes, they don't understand their magnitude. As a parent, it is very important that you talk to your child as frequently as possible about the nature of the Cyber Crime. Alert them about the situations where they can become weak to crime. 5. Keep a check on your child's activity: Without involving on your child's privacy, look out for the signs that tell you what your child has been doing while online. Also keep the conversation between your child and you easy and owing. It is very important for your child to feel the secure enough to confess in you, in case a problem takes place.

A cybercrime is an offence carried out anonymously by any person under the garb of the internet. Technology allows perpetrators to act anonymously and provides them access to a large, vulnerable population including children.

6.Teenagers around the world addicted to social media : platforms such WhatsApp, Facebook, Instagram and Snapchat are easy targets for the perpetrators of cybercrime. While children are often oblivious to the dangers associated with the cyberspace, parents and it difficult to protect them from cybercrimes as they lack awareness of the legal remedies available under national and international law.

CONCLUSION:

Though not all people are victims to Cyber Crimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they executed by computer. The hacker's identity is ranged between 12 years young to 67 years old. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren't guns anymore; they attack with mouse cursors and passwords. In order to prevent cyber stalking, individuals should avoid disclosing any information pertaining to them. This is as good as revealing your identity to strangers in public area, always avoid sending any picture online especially to strangers and chat friends as there have been incidents of misuse of pictures. Always use current and updated anti- virus software to guard against

virus attacks. Always save back up volumes so that one may not suffer data loss in case of virus corruption. Never ever send your credit card numbers to any site or to any stranger, this is not secured to guard against frauds. Always lookout on the sites your children are accessing to avoid any kind of harassment in children. It is much better to use a security programme that gives control over the cookies and send all the information back to the site as leaving the cookies unguarded might prove lethal. Web site owners should lookout the traffic and the irregularities on the sites. It is very important to discuss and calculate the effects of various other information security awareness delivery methods used in improving the end users, information security awareness and behavior.

REFERENCES :

Cyber crime impact of new millennium

Information technology Act 2000

www.brainyquote.com

kshamablog

www.britannica.com