“CYBER CRIMES IN INDIA”

SARIKA .K.

ANAGHA .K.

UNDER THE GUIDENCE OF

Asst. Prof. VIJAYALAKSHMI

V. R. KRISHNAN EZHUTHACHAN LAW COLLEGE

NEMMARA, ELAVANCHERY.

INTRODUCTION

Cyber crime is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Offences that are committed against individuals on groups individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or lost to the victim directly or indirectly. Using modern telecommunication network such as internet (chartrooms, emails, notice boards) and mobile phones (SMS,MMS) such cr4imes may inreaten a nation’s security and financial health issues surrounding these types of crimes have become high profile , particularly those surrounding hacking, copy right infringement, child pornography and child grooming. There are also problems of privacy when confidential information is interpreted or disclosed, lawfully. Cybercrimes are any crimes that involve a computer and a network. In some cases , the computer may have been used in order to commit the crime and in other cases, the computer may have been the largest of the crime.(Cyber crime consist of legal activity conducted on a computer).(Traditional crimes may be committed while using a computer, but cyber crime such as phishing schemes and viruses.)

TYPES OF CYBER CRIMES IN INDIA

1. Cyber crime against person
2. Cyber crime against property
3. Cyber crime against government
4. Cyber crime against society

1.cyber crime against person

In this category crime is committed against a person using electronic service as a medium. Below are some offences that comes under this category

a. Cyber stalking

The term stalking means unwanted or obsessive attention by an individual or group towards another person. Cyber stalking refers to threat that is created through the use of computer technology such as Internet, e-mails, SMS, webcams, phones calls, websites or even videos.

b. cyber crime Hacking

This means gaining unauthorised access over computer system. Screenshots 2 shows message that hacker can post once your system is compromised.

c. Cracking

Cracking refers to digitally removing the copy write protection code that prevents copied or pirated software form running on computers that haven’t been authorised to run it by the vendor of the software. The person who carries out this task if called as Cracker.

There is difference between Hacker and a Cracker. Hacker uses their knowledge to find the flaws in the security of systems where as cracker uses their knowledge to break the law .

d. Defamation: it involves action of damaging the good reputation of someone using computer or electronic service as medium.

e. online fraud: this refers to acts of stealing confidential details of victim such as banking credentials using phishing sites and thereafter withdrawing money from victims account, online lottery scams such as Nigeria lottery scams. Screenshot 3 shows online lottery scam claiming that you have won $5,00,000 amount

f. child pornography: this involves the use of electronic device and service to create, distribute or access materials that sexually exploit minor children.

g. spoofing: the term spoofing means imitate something while exaggerating its characteristic features with some personal gain or profit. Spoofing of user identity can be described as a situation in which one person or program successfully masquerades (means pretending to someone is not as another by falsifying dat. Spoofing can be done using email or sms or whatsapp

2.cyber crime against person

In this category crime is committed against property of person using electronic service as a medium. Below are some offence that comes under this category:

a. Transmitting virus: A computer virus is malware program that reproduce itself into another computer programs, disk drive, files or booting sector of hard drive. Once this replication of so called virus is succeeded the areas affected are termed as “ infected” Hacker generally transmit virus to target system using email attachment as medium. When victim opens to attachment this virus grts replicated throughout the system and thereby slowing down your system.
b. Cyber squatting

The term squatting means unlawfully occupying an uninhabited place. Cyber squatting is where two or more persons claimed for the same Domain Name or any service available on Internet such as face book profile etc. The hacker climes That he/she had first registered the name before other person or he/she is the owner for twitter handle.

c. Cyber vandalism

Vandalism refers to action involving deliberate destruction or damaging the data when a network service is unavailable.

d. Intellectual property crimes
Intellectual property are intangible property that is the result of creativity such as copyrights, trademark, patent etc. Intellectual property right (IPR) crime is any unlawful act by which the owner is deprived of his/her rights completely or partially. These are the most common offence occurring in India and includes software piracy, infringement of patents, designs, trademark, copyright, theft of source code etc.

3. Cyber crime against government

In this category crime is committed against government by using internet facilities.

a. Cyber Warfare

Cyber warfare is internet –based conflict that involves politically motivated attacks on information and its related system .It can disable official websites and networks, disrupt or even disable essential services such as internet connection steel or even alter classified data such as sensex details on official website ,and Cripps financial system such as blocking payment gateways b.CyberTerrorism

One area of a law which they enforce is cyber terrorism which occur electronically. Thus crimes occur against individuals, business organisation and against the government itself.

So much of our lives are accessible electronically now- form your social security number on a job application, to your bank account, to medical records and more. With the greater convenience of using technology , we tried of some degree of security as it is very difficult to stop every instance of cyber terrorism.

Example

Terrorism can occur over the public internet, over private computer servers, or even through a secured government network. There are many ways is which a criminal could use electronic means to incite , fear and violence. It is far less expensive to purchase a computer than to access or bombs, making this approach appealing for many potential criminals world wide it can be anonymous and conducted at a great distance away from the target. For just a few examples, consider these suituations.Domestic terrorists may break into the private severs of a corporation in order to learn trade secrets, steal banking information, or perhaps the private data of their employees.

Potential consequences of cyber Terrorism

Experts in cyber terrorism have pointed out that the potential harm posed by these threats may be exaggerated , but there is some disagreement. If it was to succeed our out dated computer networks owned by the national government could be comprised. Bombs could be detonated or dismantled , private data could be given to our enemies. This may not be an accurate assessment of attention.

4. Cyber crime against society

An unlawful activity done with the intention of causing harm to the cyber space that can be affect entire socity or large number of persons. Below are offences that comes under this category.

a. Online gambling
The term gambling means involving activities that allows chance for money. Online gambling is one of the most lucrative businesses that is growing today. In the list of cyber crimes in india. It is also known as internet gambling or iGambling. The cyber crime incident such as online lottery scam,(particularly those Nigeria lottery scam),online jobs i.e. work from remote location etc.
b. Cyber Trafficking
The term trafficking means dealing or involving in trade activities that is considered to be illegal and is prohibited by cybercrime law. Cyber trafficking carried out using computer and/or computer services.

PERTAINING TO CYBER CRIME IN INDIA

Cyber crimes are increasing day-by-day due to extencive use of internet by people. In order to deal with this government of india (GOL) has imposed information technology Act, 2000 which was enacted with prime objective to create an enabling environment for commercial use of information technology.
There are several different offences related to internet that have been considered to be punishable under the IT Act and IPC (Indian Penal related to internet that have been considered to be punishable under the IT Act and the IPC (Indian Penal Code). An extract of this act is illustrated below:

1. CYBER CRIMES UNDER THE IT ACT
-Section 65: Tampering with computer source documents.
-Section 66:Hacking with computer systems, data alteration.
-Section 67: Punishing obscene information.
-Section 68: Power of controller to give direction.
-Section 69: Direction of control to a subscriber to extent facilties to decrypt information.
-Section 70: Unauthorised access to protected system.
-Section 71: Penalty for misrepresentation.
-Section 72: Breach of confidentiality and privacy.
-Section 73: Publishing false digital signature certificates.

Note: Section 66A has been removed.

There is one such incident related to this section happened recently. A 21- year old palghar (district in Maharashtra which is nearby to virar) girl was arrested on 19 November, 2012 for posting a message on face book that crisis the shutdown in Mumbai due to funeral of Bal Thackeray (former chief Shiva Sena political party in Maharashtra).

Also her friend was arrested " liking" the post. Initially they were arrested under section 295 A of Indian Penal Code (IPC) that stands for hurting religious sentiments and section 66 A of Information Technology Act, 2000. However later a local court dropped all charges against the girls.

2. CYBER CRIMES UNDER IPC AND SPECIAL LAWS

- Section 503 IPC: Sending threatening messages by email.

-Section 499 IPC: Sending defamatory messages by email.

-Section 463 IPC: Forgery of electronic records.

- Section 420 IPC: Fake websites cyber frauds.

-Section 463 IPC: Email spoofing.

- Section 383 IPC: Web-jacking.

- Section 500 IPC: Sending abusive message by email.

3. CYBER CRIMES UNDER THE SPECIAL ACTS

- NDPS (Narcotic drugs and psychotropic substances) Act: Online sale of drugs.
- Arms Act: Online sales of arms and ammunitions.

REMEDIES AVAILABLE FOR THE VICTIM OF CYBER CRIMES

It happens that people who become victim cyber crime doesn't know what to do and even some people don't report the crime thus allow hacker to target next victim. If you become of cyber crime you can report in charge of cyber crime cell falls under the jurisdiction where crime has occurred. Cyber crime cell is present in almost all cities across world.

You can file cyber crime complaint alleging. Cyber crime with following mandatory documents.

1. Cyber crime that involves email abuse, email bombarding ect... should be provided with following documents:

   - Extract the extended headers of abusive email and submit soft copy and hard copy of email. Please note that hard copy submitted should tally exactly with soft copy and should mentioned data and time of email correctly. Never delete such email until cyber crime investigation is completed or the accused is brought charges.

2. Cyber crime that involves hacking of system should be provided with following documents:

- Server logs (both soft copy and hard copy).
- Duplicate copy of defaced web page (both soft copy and hard copy) in case your website is defaced.
- If your data is compromised maybe it on server or computer or on any network submit soft copy of original data and compromised data.

Conclusion

As someone rightly said "bytes are replacing bullets in the crime world". The growth of cyber crime in India, curb its scope and complexity is the pertinent need today. Cyber space offers a plethora of opportunities for cyber criminals either to cause harm o innocent people, or o make a fast buck at the expense of unsuspecting citizens. India's profile and wealth have risen enormously in the world due to the constructive use of information technology. At the same time India ranks 5'th in the world for cyber crime.Accordsing to a report last year by the U S based internet crime complaint centre, a partnership between the federal Bureau of investigation and the national white collar crime center.Even under the I T Act, investigation India are not easy. This is mainly due to the lack what is called "cyber forensics". We know that forensic evidence is important in normal criminal investigation. But the collection and the presentation of electronic evidence to prove cyber crimes have posed a challenge to investigation and prosecution agencies and the judiciary.

To sum up, India needs a good combination of laws and technology, in harmony with the laws of other countries and keeping in mind common security standards in the era of e- governance and e-commerce, a lack of common security standards can create havoc for global trade as well as military matters.

References

- 18 USC &1001 Statements or entries generally (sometimes cited on federal websites as a statute that would be violated by a hack)
- 18 USC & 1029. Fraud and Related Activity in connection With Access Devices
- Computer Fraud and Abuse Act of 1986 18 U. S. C 1030.
- 18 U. S. C. & 1362. Communication Lines, Stations, or Systems
- 18 U. S. C. & 2511 .Interpretation and Disclosure of Wire ,Oral , or Electronic Communications Prohibited
- 18 U. S. C. & 2701. Unlawful access to stored Communications
- 18 U. S. C. & 2702. Disclosure of Contents.