CYBER MONITERING

*Tejashwani Pabbi, **Disha Ghai, ***Poonam Pabbi
*Asst Professor , MBA Deptt , Guru Kashi University, Talwandi Sabo
**Lecturer, Applied sciences, Regional Polytechnical College, Behman diwana , Bathinda
***Student, ECE Deptt, GRDIET, Lehra Begga, Bathinda

ABSTRACT
The growing use of internet allows everyone to get attached with the world, but this also enables the participation of anti social elements to enter this world and commit cyber crimes .Cyber law is a much newer phenomenon having emerged after to check the cyber crime. Internet grew in a completely unplanned and unregulated manner. Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. The growth rate of cyberspace has been increasing enormous day by day. Internet is growing rapidly and with the population of doubling roughly every 100 days, Cyberspace is becoming the new preferred environment of the world. With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. The internet in India is growing at very fast pace, It has created many new opportunities in every field we can think of – be it entertainment, business, sports or education. There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cybercrime – illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spam's, and software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise. The lack of vision to get rid off this is the major issue; the government has to take some important steps in order to maintain law an order in the cyber space. Also the main reason is the implementation of these laws was very slow and somewhere nobody matter about this.
The Cybercrime can be everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money and using this information against anyone which effect the person , property or government ".
"The modern thief can steal more with a computer than with a gun.
Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb"[1]

1.2 TYPES OF CYBER CRIME

Cyber crimes can be basically divided into 3 major types

- Those against persons.
- Against Business and Non-business organizations.
- Crime targeting the government. [2]

1.2.1 Cyber crime against Persons

Financial Claims: This would include cheating, credit card frauds, money laundering etc.
Cyber Pornography: This would be the use pornographic websites; pornographic magazines produced using internet & computer (down load and share pornographic pictures, photos, writings etc.)
Sale of illegal articles: It refers to the sale of narcotics, weapons and wildlife etc., by sharing the information on websites, bulletin boards or simply by using e-mail communications.
Online gambling: There are numbers of websites ,hosted on servers abroad, that offer online gambling.
Intellectual Property Crimes: IP crime related to software piracy, copyright infringement, trademarks violations etc.
E-Mail spoofing: A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging.

Forgery: Copy of currency notes, postage and revenue stamps, mark sheets etc., can be forged using latest computers, printers and scanners.
Cyber Defamation: This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person's friends. [3]

Related Example:
A minor girl in Ahmadabad was lured to a private place through cyber chat by a man, who, along with his friends, attempted to gang rape her. As some passersby heard her cry, she was rescued.[7]

1.2.2 Cyber crime against Business and Non-business organizations.
Threat of Unauthorized access to computer system or network: This activity is commonly referred to as hacking. The Indian Law has however given a different connotation to the term hacking.
Theft of electronic information: This related to the theft of the information stored in computer hard disks, removable storage media etc.
Bombing E**-Mail:** Email bombing is a process of sending a large number of e-mails to the victim resulting in the victims' e-mail account or mail servers.
Salami attacks: The attacks are used for the purpose of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer.
Denial of Service: This includes flooding computer resources with more requests than it can handle. This causes the computer resources to crash at the mean time denying authorized users the service offered by the resources.
Virus/worm: Viruses are mainly programs are made in such away that it attach themselves to a computer or a file and then circulate themselves to rest of the files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.
Logic bombs: These are dependent programs which is made to encounter at a specific time, means programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.
Use of Trojan Horse: A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
Internet Usage Theft: This linked with the usage by unauthorized persons of the Internet hours paid for by another person.
Physically damaging: This crime is committed by physically damaging a computer or its peripherals or by altering IP's etc.
Related Example: In the United States alone, the virus made its way through 1.2 million computers in one-fifth of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug"[3][4]

2.0 CYBER LAW
India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes

along with certain other provisions scattered in this Acts .These laws are generally based on the cases held earlier.

The various offences which are provided under this

2.1 Offence	**Section under IT Act**
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73
Computer Related Crimes Covered under Indian Penal Code and Special Laws	
2.2 Offence	**Under IPC**
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec 463 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 463 IPC
Web-Jacking	Sec 383 IPC
E-Mail Abuse	Sec 500 IPC

[5][6]

3.0 Protection to Cyber crime

1. **Awareness:** The main protective measure that points of Individual, business house and government is the awareness about the cyber crime. Just like ignorance of law is of no excuse, similarly ignorance of unlawful activities is also of no excuse. If we are using the computers, internet and all allied accessories, this means we are responsible for all the outcomes. We should have to prepare our self to fights with the crime by updating knowledge and using recent software's and techniques etc to protect the authenticity& security of the material & also this type of crime happens immediately report t to the judiciary.
2. **Proper security**: Proper installation of the combination Firewalls, Routers, Gateways so that any external person is not able to enter in your domain.
3. **Honey pots**: Business house and governments can also use **Honey pots** for conquering the cyber criminals. honey pots are the term used for the computer system which is deliberately set to attract and trap the criminals who attempt to enter into others people's computer system.[7][8]
4. **Strong passwords**: The passwords used in the security entrance should be lengthy, because a short password can be cracked easily. Do not enclose your password to anyone, use only secure port for banking and other shopping purposes.

5. **Hard cyber laws/ Proper implementation**: Hard rules are to be made so that these types of crime should be ceased. We have many laws but the implementation part is not so strong, that should be must strong enough.
6. **Detection of fraudulent E-mails:** On the detection of fraudulent e-mails one must report it, so that the source can be detected or a warning alert should be sent to the users. Also do not enclose any information regarding account no, D.O.B, address, etc.
7. **Use Encrypted information**: The use of encrypted language is also a very commonly used techniques. In this techniques the data/information is stored in some encryption means it is coded. It becomes very difficult for any criminal to crack the codes/ encryption. [9][10]
8. **Watchdogs/use intrusion alert programs**. As we discuss earlier that there must be some alert programs which tell us about the penetration of some unknown/known elements who will be a threat to the system[11]
9. **Don't rely on the free to download & installed software etc:** The main problem for the cyber crime that mostly we use free to download software's as well as these are not from the authentic modes/sites, which can also harm our security system .[12][13][14][15]

4.0 Conclusion

The wide use of the computers & internet is very important of human life. The use of sophisticated tools for knowledge gathering, interpreting & sharing is very effective, time saver and economic. But the new generation thieves find it easy to capture and use the

data/information as they want to use . So the solution to the problem is that prevent it as the old proverb says that "Prevention is better than cure". The probing is to be done like honey pots to capture these criminals. Also knowledge is also an important constrain for that. We have to update our knowledge in order to catch the crime

The era of computers open as many windows /option as one can think for any problem but also it can open as many problem as one cannot imagine it can be.

References

[1] http://www.crimeresearch.org/analytics/702/
[2] http://www.cyberlaws.net/new/faqscybercrime.php
[3] http://www.cidap.gov.in/htmlfiles/cybercrimes.html
[4] http://www.cyberlawclinic.org/cyberlaw.htm
[5] http://searchsecurity.techtarget.com/definition/honey-pot
[6] http://www.cidap.gov.in/documents/cyber%20Crime.pd
[7] http://www.tracking-hackers.com/papers/honeypots.html
[8] http://www.cidap.gov.in/documents/cyber%20Crime.pd
[9] http://www.mrp3.com/encrypt.htmlhttp://www.cyberlawclinic.org/cyberlaw.htm
[10] http://www.wisegeek.com/what-are-the-different-encryption-techniques.htm
[11] http://www.ganssle.com/watchdogs.htm
[12] http://www.fbi.gov/scamssafety/computer_protect
[13] http://www.makeuseof.com/tag/top-five-computer-crimes-protect/
[14] http://www.crime-research.org/news/08.02.2006/cybercrime-protect-your-computer/
[15] http://indiacyberlab.in/cybercrimes/safety.htm