© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Cyber Crimes : An Overview

Jyotsana Choudhary
Assistant Professor, Department of Law, Chaudhary Devi Lal University,Sirsa, Haryana, India

ABSTRACT

Present article is an overview of cyber crimes and other related issue. It has been written in order to generate awareness and educate concerned persons about the threat of cyber crimes. In this digital age we came across about various cyber crimes in form of stalking, hacking, spoofing, phishing, financial frauds among various other types. Cyber crimes have posed a grave threat to the execution of various governmental services through the digital platform. Present article is written in a general manner and it also discusses some preventive measures in order to deal with the menace of cyber crimes.

Keywords: Cyber crime meaning, hacking, spoofing, crimes against person, property, government, society; preventive measures.

I. INTRODUCTION

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term **'Cyber'** became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well.

Though the word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both".

The world 1st computer specific law was enacted in the year 1970 by the German State of Hesse in the form of 'Data Protection Act, 1970' with the advancement of cyber technology. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. It is under these circumstances Indian parliament passed its "INFORMATION TECHNOLOGY ACT, 2000" on 17th oct to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes.

Cyber Crimes Actually Means: It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail,

spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Classifications Of Cyber Crimes: Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:

II. CYBER CRIMES AGAINST PERSONS

There are certain offences which affects the personality of individuals can be defined as:

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- Cyber-Stalking**:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- Dissemination of Obscene Material**:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- Defamation: It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- Cracking: It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- Child Pornography: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- Assault by Threat: refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

III. CRIMES AGAINST PERSONS PROPERTY

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- *Intellectual Property Crimes:* Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- *Cyber Squatting:* It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- *Cyber Vandalism:* Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- *Hacking Computer System:* Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- *Transmitting Virus:* Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- *Cyber Trespass:* It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- *Internet Time Thefts:* Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft There are certain offences done by group of persons if your Internet time has to be recharged often, despite infrequent usage.

IV. CYBERCRIMES AGAINST GOVERNMENT

- It includes intending to threaten the international governments by using internet facilities. It can be classified as:

- *Cyber Terrorism:* Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

- *Cyber Warfare:* It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- *Distribution of pirated software:* It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- *Possession of Unauthorized Information:* It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

V. CYBERCRIMES AGAINST SOCIETY AT LARGE

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- *Child Pornography:* It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- *Cyber Trafficking:* It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- *Online Gambling:* Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- *Financial Crimes:* This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- *Forgery:* It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Affects To Whom: Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. In the modern cyber world cyber crimes is the major issue which is affecting individual as well as society at large too.

Need of Cyber Law: information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

Penalty For Damage To Computer System: According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine upto 1crore to the person so affected by way of remedy. According to the Section:43A which is inserted by

'Information Technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Case Study-Attacks on Cyberspace:

- *Worm Attack*: The Robert Tappan Morris well Known as First Hacker, Son of former National Security Agency Scientist Robert Morris, was the first person to be prosecuted under the 'Computer and Fraud Act, 1986'. He has created worm while at Cornell as student claiming that he intended to use the worm to check how large the internet was that time. The worm was uncontrollable due to which around 6000 computer machines were destroyed and many computers were shut down until they had completely malfunctioned. He was ultimately sentenced to three years probation, 400 hours of community service and assessed a fine of $10500. So there must be strict laws to punish the criminals who are involved in cyber crime activities.
- *Hacker Attack*: Fred Cohen, a Ph.D. student at the University of Southern California wrote a short program in the year 1983, as an experiment, that could "infect" computers, make copies of itself, and spread from one machine to another. It was beginning & it was hidden inside a larger, legitimate program, which was loaded into a computer on a floppy disk and many computers were sold which can be accommodate at present too. Other computer scientists had warned that computer viruses were possible, but Cohen's was the first to be documented. A professor of his suggested the name "virus". Cohen now runs a computer security firm.
- *Internet Hacker*: Wang Qun, who was known by the nickname of "playgirl", was arrested by chinese police in the Hubei province first ever arrest of an internet hacker in China. He was a 19 year old computing student, arrested in connection with the alleged posting of pornographic material on the homepages of several government-run web sites. Wang had openly boasted in internet chat rooms that he had also hacked over 30 other web sites too.

Preventive Measures For Cyber Crimes:

Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes 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 are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility

of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmes 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 netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

VI. CONCLUSION

Since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by netizens while using the internet which will assist in challenging this major threat Cyber Crime.