LEGALFOXES LAW TIMES

CYBER CRIME AND ITS IMPACT ON YOUTH WITH SPEACIAL REFERENCE TO SOCIAL NETWORKING SITES

By: K Jyotsna & Bhumika Thakur

ABSTRACT

In India, the use of Information technology is increasing day by day. In the modern times almost every individual has access to internet, which has increased the range of the cybercrime. Cybercrime is known to all over the world as a crime which is committed by the means od internet. It is, nowadays, becoming a serious matter of concern all over the world. The purpose of this paper is to understand the common cybercrimes and how it impacts the youth of the nation. It also seeks to know the level of awareness among the youth. The internet users are not getting updated on the vulnerable cyber threats and security issues, at the pace they are getting updated with the usage of internet enabled tools and apps. The association with digital supported platforms and gadgets, which protect parents and students from cybercrimes have become a challenging task. This paper also suggests the effective prevention strategies for protecting the internet users form the cybercriminals.

Key Words: Cybercrime, Social Networking Sites, Youth, Information Technology.

1. INTRODUCTION

The modern technological evolution has enabled people to prosper and progress in today’s world but at the same time, it has given rise to new problems which were not known to the mankind and cybercrime is one such area which has emerged in the past few decades. This tremendous progress of technology has made it possible for the people to transmit information from one person to another, visually chat and conduct business with any person form any part of the world. People dependence and their behavior towards the internet deeply affect the way they intend to use information technology. The invention of computers has made the life of the humans easier starting from individuals to large organizations, from online dealing to online transactions. In simple terms we can define computer as an innovative mechanism which stores, manipulates/process the information or the instructions instructed by the user. The computer has the capacity to store, search, and communicate data. This leads to accessibility to information which has made it possible for the individuals to communicate with any person, anywhere, anytime in the world. "Cyber Crime" can be defined as the crimes committed using computers or computer network and usually takes place over the cyber space especially the Internet. Common internet users are unaware of the cybercrimes because of which they do not take proper precautionary methods to prevent such attacks from taking place. Cybercrimes have led to the creation of hacking, identity theft, Credit/debit card frauds, cyber terrorism and many more crimes. Cybercrimes can occur to anyone if their information or data is stored in the network. In order to stop these crimes or to punish the cyber criminals the term "Cyber Law" was introduced. Cyber law can be defined as the part of the legal system that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, as well as includes freedom of expressions, access to the Internet, and online security or online privacy.

2. CYBERCRIME AND CYBERLAW

"Cyber Crime" can be defined as any crime or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of them.[1]

"Cyber law" can be defined as the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e. the Internet. It is an endeavor to integrate the challenges

[1] https://cybercrime.org.za/definition

presented by human action on the Internet with legacy system of laws applicable to the physical world[2]

2.1 CYBER CRIME

Sussman and Heuston first proposed the term “Cyber Crime” in the year 1995. Cybercrime is considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc. Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.[3]Cyber-crime encompasses any criminal act dealing with computers and networks . Additionally, cyber-crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the Internet.[4]

2.1.1 Elements of cyber-crime:

The two main essentials of cyber-crime are 'Actus Reus' and 'Mens Rea'. Actus reus is also called the exterior element and is the objective ingredient of a crime. It is the Latin term for the "guilty act" which, when proved beyond a reasonable doubt in combination with the mens rea, (it is the Latin term for "guilty state of mind"), produces criminal liability in the common law-based criminal law jurisdictions of England and Wales, Canada, Australia, India, the United States of America and many other countries of the world. Mens rea is the mental ingredient of a person's malafide intention to commit a crime; or knowledge that one's action or lack of action would be a basis for crime to be committed. It is an essential ingredient of many crimes.

2.1.2 Types of cybercrime

1. **Online Harassment**: It involves sending harassment letters, messages etc. via emails. This form of cybercrime usually occurs in social media.

[2] http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws
[3] https://techterms.com/definition/cybercrime
[4] https://www.webopedia.com/TERM/C/cyber_crime.html

2. **Cyber-Stalking**: It means tracking a person's personal whereabouts and creating a sense of invasion in a user's personal space. It also creates a sense of insecurity to the person.
3. **Hacking**: It means unauthorized access over computer system. It involves unauthorized access and use of a person's computer. It involves collecting private data and deleting personal data.
4. **E-Mail Spoofing**: It refers to sending fake emails to random internet users with fake sender address.
5. **SMS Spoofing**: Spoofing is blocking through spam, which means the unwanted uninvited messages. In this case, an offender sends out false messages to the victim to steal his identity and personal data such as bank information.
6. **Carding**: It means use of false ATM cards i.e. Fake Debit and Credit cards used by criminals which is used by them to withdraw money from the victim's bank account.
7. **Virus attacks**: It occurs when a criminal releases harmful viruses into the victims' computer with the intention of damaging and deleting his personal data and also to extract information from the computer.
8. **Email spamming**: It involves sending thousands of emails to various users with the intention to get personal data. Illegal download: It means download of the latest movies via torrent and downloading the latest games. All these falls under cybercrimes.
9. **Identity theft**: This refers to a crime where the criminal uses the victims' names to conduct online transactions for his personal gain.

Cyber Crime can be classified into three major categories. They are as follows:

- **Against Individual**:
  (a) The person, and
  (b) The property of an individual
- **Against Organizations**:
  (a) Government,
  (b) Firm, Company, Group of Individuals
- **Against Society at large**

The following cyber-crimes are committed against the following groups:

Against Individuals:

(i) Harassment via e-mails.
(ii) Cyber-stalking.
(iii) Dissemination of obscene material.
(iv) Defamation.
(v) Hacking/cracking.
(vi) Unauthorized control/access over computer system.
(vii) Indecent exposure.

(viii) Email spoofing.

(ix) Cheating and Fraud.

Against Individual's Property:

(i) Computer vandalism.

(ii) Transmitting virus.

(iii) Hacking/cracking.

(iv) Unauthorized control/access over computer system.

(v) Intellectual Property crimes.

(vi) Internet time thefts.

Against Organization:

(i) Hacking/cracking.

(ii) Unauthorized control/access over computer system.

(iii) Possession of unauthorized information.

(iv) Cyber terrorism against the governmental organization.

(v) Distribution of pirated software etc.

Against Society at large:

(i) Pornography.

(ii) Polluting the youth through indecent exposure.

(iii) Trafficking.

(iv) Financial crimes.

(v) Sale of illegal articles.

(vi) Online gambling.

(vii) Forgery.

2.2 CYBER LAW

Cyber law is the part of the legal system that deals with the internet, cyberspace and their respective legal issues. Cyber law controls the crimes committed through the internet or through the uses of the computer resources. It prevents the users by reducing large scale damage from cybercriminal activities by protecting information, intellectual property, piracy and also the freedom of speech related to the use of the websites, emails, cell phones, computers, software and hardware, such as data storage devices.

2.2.1 Importance of Cyber Law

Cyber law plays a very important role in this modern era of technology. With the increased dependence of e-commerce and e-governance a wide range of legal issues related to use of internet as well as other forms of computer or digital processing devices such as violation of intellectual property, piracy, freedom of expression, jurisdiction etc. have emerged, which need to be tackled through the instrumentality of law. Whether we are aware of it or not, but each action and ereaction in Cyberspace has some legal and Cyber legal views.

2.2.2 Cyber Laws in India

- **Information Technology Act of India, 2000**

The IT Act of India was passed by the Indian Government in May 2000. This Act contains the various cyber laws of the state. It is the law that deals with cybercrime and e-commerce. The Act was based on the United Nations Model Law on Electronic commerce. The Act aims to provide legal structure for all electronic transactions in India. Chapter IX of the Act states the various penalties for cybercrime offences. The Act also talks about the compensation for the victims affected by cybercrime which does not exceed Rs. 1,00, 00,000. The Act talks about the various offences that can be classified as cybercrime.

- **Cyber Swachhta Kendra**

The Cyber Swachhta Kendra is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology to create a secure cyberspace by detecting botnet infections and to enable cleaning and securing systems of users so as to prevent further infections. This policy is set up in accordance with the objectives of the 'National Cyber Security Policy'. The policy operates in close coordination with various internet service providers and antivirus companies to notify the users regarding the botnet infection in their computer and also provides them assistance to clean their systems. The policy also aims to provide awareness regarding botnet, malware infections and measures to be taken to prevent malware infection. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under the provisions of Section 70B of the Information Technology Act, 2000.

- **National Cyber Security Policy, 2013**

This Act was formalized by the Indian Government in 2013. It was taken as a step to counter cybercrime. The purpose of this document is to ensure a secure a safe cyberspace for the citizens of India. The Cyber Security Policy ensures protection of information in cyberspace, reduce vulnerabilities, and minimize the threats of cyber incidents and also to minimize the damage from cybercrimes. The policy states that education and training programmes are required for reducing the cybercrime rate. The policy aims to create 500,000 professionals within 2018 through advanced training and skill development programs. The policy plans to launch various national awareness programs across the country with a view to increase cybercrime awareness. The policy calls for a public and private partnership in order to tackle the cybercrimes.

3. SOCIAL NETWORKING SITES AND CYBERCRIME

A social networking site is a phrase that is used to describe any website that enables users to create public profiles within that Web site and form relationships with other users of the same web site. Social networking sites can be used to describe community-based Websites, online discussions forums, chatrooms and other social spaces online. A social networking site is an online platform which allows the users to create a public profile and interact with other users on the website. Social networking sites usually have a new list of people with whom they share a connection and then allow that person on the list to confirm or deny the connection. After connections are established, the new user can search the networks of connections to make more connections. The social media platforms have given rise to the vast global cyber criminal network.

Most cyber crimes are committed by individuals or small group of individuals. However, large organized crime groups also take advantage of the Internet. These professional criminals find new modes to commit old crimes, treating cyber crime like a business and forming global criminal communities. Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They are usually technology buffs who have expert level skills in one particular software program or language. In hacking, the criminal uses a variety of software to enter a person’s computer and the person may not be aware that his computer is being accessed from a remote location. This crime occurs when a person violates copyrights.

Today, the cyber law is addressing this cyber crime and preventing people from being trapped in these crimes. Social media sites can also be used for positive activities, like connecting kids with friends and family, helping students with school, and for entertainment. But it can also be used to cause harm to other people. Whether done in person or through technology, the effects of bullying are similar. Identity theft has also become a major problem with people using the Internet for cash transactions and banking services. Child soliciting and abuse is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. These can be broadly categorized as the monitoring and criminal prosecution of offenders, community education, and restriction of children's access to offensive material on the internet.

4. CYBERCRIME AND YOUTH

In today's world, almost every individual has access to the internet. The youngsters from very early age are dependent on the internet nowadays for educational purpose, entertainment and so on. As, these youngsters are new to IT world they are usually not aware of the entire working of the cyberspace , because of which they perform such actions which makes easy for the cybercriminals to commit crimes by using their data. To protect youngsters from performing such actions they must be provided the full knowledge to ensure that they do not come into the trap of the cybercriminals.

(Marcum, Higgins, & Ricketts, 2010) through their study proved that more effective policies and plans can be established to teach youth and people about defending themselves while online. Youth should be mindful of who they are communicating with online and abstain from as long as any type of personal information to persons they do not identify and belief. Also, further analysis of the use of social networking websites and the wrong actions of youths, as well as their knowledge with misleading Internet practices, will spread our awareness of the online activities and practices of adolescents. With this understanding, better safety measures and strategies can be established to keep adolescents safe online.

(Oksanen & Keipi, 2013) in the study explored cybercrime, which has grown into a major topic within the last two decades. Young societies are more likely to be the targets of cybercrime. In addition to age, other aspects including gender, education, financial status, and forceful victimization relates with cybercrime victimization. Decent offline social networks were a defending aspect against cybercrime harassment among females. Young cybercrime preys were more likely to be bothered about future harassment. They showed the significance of understanding both psychosocial threat elements in offline and patterns of uncertain online actions.

It is always important to keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children. Also, while using the personal data it is important to know whether the site you are using is trustworthy or not because cybercriminals use various techniques so that they can get the personal data of yours.

5. CYBERCRIME PREVENTION STRATEGIES

1. There is only partial awareness among the general users about the cyber crimes and government agency should take proper measures to protect the users and should also conduct awareness programs so that they can spread awareness to public at large
2. The cyber café or the internet centre owners have done appreciable work by adopting the system of asking for address proofs and identity of the cyber users. This system has been adopted after the enforcement agency made it compulsory from the year 2010 to have the login time and logout time of every user with their identity to identify incase of cyber crime takes place. But the enforcement agency should have a follow-up action to see whether their records are maintained properly or not by each internet centers in city for preventing the city users from cyber crimes.
3. Always keep an eye on your children while they use the internet and protect them from identity theft. Identity thieves often target children because their Social Security number and credit histories are usually easy to crack. You can help guard against identity theft by being careful when sharing your child’s personal information. It’s also smart to know what to look for that might suggest your child’s identity has been compromised. You should teach your kids about acceptable use of the internet without shutting down communication channels. Also, they should come to you freely without hesitation if they’re experiencing any kind of online harassment, stalking, or bullying.

4. The internet users should be taught to protect their password and importance of protecting the password. This should be done by the internet café/ center's (owners) supervisors and teachers of school and colleges. Also it is good if a person use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport. Because a Virtual Private network (VPN) will encrypt all traffic leaving your devices until it arrives at its destination.
5. The children may become addict to games and visiting unscrupulous and objectionable sites not suited to their age. Parents, teachers, responsible citizens, cyber café owners and enforcement officers should take some action in this regard to protect the psychological health of future generation of India.
6. Susceptible for this type of crimes when give away their personal details like name, address, email and email address and other passwords to the sites while making purchases or e-money transfers on internet without taking proper precaution.
7. The survey reveals a need of educating all users about the types of cyber crimes and their consequences and importance of protecting one's password/ bank pin number and email address while using internet, because many users are not aware of the cybercrimes.
8. Prevention of cyber crimes and training requirement of enforcement authorities - through years of research which would be of help for government and all other stake holders in the process and especially to the benefit of the society in creating fearless environment where they will have happy surfing, e-banking, e-shopping and e-mailing internet experiences for their lifetime.
9. Install or update your antivirus software, antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without the users' knowledge. Most types of antivirus software can be set up to update automatically.
10. Turn off your computer, the growth of high-speed Internet connections, many opt to leave their computers on and ready for the action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

If the user become a victim of a cybercrime, he/she need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. The users report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.

6. CONCLUSION

The use of the internet has increased from the past few decades which also increased the range of the cybercrime. The information technology has made work easy for the users in all aspects, but has also upsurge the crimes. This is because many users are not thoroughly aware of the cybercrimes and cyber security that are prevailing. There are a wide range of information security awareness delivery methods such as web-based training materials, contextual training and embedded training. In spite of the increased efforts of information security awareness, research is scant regarding information security awareness delivery methods. The risk of cybercrime has increased among the youngsters because nowadays the youngsters can easily access the internet and due to lack of knowledge and awareness they commit such acts which are inappropriate in the world of cyberspace. Current cybercrime policy is concerned with particular online risks adolescents are exposed to, for example online grooming and sexting, and other issues such as exposure to harmful or illegal content. While paying attention to online risks of adolescents, the opportunities of the Internet for the development of young people should not be neglected. For the protection of the youth the primary responsibility lies with parents and also with the youths themselves. It is the most important approach, to try and make children and adolescents more resilient, by fostering digital literacy and safety skills. For preventing cyber stalking the user must avoid disclosing any information pertaining to one self and the user should avoid disclosing any personal information to strangers via e-mail or while chatting also, the user must Block pornographic sites on the Internet, which is the primary source of the photos and videos that transmits through Social networking sites. Along with the users the government should also spread the awareness and protect the rights of the people and must ensure that proper actions are taken against the cybercriminals.

REFERENCES

[1] http://www.cyberlawsindia.net/cyber-india.htm.

[2] https://cybercrime.org.za/definition.

[3] http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws.

[4] Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.

[5] https://www.tutorialspoint.com/information_security_ cyber_law/introduction.htm.

[6] Cybercrime classification, [Online],Available: http:// shodhganga. inflibnet.ac.in/ bitstream /10603/7829/12/12_ chapter % 203.pdf [29 September 2013].

[7] A comparative analysis of cyber security initiatives worldwide, international telecommunication union, Geneva, 28 June -1 July 2005.

[8] https://techterms.com/definition/cybercrime.

[9] https://www.cyberswachhtakendra.gov.in.

[10] https://www.webopedia.com/TERM/C/cyber_crime.html.

[11] Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior, 31(5), 381-410.

[12] Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population based study in Finland. Vulnerable children and youth studies, 8(4), 298-309.

[13] Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education In Proceedings of the 2011 conference on Information technology education (pp.113-122).ACM.