International Journal of Humanities and Social Science Research
ISSN: 2455-2070
Impact Factor: RJIF 5.22
www.socialsciencejournal.in
Volume 4; Issue 1; January 2018; Page No. 73-77

Cybercrime in digital world and possible prevention

Dr. Mandira Gupta
Associate Professor, Department of Sociology, M.M.H. College, Ghaziabad, Uttar Pradesh, India

Abstract
Cyber crime is a criminal activity that involves a computer and a network. These offences are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat room, emails, notice boards and groups) and mobile phones (Bluetooth SMS MMS).

Keywords: Cybercrime, networks, Bluetooth SMS MMS

Introduction

Cyber crime is a criminal activity that involves a computer and a network. These offences are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat room, emails, notice boards and groups) and mobile phones (Bluetooth SMS MMS). It covers like phishing, Credit card frauds, bank robbery, illegal downloading industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, Cyber stalking and distribution of viruses and so on.

"Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communication or information system including any device or the internet or any one or more of them." [1]

The first time India went online was in 1986 but initially internet was only used for educational, research communities and defense purposes. Videsh Sanchar Nigam Limited introduced internet access to public by using modem in the year 1995. After that many Indian have mobile phone which have internet access. A report on digital adoption and usage trends in India, compiled by IMRB's Icube 2018, the number of internet users in India grew 18% annually; This figure is expected to grow over 900 million internet users by 2025 with at least one internet user present in more than 87% of Indian households, according to a report by Kantar, a market research agency. According to recent data at present in India there are 840 million internet users.

Cyber crime is and uncontrollable evil having its base in the misuse of growing dependence on computer in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us is it has its dark side too. [2]

Computer and Internet has made our life very easy. Information and communication technology development has made the world very small, today it has become easy to gather information about any subject through the Internet that is why information technology is the revolutionary invention of this century [3]. However, just like all of the things, it gets to used wrongfully and often times abused. There are times that people use the internet to open the black market. The problem is many people misuse and abuse the use of internet. It pretty easy for those hackers or even ordinary people to do malicious things online. Internet abuse refers to improper use of the Internet and may include use of the Internet for threats and intimidation, cybercrime, computer use in criminal activities, cybersex trafficking, etc.

Origin of Cybercrime

The first person was Lan Murphy also known as Captain Zap, found guilty of cybercrime and that happened in the year 1981. He had hacked the American Telephone Company to manipulate its internal clock, so that users could still make free calls at peak time [4].

Modern age is also economic development era and human needs a lot of money to fulfill his needs, but poverty is such a curse that takes human beings to any extent. Due to poverty, a situation of misery arises in the state, due to which there is an increase in the number of crimes, most of the criminal acts are done not only for the fulfillment of the need but with a view to get extra luxury things [5].

Cyber crime has become major concern because everyone is using computers in society. Internet has given access to everything while sitting at one place due to the advancement of Technology like social networking, online shopping, online studding, online jobs all possible things that we can think can be done through this. We cannot consider cybercrime just like other crime because it has no geographical boundaries and the cybercriminals are not known. It is affecting all the stakeholders from government, business to citizen alike. In India cybercrime is increasing with the increased use of Information and Communication Technology.

Table 1: Cases registered and crime rate in India

Year	Crimes	Crime rates
2016	12317	1
2017	21796	1.7

Source: NCRB, India Spend

Cyber crime can be categorized in three groups

1. Individual
2. Property
3. Government

Individual Cybercrime entails a single person disseminating malicious or unlawful material via the internet. This type of Cyber crime has been taken seriously by law enforcement agencies and now they are keeping a track over every such attack on an individual.
Property The attacker steals a person's bank details and misuse the credit card for online purchase by using malicious software. The attacker attacks the property to disrupt the system of the organization.
Government The attacker can get hold of essential documents related to government projects. An enemy Nation or terrorist usually makes such attacks.

Different mode of Cybercrime

Hacking

Hacking is considered as amongst the most serious of all cyber crimes. Hackers normally hacks the computer system or mobile networks of the person to get personal information and act of hacking completely destroys the whole data and program.
Hacking is committed to damage the business of competitors and enemies. Disruption of a computer and denial of access to a person authorized to access any computer, are some of the damages that may be caused by hacking. Hacking is done to spy into others computer systems and for stealing information/data residing there in. Hacking is also used as a weapon to commit other crimes such as cheating and misappropriation of funds electronically from the bank account of another.

Cyber Stalking

It is online harassment by an individual or a group of people. Normally these stalkers target an individual and harass online. There are many cases of Cyber stalking in India resulting in the target person ending uptake taking self life.
The Wikipedia define cyber stalking where the internet or other electronic means to stalk or harass an individual or a group of individuals or am organization it include the making of false accusations for statements of fact as in defamation monitoring making threats identity theft damage to data or equipment the solicitation of minors of for sex or gathering information that may be used to harass [6].

Child pornography

This is extensively used for sexual abuse of children. In today's world every children especially adolescents are exploring information through internet. Every children of this generation have access to computers at home and the internet because it is part of their studies and this makes them very vulnerable to the potential danger of internet. Many children's are curious about sexuality and sexual explicit material. Most of the parents are busy with their work and not able to control what their children are doing on computer, whether they are studding or doing wrong things. Sex offenders exploit these conditions and fulfill the need of children. The child at this age so tender. does not understand and recognize the potential danger of these contacts. The internet is highly used by the abusers to abuse children sexually worldwide. The children in India become viable victim to the cybercrime as internet becomes the household item in India. The children are becoming victims of the aggression of pedophiles.

Cracking

Cracking means that a hacker has broken into your computer system without your knowledge and can destroy your confidential Data.

Cyber Terrorism

The word "Cyber terrorism is of recent vintage and was coined by computer whiz Bary C. Collin" [7]. The term cyber terrorism is the combination of cyberspace and terrorism and we do not have any definition of Cyber terrorism which can be accepted worldwide. Every research or scholar in the subject gives a different dimension while defining the term cyber terrorism.
Terrorist exchange secret information, messages with other group through computer networks. Osama Bin Laden carried out violent incidents by sending secret and symbolic messages to different countries through email to his terrorist group.
Cyber terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. While we would often associate with the loss of life, we cannot overlook important results like intimidation or coercion that can be brought about by cyber-terrorism [8].

Phishing

A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites or they may ask the receiver to respond with confidential information. Another type of phishing campaign is known as a spear-phishing. These are targeted fishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for. They send fake emails which appear like genuine and ask your personal and bank account information and take money from your account.

Theft from credit/debit card/bank account

Customers are also robbed by cyber crime. These people are not robbed in the traditional way, by burglary in which valuables are stolen but this is done by using technology from customers' account or from their credit/debit card. The customer is either deprived of the amount deposited in his account or he becomes a victim of online fraud.

Transmitting Virus

Sending a virus to another computer by a person through a program or file, which damages the files or destroys the data present in the system? Some viruses can spoil your motherboard, so with problems it also gives your monetary loss.

Distribution of pirated software

The pirated software is being distributed from one computer to another computer which can destroy the data and official records of the Government.

Sources of cyber attack

Cyber attack on computer is mainly through program which is small software of computer virus that spreads from one

computer to another and also has the ability to interfere in computer operation.

Downloadable Program

Downloadable file is the most important and possible source of virus. Any type of executable file like games, screen saver etc. are its main source so it is necessary to scan any program before downloading it from internet.

Cracked Software

This software is another source of virus attack. This type of cracked software is more likely to contain viruses and bugs, which are very difficult to find and remove from the system. So any information from the internet should be downloaded from the reliable source**.**

Email attachment

Some viruses are sent through email attachments. Once any user will download this attachment and it will harm the computer.

Threat to computer security

Malware is a specific type of virus that self replicates by inserting its code into the other programs and main function is to harm the computer.

Virus is a program that has a negative effect on the computer or on the PC, by gaining control, he makes them perform unusual destructive actions, as soon as the virus is there, it copies itself into the system, it gets associated with the numbers for further use. Some virus can enter and s block operating system and other application programs from. The Viruses are of many types like Direct action virus, Overwriting virus, Boot sector virus, File system virus, Web virus etc.

Effects of Viruses

Viruses can do many effects on a computer.

1. Monitoring user activity
2. Decreasing the efficiency of computers
3. Destroying all data on local disk
4. Affecting computer networks and Internet connections
5. Increasing or decreasing the size of memory
6. Displaying different types of error messages
7. Changing PC settings
8. Displaying unwanted attachments
9. Extending boot time

Challenges to prevent the Cybercrime

Cybercrime lacks eyewitnesses and accomplices. Cybercrime is a difficult and challenging task due to the following reasons.

1. High tech crime- Information technology is changing rapidly but general investigators have limited knowledge about this technology. The investigator needs to be trained for the interpretation of the Cybercrime.
2. Sometimes cyber crimes occur in one country but the result is found in another country, in such a situation the problem of juridiction arises.
3. Lack of crime scene- Two computers can be connected to the satellite from any place, so the crime of withdrawing money with credit card can be done without any particular place, so cybercrime does not have any definite place of occurrence.
4. No face in Cybercrime- The crime of cyber crime does not require personal presence in writing and a signature or voice but at the press of a button criminal incidents are carried out. So it is clear that this crime can be done without showing the face.
5. Short term crime- cybercrime can happen immediately, but crime is detected after several days and months, and the evidence related to it can be completely.

The most complex aspect of cyber crime is that this crime can be committed by sitting in any corner of the world. Even the most powerful country of the world America is also no exception to this. Hacking has become an interest and business today. The sites of government institutions of all countries of the world are also sometimes attacked even from the Prime Minister's Office in India to the Ministry of Defense and External Affairs, Indian Embassies. There has been a cyber attack on the computer of missile systems etc. Terrorists have become prominent. Bulletin boards of porn websites cannot be easily done on the website. Internet remains a safe and medium of exchange of messages for terrorists. In Internet banking also the deadly effects of cyber crime are seen.

Due to cyber crime, the economy of the country also suffers, on the other hand, crores of rupees have to be spent for the prevention of cyber-crime exams. In America, every year due to these crimes, there is a loss of 10 billion dollars, it has become a worldwide problem. A strong international law is needed to deal with it. One needs to be strengthened.

Cyber Law in India

1. Tampering with computer source Documents Sec.65
2. Hacking with computer systems, Data Alteration Sec.66
3. Sending offensive messages through communication service, etc Sec.66A
4. Dishonestly receiving stolen computer resource or communication device Sec.66B
5. Identity theft Sec.66C
6. Cheating by personation by using computer resource Sec.66D
7. Violation of privacy Sec.66E
8. Cyber terrorism Sec.66F
9. Publishing or transmitting obscene material in electronic form Sec.67
10. Publishing or transmitting of material containing sexually explicit act, etc. in electronic form Sec.67A11. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc in electronic form Sec.67B.
11. Preservation and Retention of information by intermediaries Sec.67C
12. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource Sec.69
13. Power to issue directions for blocking for public access of any information through any computer resource Sec.69A
14. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security Sec.69B
15. Un-authorized access to protected system Sec.70
16. Penalty for misrepresentation Sec.71
17. Breach of confidentiality and privacy Sec.72
18. Publishing False digital signature certificates Sec.73

19. Publication for fraudulent purpose Sec.74
20. Act to apply for offence or contraventions committed outside India Sec.75
21. Compensation, penalties or confiscation not to interfere with other punishment Sec.77
22. Compounding of Offences Sec.77A
23. Offences with three years imprisonment to be cognizable Sec.77B
24. Exemption from liability of intermediary in certain cases Sec.79
25. Punishment for abetment of offences Sec.84B
26. Punishment for attempt to commit offences Sec.84C
    Note: Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act
27. Offences by Companies Sec.85
28. Sending threatening messages by e-mail Sec.503 IPC
29. Word, gesture or act intended to insult the modesty of a woman Sec.509 IPC
30. Sending defamatory messages by e-mail Sec.499 IPC
31. Bogus websites, Cyber Frauds Sec.420 IPC
32. E-mail Spoofing Sec.463 IPC
33. Making a false document Sec.464 IPC
34. Forgery for purpose of cheating Sec.468 IPC
35. Forgery for purpose of harming reputation Sec.469 IPC
36. Web-Jacking Sec.383 IPC
37. E-mail Abuse Sec.500 IPC
38. Punishment for criminal intimidation Sec.506 IPC
39. Criminal intimidation by an anonymous communication Sec.507 IPC
40. When copyright infringed:- Copyright in a work shall be deemed to be infringed Sec.51
41. Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of Sec.63
42. Enhanced penalty on second and subsequent convictions Sec.63A
43. Knowing use of infringing copy of computer programme to be an offence Sec.63B
44. Obscenity Sec. 292 IPC
45. Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail Sec.292A IPC
46. Sale, etc., of obscene objects to young person Sec.293 IPC
47. Obscene acts and songs Sec.294 IPC
48. Theft of Computer Hardware Sec. 378
49. Punishment for theft Sec.379
50. Online Sale of Drugs NDPS Act51. Online Sale of Arms Act.

Prevention from Cyber crime

Though it is highly impossible to completely stop the cybercrime but one can always prevent it and save from this. We can follow some important measures to protect our computer and personal data from cyber crime.

Keep software and operating system updated

Software and operating system to be kept updated so that ensures benefit from the latest security patches to protect the computer. Updating your software will minimize the chances of them being able to gain entry to any personal data or information**.**

Use antivirus software and keep it updated

Using anti-virus or a comprehensive internet security solution is a smart way to protect your system from attacks. Antivirus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving peace of mind and always update anti-virus software to receive the best level of protection.

Strong password

To use always strong passwords so that no one will be able to guess. It should be of 8 characters including a combination of letters numbers and symbols. Normally we all want passwords that are easy to remember hence we go for birthday, anniversary etc. that are easy to remember but that is putting device and possibly finances at risk. Use a reputable password manager to generate a strong password randomly to make this easier.

Never share personal information to a stranger

It is always advised that never give out personal data over the phone or via Email unless you are completely sure the line or email is secure and on phone you are a speaking to the person you know personally.

Do not click on links in spam emails, untrusted websites or Pop-ups

People become victim of Cyber crime by clicking on links in a spam mails or other messages, or familiar websites. If an email or popup window ask you to enter username or password don't do it instead open your browser and visit the site directly if you are fully convince then contact the company or entity that supposedly got you. Know that established and recognize companies will never ask you for your login information through an email.

Use virtual private network (VPN)

VPN enable us to hide our IP addresses so we can be safe on internet. A VPN will encrypt all the traffic other than your devices until it reaches the final destination. If cybercriminals do work to hack your communication line they won't intercept anything accept encrypted data. With VPN you know you are not being tracked and save your internet traffic unbreached. It is an essential internet tool that provides the best quality of security when it comes to the internet.

Secure wireless network

Wi-Fi networks are vulnerable to intrusion if they are not properly secured so review and modify default settings. Public Wi-Fi and hotspots are also vulnerable. Avoid conducting financial transaction on these networks.

Ensure social media setting private

Social networking profiles like Facebook Twitter YouTube set to be private. to check your security settings be careful with the information that you post online once if you put something on the internet it is there forever. Always keep your personal and private information locked. Keeping your posts on the public is never a good idea. Revealing personal information like your nick name or pet's name can expose the answers to common security questions.

Secure mobile phones

Make sure that you download application only from trusted sources. Be aware that your mobile device is vulnerable to

viruses and hackers. It is also necessary that you should keep your operating system up to date and make sure to install antivirus software. Also use a secure lock screen as well otherwise anybody can retrieve all your personal information on your phone if you lost it. Even hackers can track your every movement by installing malicious software through your GPS. Turn on automatic updates to prevent potential attacks on older version of software.

Educate children about the threat of internet

Children are already using the internet on mobile and computer devices to a great extent because it has become necessity in a student's life. Every parent must educate their children about the risk that comes with it. Make sure that your child comes to you if he or she is experiencing any form of online harassment abuse or any other cyber criminal activity.

Conclusion

The attention of the whole world is now towards cyber crime. Cyber security is not a separate phenomenon in any way, but it is directly or indirectly affecting the social structure of all countries, through this people fulfill their own political, religious and other purposes and make financial fraud to get money to promote terrorism. It has big dimensions due to which financial stability is being affected [9].

Cybercrime now used by the government of many countries indirectly or directly during the election process. Cybercrime today is a matter of concern not only in developed countries but also for the people of developing countries and developing countries, it is necessary to make efforts of all national and international powers for its control.

India's cyber security agency has laid special emphasis on not revealing information of their voter ID and Aadhar card on social media platforms and advising internet users to close their inactive accounts. The country's nodal agency Computer Emergency Response Team of India(C.E.R.T.N) asked not to share personal information on social media to prevent hacking and forgery.

In an effort to promote demonetization and digital life in India, has increased the risk of cyber crimes on smart phones. The government will have to set up a cyber security commission on the lines of the Atomic Energy and Space Commissions to curb this potential threat of cyber crimes.

Cyber crime is a fatal problem for all human beings, which we all have to worry about. Cybercriminals always keep updating with new information and technical advancement. We also have to stay with the relevant law, only then it will be possible to get rid of this problem because this crime is not limited against one person or institution but affect the whole society.

References

1. http://cybercrime.org.za/definition
2. Prof. R.K.Chaubey," An introduction to Cyber Crime and Cyber Law",Kamal Law House 2012.
3. उपाध्याय ज्योति, "रिसर्चलाइन अंतर्राष्ट्रीय जर्नल" अंक XXIII त्रैमासिक अगस्त- अक्टूबर 2016.P.42
4. www.legalserviceindia.com, "Cyber Crime In India: An Overview", Nidhi Narnolia
5. एन. वी. परंाजय, "अपराध शास्त्र एवं अपराधिक न्याय प्रशासन" 1990.P.102
6. http://en.wikipedia.org/wiki/Cyberstalking
7. Barry Collin, "The future of Cyber Terrorism" Proceedings of the 11th annual International symposium on criminal justice issues, the University of Illinois at Chicago, 1996.
8. Dr. Sirohi M.N. Cyber Terrorism and Information Warfare, Alpha editions Delhi.
9. मूंदड़ा एस.एस., "सूचना प्रौद्योगिकी और बैंकिंग क्षेत्र में साइबर जोखिम" बैंकिंग चिंतन अनु चिंतन, P.5 -12
10. http://bitbusinessit.com/top-10-cybercrime-prevention-tips.
11. http://intellipaat.com/blog/what-is-crime