A STUDY ON THE OFFENCES RELATED TO CYBERCRIME AND CYBERSPACE

Kismat, Geeta Institute of Law, Panipat, Haryana, India

ABSTRACT

Cybercrime directly refers to the activities which are particularly done with using the various modes of communication technology equipments such as the cyberspace, the internet, the world wide web, etc. Generally, cybercrime is also known as the computer oriented crime. Cyber crimes are done using the components such as the internet or includes illegal online activities which are inculcated using the medium of internet. This internet crime is also referred to as the branch of the cybercrime. Many of the cyber crimes are also penalized by the IPC. Cyber crimes also includes offences under which penalty or compensation has to be fulfilled by the wrongdoers. Compensation or Penalty for the damage to the computer system are also permitted under the cyber crime. Whosoever fails to obey the rules which are made under the cybercrime are liable to pay compensation or penalty. Anyone who knowingly or intentionally destroys someone's computer data or computer source shall be punishable with imprisonment. Anyone who works through the source of online medium must be aware of the rules and who so ever is injured by the hackers must report it as there are various punishments and penalties which would satisfied the people those who suffers from those crimes. Thus, cyber crime also plays a role in spreading wrong information to the people which makes them fool by doing fraud with them.

1. INTRODUCTION

The term Cybercrime is used to denote criminal activities which is an act particularly punishable by the state. The tools of networks such as computers or computer networks, internet, etc. are the activities that give place to the criminal activities. The life of humans has become easier after the invention of computers as we know that the computer is an electronic device which helps us in storing data. Most of the users of the computers uses the computers for the purposes of their benefits and that leads to the birth of "Cyber Crimes". This leads society to illegal engagements. As we all know that the cyber crimes are always committed through the modes of computer networks, computers or the internet. Cyber Law is known as the laws which govern the area of cyberspace. The Cyber Law mainly comprehends digital and electronic signatures, cyber crimes, privacies and data protection, etc. "United Nations Model Law on Electronic Commerce" Model (UNCITRAL) (4) was the first IT Act that was recognised by the UN's General Assembly. Traditional espionage, activism, or information warfare, related activities, false in the context of national security in the cybercrime.

2. OBJECTIVES

The main motive of my paper is only to straighten out great information regarding the offences or the crimes which take place through the medium of networks. Cyberspace also plays an important role in the involvement of Cybercrimes. In the year 1820, the first cybercrime was recorded. Since 3500 B.C Japan, India and China includes primaeval types of computers. Joseph Marie Jacquard, a textile manufacturer in France, in the year 1820, created the loom.

3. TYPES OF CYBER CRIMES

Almost for all the Cybercrimes computer is an indispensable tool. As the communication networks are increasing such as the internet, the numbers of hackers are also increasing. For the evidence of the offence, the computer is a major target and a tool that is mostly used in the offence. The criminal statutes would result in the different or various uses of computers.

The goal of the criminal is majorly to steal the information from the computer system, computer or computer networks when the computer is targeted of the offence. The different forms of crime that target the computer are espionage, hacking, cyberwarfare and malicious computer viruses. Professionals, teenage, students or the terrorists could be the perpetrators of the offence. Therefore, there are various different types of Cyber crimes today-

A. Cyberstalking

The electronic means to stalk someone with the use of internet is known as cyberstalking. Online abuse and harassment are related to Cyberstalking. [1]It involves threatening behaviour or harassment towards the individual. It harasses an individual by obtaining its personal information such as person's home address, place of business, leaving written messages or making harassing phone calls, etc. This can afraid or spoil the life of the victim and could threatened him.[2]

Usually, cyberstalking occurs with women and they are severally stalked by men. Females are the main targets including emotionally weak people, children or unstable people, etc. Majorly 75% of the females are victim of cyberstalking. Many times men are also stalked. Most of the cyber crimes go unreported.

B. Hacking

The crime 'hacking' [3]entitles the un-authorized data's access stored in the computer system and and tails cracking or hacking. In this year, 37% hacking had been witnessed. The hackers obtain the residential addresses of the victims from the email accounts of certain web portals of the residents of the cities. The hacking is normally done by the use of 'backdoor' program which is particularly installed on the systems. The hackers also tries to access the data of the users by password cracking software, in which they tries billions of password for accessing the correct passwords of the computer users. One must change their password regularly from preventing hacking from the hackers.

C. Phishing

Phishing[6] is the act of making fraud over the internet which includes fooling the people. It involves accessing the username, password or personal information by the emails of the customers from the financial institutions. Customers are not aware about the fake websites and when they click on the links over the emails to enter their personal information, fraud constitutes with them. The frauder access the personal bank account details of the customers

[1] Available online at www.irjet.net. International Research Journal Engineering and Technology.
[2] Available online on http://www.lawyersclubindia.com/articles/classification of cyber Crimes.
[3] Available online at http://www.netmeg.net/jargon/terms/h/hacking/.html/ The Jargon dictionary.
[6] Available online at http://www.indiankanoon.org/doc/1439440.

and misuses them.

Phishing is a type of fraud in which the frauder falsely sends wrong information to the customers in enhancing himself to be a established legitimate institution, so that he could access the personal information of the customers for the purpose of Identity theft. The frauder directs the user to access the website and ask them to update their private information such as credit card information, password, bank account numbers, social security, etc. so that he could steal the information of the user. This is also known as the method of email fraud.

D. Drug Trafficking

Drug trafficking uses latest technologies to sell narcotics for encrypting mails. Drug traffickers contribute a major role in the cyber crime. They manages all the plans for making the exchange of drugs through couriers. There happens a personal communication between the buyer and the dealer for the exchange of the drugs. Thus, drug trafficking contributes a part in the involvement of Cyber crimes.

E. Bot Networks

The 'Bot Networks' is also known as cybercrime, in which the spamsters took over the control of the user's computers. It is increasing on an alarming rate as the user gets unaware of it. The computer automatically gets linked to the bot networks when the users unknowingly operates malicious codes on their computers by accepting the email sent by the spamsters or other perpetrators. When the malicious codes gets activated within those computers the bot network spamsters attacks the computer by activating thousands of systems in it. Computer Emergency Response Teams (CERTs) have been established by the countries including India with and objective to secure the incidents / events. The internet has become a source of many funding to terrorist and money laundering in an organised manner. [4]

F. Spamming

Junk email is also known as email spam. This email is a type of unsought mass message which is particularly sent through the email. From the 1990s, the use of spam messages have widely become popular and it creates lots of problem to the email users in their life at daily basis. The email addresses of the users are obtained by the spam bots, the spam bots are a type of automatic

[4] Internet Crime and Cyber Terrorism, http://www.dfaitmaeci.gc.ca/international crime/cybercrime-en.asp.

program that uses the internet for the use in searching the email addresses of the users over the internet. The email distribution list is used by the spammers to use spam bots. When the spammers receives response from the other users, they automatically sends the emails to the email addresses of millions of users over the internet.

G. Cyber Defamation

Cyber defamation means defamating the reputation of an individual through the cyberspace in the eyes of others. The spammers purpose was to defame the users by making defamatory statement so that the reputation of the individual could get affected in front of others. The cyber defamation takes place through the computer or internet. Sometimes the spamsters sends defamatory statement to the email of the user and also to the friend of the user.

H. Theft in the Services of Telecommunications

Theft in the services of telecommunications refers to the access of the switchboard of the individuals in which various criminal organizations access to the switchboards of the users and from there they access the data and obtain the dial out or dial in circuits. From this they are allowed to make any local call or free calls to any distant number. This theft of telecommunication has been considered as to be a misdemeanor and it is one of the earliest crime throughout the cybercrime.

I. Financial Crimes

Financial crimes have increased at an alarming rate with the increase in the demand of the online banking. Stealing money by online from the banks, credit card frauds, etc. are the parts of financial crimes. The frauders gathers information from the victims by impersonating themselves as the part of financial organisation or identifying themselves as government officials and ask them to tell about their credit information and makes the fraud to them. The victims unknowingly gives their information to the criminals without proper enquiry and false pray to them. The criminals often hide their identities which results in the financial damages to the victims.[5]

[5] Financial crimes, Available at http://www.statista.com/statistics/financial damage-caused-by-cybercrime.

J. Intellectual Property Crimes

Intellectual Property crimes are the crimes those includes trademarks violations, software piracy, copyright infringement, theft of computer source code, etc.

K. Online Gambling

Online gambling is one of the most important sites for the money launderers. These websites have their servers at abroad and offers thousands of websites through abroad services. Money launderers are the websites of many fronts online gambling.

L. Sale of Illegal articles

Sale of illegal articles includes the sale of weapons, wildlife, narcotics, etc. by uploading informations through the auction websites, bulletin boards, websites, email communications, etc. In the name of 'honey' it is believed that many websites in India also selling cocaine.

4. OFFENCES RELATED TO CYBERCRIME IN INDIA

Penalties, Compensation and Adjudication under Information Technology Act, 2000.[6]

According to **Section 43-** "Where a person without the permission of the owner or the other personin-charge damage the computer, or computer system, or computer network, that he shall be liable for Penalty and Compensation to the person so affected".

According to **Section 44-** "Where a person fails to furnish any document, return, report to the controller, or certifying authority, then he shall be liable to pay penalty up to Rs. 1,50,000/- per failure. Further where a person fails to furnish any information, books or other documents within time specified, then he shall be liable to pay penalty up to Rs.5,000/- per day. Further provided that where a person fails to maintain books of accounts or other records, then he shall be liable to pay penalty up to Rs.10,000/- per day".

According to **Section 65- "**Tempting with the computers source documents. Whoever intentionally or knowingly destroy, conceal or change any computers source code that is used for a computer, computer program, and computer system or computer network".

[6] Penalties, Compensation in Indian Technology Act, 2000.

Punishment:

A fine of Rs. 2 lakhs and three years imprisonment would be sentenced to the person who is involved in this crime.

According to **Section 66-** "Hacking with computer system, data alteration, etc. whoever with the purpose or intention to cause any loss, damage or to destroy, delete or alter any information that resides in a public or any person's computer. Diminish its utility, values aur effects it injuriously by any means, comets hacking".

Punishment:

A fine of Rs. 2 lacs and 3 years imprisonment would be sentenced to the person who is involved in this crime.

According to **Section 66A-** "Sending offensive messages through any communication services. Any information or message sent through any communication services this is offensive or has threatening characters. Any information that is not true or is not valid and is sent with the end goal of annoying inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will. Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages".

Punishment:

The person would be sentenced to three years imprisonment along with the fine imposed on him who is found involved in such crime.[7]

According to **Section 66B-** [11]" Receiving stolen computers resources or communication devices dishonestly".

Punishment:

The individual would be sentenced to 3 years of imprisonment along with fine of Rs. 1 lakh who is found involved in such crimes.

According to **Section 66C-** " Identity theft. Using of one's digital or electronic signature or

[7] Penalties and Offences available online at http://niiconsulting.com/ Information Technology Act, 2000.
[11]Introduction to Cyber law Act, 2000, India. Available online at https://www.slideshare.net/an

one's password or any other unique identification of any person is a crime".

According to **Section 67A-** " Transmitting aur publishing of materials tha contains sexually explicit contents, acts etc. in electronics form. Whoever transmits aur publishers materials that contains sexually explicit contents or acts shall be sentenced".

According to **Section 67B-** " Transmitting or publishing of materials that depicts children in sexually explicit act etc. in electronics form. Whoever transmits or publishes any materials that depict children in any sexually explicit act or conduct in an electronic form shall be sentenced".

According to **Section 67C-** " Retention and preservation of information by intermediaries. Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the central government may prescribe. Any intermediaries knowingly or intentionally contravene the provision of the subsection".

According to **Section 69-** " Power to issue direction for monitor, decryption or interception of any information through computers resources. The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carried out, shall be such as may be prescribed.

Providing safe access or access to computers resources".

According to **Section 70-** " . Unauthorized access to protected system".

According to **Section 71-** " Penalty for misrepresentation".

According to **Section 72-**" Breach of confidentiality and privacy".

According to **Section 73-** " Publishing false digital signature certificates".

According to **Section 74-** " Publication for fraudulent purpose".

According to **Section 75-** " Act to apply for contravention or offence that is committed outside India".

According to **Section 77-** " Compensation, confiscation or penalties for not to interfere with other punishment".

According to **Section 77A-** " Compounding of Offences".

According to **Section 85-** " Offences bike companies".

According to **Section 503** of IPC- "Sending threatening messages by email".

According to **Section 499** of IPC- " Sending defamatory messages by email".

According to **Section 420** of IPC- " Bogus websites, cyber frauds".

According to **Section 463** of IPC- " Email spoofing".

According to **Section 383** of IPC- " Web jacking".

According to **Section 500** of IPC- " Email abuse".

According to **Section 507** IPC- " Criminal intermediation by anonymous communications".

Conclusion

From this study, this had been found that there are many ways through which the individual possesses crimes through cyberspace. The rise of new technologies is the main cause of Cyber crimes in the recent years. It had led to a great threats to the mankind at large. The offences in the cybercrime are punishable by the law. The main purpose of writing this paper is just to straighten out the knowledge of Cyber crime among those individuals who are unaware of it. "A brief study on offences related to cybercrime and cyberspace" I would like to covey that Cyber crimes shall never be acknowledged. If the criminals won't get punishment for their deed, they will never stop. One must report who faces these types of criminal activities related to cyber crime or cyberspace.