

CYBER CRIME – PREVENTION & DETECTION

- V.Shiva Kumar,
Asst.Director
A.P.Police Academy

1.0 CYBER CRIME

1.1 Cyber Crime is an evil having its origin in the growing dependence on computers in modern life.

A simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”. Defining cyber crimes, as “acts that are punishable by the information Technology Act” would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as e-mail spoofing, cyber defamation etc.,

1.2 TYPES OF CYBER CRIME

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

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

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computer. Some examples are;

1.2.1 Financial Claims: This would include cheating, credit card frauds, money laundering etc.

Cyber Pornography: This would include pornographic websites; pornographic magazines produced using computer and the Internet (to download and transmit pornographic pictures, photos, writings etc.)

Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, bulletin boards or simply by using e-mail communications.

Online gambling: There are millions of websites, all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property Crimes: These include 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: Counterfeit currency notes, postage and revenue stamps, mark sheets etc., can be forged using sophisticated 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.

Cyber Stalking: Cyber stalking involves following a person's movements across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim.

Let us examine some of the acts wherein the computer or computer Network is the target for an unlawful act. It may be noted that in these activities the computer may also be a tool. This kind of activity is usually out of the purview of conventional criminal law. Some examples are:

1.2.2 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 information contained in electronic form: This includes information stored in computer hard disks, removable storage media etc.

E-Mail bombing: Email bombing refers to sending a large amount of e-mails to the victim resulting in the victims' e-mail account or mail servers.

Data diddling: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

Salami attacks: Those attacks are used for the commission 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 involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

Virus/worm: 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. Worms, unlike viruses don not need the host to attach themselves to.

Logic bombs: These are dependent programs. This implies that these 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.

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 Time Theft: This connotes the usage by unauthorized persons of the Internet hours paid for by another person.

Physically damaging a computer system: This crime is committed by physically damaging a computer or its peripherals.

2.0 PREVENTION

2.1 PREVENTIVE STEPS FOR INDIVIDUALS

2.1.1. CHILDREN:

Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to-face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

2.1.2 PARENTS:

Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for use of limpets (for example blocking usage after a particular time) and allowing parents to see which site item children have visited. Use this software to keep track of the type of activities of children.

2.1.3. GENERAL INFORMATION:

Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these.

- Try not to panic.
- If you feel any immediate physical danger contact your local police.
- Avoid getting into huge arguments online during chat and discussions with other users.
- Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.
- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as others.

- Do not share personal information in public space online; do not give it to strangers.
- Be extremely cautious about meeting online introduced person. If you choose to meet, do so in a public place along with a friend.
- If a situation online becomes hostile, log off and if a situation places you in fear, contact local police.
- Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

2.2 PREVENTIVE STEPS FOR ORGANISATIONS AND GOVERNMENT

2.2.1 PHYSICAL SECURITY: Physical security is most sensitive component, as prevention from cyber crime Computer network should be protected from the access of unauthorized persons.

2.2.2 ACCESS CONTROL: Access Control system is generally implemented using firewalls, which provide a centralized point from which to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

2.2.3 PASSWORD: Proof of identity is an essential component to identify intruder. The use of passwords in the most common security for network system including servers, routers and firewalls. Mostly all the systems are programmed to ask for username and password for access to computer system. This provides the verification of user. Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge.

2.2.4 FINDING THE HOLES IN NETWORK: System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

2.2.5 USING NETWORK SCANNING PROGRAMS: There is a security administration's tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities include bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.

2.2.6 USING INTRUSION ALERT PROGRAMS: As it is important to identify and close existing security holes, you also need to put some watchdogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behaviour on network is caught immediately.

2.2.7 USING ENCRYPTION: - Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to any one but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

3.0 DETECTION: Cyber crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking, cyber defamation, cyber pornography can be detected and investigated through following steps:

After receiving such type of mail

- (1) Give command to computer to show full header of mail.
- (2) In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system from which the mail had come.
- (3) To know about Internet Service Provider from IP number take the service of search engine like nic.com, macffvisualroute. Com, apnic.com, arin.com.
- (4) After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.
- (5) After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.
- (6) ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.

After Knowing the address and phone number criminal can be apprehended by using conventional police methods.

4.0 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 .The various offences which are provided under this chapter are shown in the following table: -

| 4.1 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 |

NOTE: Sec.78 of I.T.Act empowers Deputy Supdt. Of Police to investigate cases falling under this Act.

4.2 Computer Related Crimes Covered under IPC and Special Laws

| Offence | Section |
|---------------------------------------|----------------|
| 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 |
| Online sale of Drugs | NDPS Act |
| Online sale of Arms | Arms Act |

5.0 ELEMENTARY PROBLEMS ASSOCIATED WITH CYBER-CRIMES:

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law any where in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under S.16 of Cr.P.C. and S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.
2. Loss of evidence is a very common & expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.
3. Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.
4. A law regulating the cyber-space, which India has done.
5. Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their

jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

6. Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and by-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalisation. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation.