Research Guru
Online Journal of Multidisciplinary Subjects (ISSN : 2349-266X)
Volume-13, Issue-1, June 2019
Impact Factor: 4.081
www.researchguru.net

Juvenile Cyber Crime

DR.BHARAT PATEL
Assistant professor, Department of Sociology, Shree K.R.Katara Atrs College,shamalji,
EMAIL ID: -bharatdantod@gmail.com, 9427366520

Abstract

Cyber Crime is the term used to broadly describe criminal activity in which computer and computer networks are a tool, a target, or palace of criminal activity and incudes everything for electronic cracking to denial of crevice attacks. Adolescent children are more likely to engage in juvenile cybercrimes such as hacking and online bullying if their friends are into it, a new study on peer influence has suggested. Recently, the Indian government reported that it is considering forcing softer punishment for teens and first time offenders involved the cybercrimes. Prevention is always better than cure. We should take certain Precaution while operating the internet and should follow certain preventive measures for cybercrimes.

Key Words: Juvenile, Cybercrime, Internet, Technology, computer, Hacker

Introduction

On April 13,2009 a news flashed in The Times Of India newspaper which brought into Light that how adolescent children are nowadays more likely to engage in juvenile cybercrimes such as hacking and online bullying.

"A 'bad boy 1st Juvenile cybercrime convict''

"MUMBAI: In the First ever web crime conviction involving a Juvenile In Mumbai, a child court held that a 16-year-old student from Ahmedabad who Threatened to blow up Andheri railway station in an email message last year, was guilty The boy said he sent the email for the fun of having his prank Flashed as a 'braking news' on television.

The boy, a class XII science student, was arrested on March 22 last year for claiming to be a member of the Dawood Ibrahim gang in his email to a private news channel. The boy created an account,dgang4blast@yahoo.com, in a cyber café in Ahmedabad on march 18,and sent the email at 5.28 PM on the same day. The email said the bomb whole be planted on the unspecified train to blow it up, 'said inspector of the cybercrime investigation cell (CCIC).

Following the receipt of the email, a café of criminal intimation under section 506 (ii)Was resisted with the Andheri police. It was transform to the CCIC the next day for the further investigation.

'We traced the internet protocol (IP)address to a cyber café in a Ahmedabad' 'said Inspector, and added the although the cyber café had seven or eight computers, the one used for sending the email was used by only one customer on march 18,2008.

The cyber café owner told the police that his friends had come on that day and are of them may have used the computer. "We summoned seven or eight people who had visited the cyber café on March 18''.

The world of the internet today has become a parallel from of life and living. publics now capable of doing things which were not imaginable few years ago. The internet is fast becoming a way of life for millions of people and also a way of living because of growing dependents and reliance of the mankind on these machines. Internet has enable the use of

website communication, email and a lot of anytime anywhere It solution for the betterment of humankind. Internet though offers great benefit to society, also present opportunities for crime using new and highly shiphisticated technology tools.

Today e-mail and website have become the preferred means of communication. Organization provide internet access to their staff.by their very Nature, They facility almost instant exchange and dissemination of data, images and verity of material. This includes not only educational and informative material but also information they might be undesirable and anti-social. Regular stories future in the media on computer crime include topic covering hacking to various ,web jerkers to internet pedophiles, sometime accurately portraying events ,sometimes misconceiving the role of technology in such activities. increase in cyber crime rate has been documented in the news media. Both the increase in the incidence of criminal activity and the possible emergency of new varieties of criminal activity pose challenges legal system, as well as for low enforcement.

Peer influence fuels juvenile cybercrime: A Study

Adolescent children are more likely to engage in juvenile cybercrimes such as hacking and online bullying if theirs friends are into it, a new study on peer influence has suggested.

The study, hitch consist of surveying 435 middle-and high-school students, showed that the biggest predictor of how likely a child is to engage in illegal online activities is whether his or her friends have committed cybercrime.

Previous research has primarily focused on college student. The study showed that a lack of self-control is also a major predictor of children cybercrimes. Risk-tacking, impulsive kids are more likely than other children to act an opportunity to commit illegal online activities, said Thomas holt, a Michigan State University criminologist who led the study.

It's important to know what your kids are doing when they're online and who they are associating with both offline and online.

Cybercrimes include digital piracy, such as "Stealing" music or movie files by downloading them without paying, or online bullying and harassment, which can consist of sending threating or sexual massage via email or text message. Computer hacking also known as cyber-tress passing, and viewing online pornography, which is illegal for those under 18,are also cybercrime. There searches, who detailed their finding in American Journal of criminal justice, recommended and parents place, parents-control software on their children's computer.

However, they warned that many kids can work around these programs. Its not just enough to have a 'Net Nanny'. Parents need to be more proactive with their kids and discuss these ethical dilemmas to using a computer, such as whether it's right or wrong to steal music or to download something without paying for it.

Juvenile Arrested Under IT Act During 2009

(10 Indian States)

SL No.	State/UT	Below 18 years
1	ANDHRA PRADESH	0
2	GOA	0
3	GUJARAT	0
4	HARYANA	0
5	HIMACHAL PRADESH	0

6	JAMMU&KASHMIR	0
7	KARNATAKA	0
8	KERALA	4
9	MADHYAPRADESH	0
10	MAHARASTRA	6

Juvenile Arrested Under Cyber Crime (ITAct+IPC Section)
During 2009 (All-India)

SL.No	Crime Head	Below 18 years
A.	Offences under IT Act	
1.	Tempering Computer source documents	0
2.	Hacking with computer systems (i) Loss/damage to computer resource/utility (ii)Hacking	 1 0
3.	Obscene publication/transmission in electronic form	9
4.	Failure (i)Of companies/orders of certifying authority (ii)To assist in decrypting the information intercept by Govt.	 0 0

Agency - Un-authorizedaccess/attempt to access of protected Computer system. - obtaining license or Digital signature ciryficate by misrepresentation/ Suppression of fact. - Publishing false digital signature certificate. - Fraud digital certificate. - Breach of confidentiality/Privacy other.	 0 0 0 0 0
Total	10
Offences under IPC - Offence by/Against Servant - False electronic evidence - Destruction of electronic evidence - forgery - Other	 0 0 0 0 0

Indian Debate over Punishment Enforcement to Juvenile Involvement in Cyber Crime.

Recently, the Indian government reported that it is considering forcing softer punishment for teens and first time offenders involved the cybercrimes. The "graded response" that the government is contemplating involves a wrning.counselling and prenatalindene for such offenders-many of whom, unaware of cyber laws, advertantlybreak the law and get caught. If and when these ensure do not work, an FIR will be launched.

While the discussion Between the home ministry and IT department for The frame work of such a response have only just begune,and it will probably be a while before its implimantation,The feat the government realigned and understand the impressionability many young of offenders is truly positive sign.

Many offenders do not have malicious intention; often, then do not even know that their action may be illegal. Experts also feel that the legalprrociding against foist time and young offenders negatively affect their education and carrier and coursesextreme social as grace that is incongruous with their harmless intenstions.currently,under the information Technology Act, uploading and assimilatingcommunallycausative ,sexually, explicit and objectionable".images,videos,and messages carries penalty of even year in jail.

What is Cyber Crime?

The Expression crime is defined as an act which subject the doer to legal punishment or any offence against morality, socialorder or any unjust or shameful act. The "offence" is defined of the code of criminal procedure to mean as an act or omission made punishable by and law for the time being in force.

Cyber Crime is the term used to broadly describe criminal activity in which computer and computer networks are a tool, a target, or palace of criminal activity and incudes everything for electronic cracking to denial of crevice attacks.it is also used to include traditional crime in which computer and networks and used enables the illicit activity. Computer crime mainly consist of authorized access to computer system data alteration, data destruction ,theft of intellectual properly.Syber crime in the context of national security may involve heactivism,traditional espionage, or information warfare and related activities.

There isn't really a fixed definition for cybercrime. TheIndian Low has not given any definition to the term 'cybercrime' in fect,the Indian penal code does not use the term 'cybercrime 'at any point even after its amendment by the information technology (amendment) Act 2008,The Indian cyber law ,But cyber security'' is defined under section (2) (b) meansprotecting information ,quipment,device ,computer,coputer resource, communication device and information stored there in from unauthorized access ,use,discloser,disruption,modification or destruction. Cybercrime have been reported across the word. Unlike in traditional crime, The information technology infrastructure are not only used to commit the crime but every of is itself the target of the crime.

Reasons For Cyber Crime

Hart in his work "The concept of law" he said human beings are vulnerable so rule of law is required to protect them'. Allying this to the cyberspace we may say that computer are

vulnerable so rule of is required to protect and safeguard them against cybercrime. The reason for the vulnerability of commuters may be said to be:

1. Capacity to Store data in comparatively small space-
   This computer has unique cheristrick of storing data in very small apace. This affords to remove or device information either through physical or virtual medium makes it much easier.
2. Organized Hackers-
   These kind of hackers are mostly organized together to fulfill certain objective. Thereason may be to fulfill their political base .fundamentalist, etc. ThePakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfill tier political objective. Further the NASA as well as the Microsoft sites is always under attack by the hackers.
3. Professional Hackers/Crackers-
   Their work is motivated by the color of money. Thesekinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information.Fuerther they are even employed to creak the system of the employer basically as a measure to make it safer by detecting the loopholes.
4. Discontented employees-
   This group includes those people who have been either sacked bytheir employer or are dissatisfied with theiremployer. Toeven, they normally hack the system of their employee.
   Mode of Cyber Crime.
   1. Cyber Stalking: Cyber Stalking is using of The Internet OR other electronic means to stalk someone. This term is used interchangeably with online hersmenent and online abuse. Stalkinggenerally involves harassing or threatening behavior that an individual engage in repeatedly, such as following a person, appearing at a person's at home or place of business ,makingharassing phone calls, leaving written message or objects. Orvandalizing a person's property.
   2. Hacking: "Hacking" is crime, which entitlecreaking's system and gaining unauthorized access to the data stored in them.Hackinh had Witnessed a 37 percent increase this year. Hacking is not defined in the Amended IT Act, 2000.Accordingwikitionary, 'hacking 'meansunauthorized attempt to bypass the securitymechanism of an information system or network. Also, in simple words, 'hacking' is the unauthorizedaccess to a computer system, programs, and data network resources. (The term 'hacker' originally meant a very gifted prograamer.in recent year though, witheasieraccess to multiple systems, it now has negative implication.)
   3. Phishing : "Phishing" is just one of the many frauds on the internet, typing to fool people parting which their money.Phising refer to the receipt of unsolicited emails by customers of financialinstitution, requesting them to enter their username, password or other personal information to access their account for some reason ,customer are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the frauds contained in that account.

F-secure Corporation's summary of 'data security' threats during the first half of 2007 ha shriveled that the study found the banking industry as soft target for fishing scams in India [The business line Monday July 23 2007].

4. Cross Site Scripting: Cross- site scripting (XSS) is a type of computer security vulnerability typically found in web application which allows code injection by malicious web user in to the web pages viewed by other users. Example of such code includes HTML code and client-said scripting vulnerability can be used by attackers to bypass access controls.
5. Vising:"Vising" is the Criminal practice of using social engineering and voice over IP (VoIP) to gain access to private ,personal and financialreward. The term is a combination of "voice" and phishing. Vising exploits the public's trust in landline telephone cervice,which have traditionally terminated in physical location which are known as to the Telephone company .and associated with a bill. Payer. The victim is often unaware that VoIP allows for caller id spoofing, in expensive, complexautomated system and anonymity fir the bill payer.

   Vising is typically used to still credit card numbers or other information used in identity theft schemes from individuals.
6. Cyber Squatting:Cybersquatting is the act of resist earing a famous domain name and them selling it for a fortune. This is an issue that has not been tackled in IT act 2000.
7. Bot Networks: A cybercrime called 'Bot networks', where in spinstersand other perpetrators of cybercrimes remotely tack control of computers without the users realizing it, creasing at an alarming rate. Computers get linked to Bot networks when users unknowingly download malicious code such as Trojan horse sent as a e-mail attachment ,such affected computers .known as zombies can works together whenever the malicious code William them get activated ,and those who are behind the boat network attacked get the computing power of thousands of system at their disposal.atteakers offer coordinate large group of Bot-controlledsystem, or bot networks to scan for vulnerable system and use them to increase the speed and breadth of their attacks.

Trojan horse provides a backdoor to the computeracquired. A Backdoor 'is a method of bypassing normal authentication or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor .may tack the form of an installed program, or could be a modification to a legitimated program.Bot networks create unique problem for organization become they can be remotely upgraded with the new exploits very quickly and this could help attackers pre-empt security affords.

Classification

The subject of cybercrime may be broadly classified under the following three groups, they are-

1. Against Individuals
   a. Their person &
   b. Their property of an individual
2. Against Organization
   a. Government
   b. Firm, Company, Group of individuals.

3. Against Society at large

The following are the crimes, which can be committed against following groups

Against Individuals:-

i. Harassment via e-mails.
ii. Cyber-stalking
iii. Dissemination of obscene material.
iv. Defamation
v. Unauthorized control/access over computer system.
vi. Indecent exposure.
vii. Email spoofing
viii. Cheating and fraud

Against individual property:-

i. Computer vandalism
ii. Transmitting various
iii. Netrspass
iv. Unauthorized control/access over computer system.
v. Intellectual property crimes
vi. Internet time thefts.

Against Organization:-

i. Unauthorized control/access over computer system.
ii. Position of unauthorized information
iii. Cyber terrorism against the government organization
iv. Disributation of pirated software etc.

Against Society at Large :-

i. Pornography (basically child pornography).
ii. Polluting the youth Through indecent exposer
iii. Trafficking
iv. Financial crime
v. Sale of illegal article
vi. Online gambling
vii. Forgery

What is Cyber law?

Cyber law is a term used to describe the legal issues related to use of communication technology ,perticulerly “cyberspace” ,i.e. The internet.it Is less of a district filled of law in the way that property,privacy,freedom of expression and jurisdiction, inabsence ,cyber law is an attempt to applies laws designed for the physical world, to human activity on the internet.IN India, The IT Act,2008 is known as the cyber law. It has a separatecheater XI entitles “offence” in which various cybercrimes have been declared as penal offences punishable with imprisonment and fine.

Law & Punishment for different Cyber crime

1. Hacking: As stated earlier, “Hacking” is a crime, whichentitlescracking system and gaining unauthorized access to the data stored in them.

Law & Punishment : Under Information technology (Amendment) Act,2008.Section 43(a) read with section 66 is applicable and section 379 & 406 Indian penal code,1860 also are applicable .f crime is proved under IT Act, Acused shall be punished for imprisonment, which may extent to three years or with fine, which may extend to five lakh rupee or both. Hacking offence is cognizable, boilable, and compoundable with permission of the court before which the prosecution of such offence is pending and treble by any magistrate.

2. Data Theft: According to Wikipedia, data thief is a growing problem primarily paper trited by office worker with access to technology such as desktop computers and handheld devices, capable of storing digital information such flashdrivers, iPods and even digital cameras. The amazed caused by data thief can be considerable, with today ability to transmit very large files via e-ails, webparesis devices, DVD storage and other hand-held devices.

   According to information technology (Amendment) Act ,2008 section 43(b) is stated as –if any person without permission of the owner or any other peso ,who is in charge of a computer, computersystem of computer network-downloads, copies of extra any data ,computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data thief.

   Law &Punishment: Under Information Technology (Amendment) Act, 2008, section 43(b) read with section 66 is applicable and under section 379,405 & 420 of India panel code, 1860 also applicable.

   Data theft offence is cognizable, billable, compoundable with permission of the court before which the prosecution such offence is pending and tribal by any magistrate.

3. Spreading Virus Worms: In most cases, viruses can do any amount of damage; the creator intends them to do. They can you're your data to a third party and then deleteyou data from your computer. They can also ruin/mess up yoursystem and render it unusable without re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Sally the virus will install files on your system and then will change your system so that virus program is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victim.

   Law & Punishment : Under Information Technology (Amendment) Act,2008,section 43(c) & 43(e) read with section 66 is applicable and under section 268 of India panel code,1860 also applicable.spreding of virus offence is cognizable bailable,copaondable with permission of the court before which the prosecution such offence is pending and tribal by any magistrate.

4. Identity theft : According to wikipidia,Identity theft is a form of fraud or cheating of other person's identity is which someone pretends to be someone else by assuming that person's identity, typically in order to access to resources or obtaincredit and other benefit in that person's name. Information Technology (Amendment) Actr,2008.Crime of identity theft under section 66-

C,whoever Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification future of any other person known as identity theft is a term used to refer to fraud that involves stealing money or getting other benefit by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity only to use it.The person whose identity is used can suffer various consequences where they are held resnsonsible for the operator'saction. At one time the only way for someone a steal somebody else's identity was by killing that person and talking his place, it was typically a violent crime.however,since then, the crime has evolved and todays white collared criminal are a lot less brutel.But the ramification of an identity theft are still scary.

Law & punishment : Under Information technology (Amendment) Act,2008.Section 66 –C and section 419 of India penal code,1860 also applicable identity theft offence is cognizable bailable,copaondable with permission of the court before which the prosecution such offence is pending and tribal by any magistrate.

5. E-mail spoofing : According to wikipidia,e-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mails headers are altered to appear as though the e-mail originated from a different source's-mails spoofing was send by someone else. A spoof e-mail is one that appears to originate from one source but actually has been sent from another source .spoofing is the act off electronicallydisguising one computer as another for gaining as the password system.it is becoming as common that you can no longer tack from granted that the e-mail you are receiving it truly from the person identified as the sender.

   E-mail spoofing is a technique hacked by hacker to fraudulently send e-mail messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual sorce.Hackers used this method to disguise the actual email address from which fishing an spam massage are sent and often use email spoofing is conjunction with web page spoofing to trick users into providing personal and confidential information.

   Law & Punishment: Under Information technology (Amendment) Act, 2008.Section 66 – D and section 417,419 & 465of India penal code, 1860 also applicable-mails spoofing offence iscognizable billable, compoundable with permission of the court before which the prosecution such offence is pending and tribal by any magistrate.

   Conclusion

   Prevention is always better than cure. Anativeshould tack certain Precaution while operating the internet and should follow certain preventive measures for cybercrimes which can be defined as:

   - Identification of exposer through education will assist responsible companies and firms to meet these challenges.

- One should avoid disclosing any personal information to stranger via e-mail or while chatting.
- One most avoid sending any photography to strangers by online as misusing of photograph incidence increasing day by day.
- An update Anti-virus Software to guard against virus attacks should be used by the all the denizens and should also keep back up volume so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children's are accessing, to prevent any kind of harassment or deprivation on children.
- Website owner should watch traffic any check any irregularity on the site .It is the responsibility of the website owners to adopt some policy for preventing cybercrimes as numbe4r of internet user are grooving day-by-day.
- Web server running public site must be physically separately protected from internet corporate network.
- It is batter to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the legislatures keeping in mind the interest of antigens.
- IT departmentshould past certain guidelines and notification for the protection of computer systems and should also bring out with some more strict laws to break down the criminal activity relating the cyberspace.
- As cybercrimes is the major threat of all the countriesworldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victim of cybercrimes by way of compensatory remedy and offenders be punished with highest type of punishment so that it will highest type of punishment so that it will anticipate the criminals of cybercrime.

Reference:

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
3. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
4. Steve Morgan (17 January 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved 22 September 2016.
5. B.M.Gandhi. Indian Penal Code. India: Eastern Book Company. p. 41. ISBN 9788170128922.
6. "Cyber Crime Investigation Cell". Cyber Cell Mumbai. Cyber Crime Investigation Cell, Mumbai. Retrieved 16 May 2017.