Chapter 6
Introduction to Cyber Crime & Cyber Law

Cyber crime encompasses any criminal act dealing with computers and networks. Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

6.1 CYBER LAW

Cyber law Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes. We can categorize Cyber crimes in two ways:

The Computer as a Target:-Using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon:-Using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

6.2 TECHNICAL ASPECTS OF CYBER CRIME

(i) Unauthorized access & Hacking

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or

computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

(ii) Virus and Worm attack

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.

(iii) E-mail related crimes

Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter. Sending malicious codes through email. E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to particular address.

(iv) Exploit

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerized). Such behaviour frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

Denial of Service attacks

Flooding a computer resource with more requests than it can handle. This causes

the resource to crash thereby denying access of service to authorized users. For e.g.

attempts to "flood" a network, thereby preventing legitimate network traffic
attempts to disrupt connections between two machines, thereby preventing access to a service
attempts to prevent a particular individual from accessing a service
attempts to disrupt service to a specific system or person.

Types of DoS

There are three basic types of attack:

1. Consumption of limited resources like NW bandwidth, RAM, CPU time. Even power, cool air, or water can affect.
2. Destruction or Alteration of Configuration Information
3. Physical Destruction or Alteration of Network Components

Distributed DoS

A distributed denial of service (DoS) attack is accomplished by using the Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into zombies and used to attack another system or website.

(v) Pornography

The Pornography is describing or showing sexual acts in order to cause sexual excitement through books, films, etc. This would include pornographic websites, pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc. Pornography delivered over mobile phones is now a burgeoning business, “driven by the increase in sophisticated services that deliver video clips and streaming video, in addition to text and images.”

(vi) Cyber Terrorism

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyber terrorism is an attractive option for modern terrorists for several reasons given below.

1. It is cheaper than traditional terrorist methods.
2. Cyber terrorism is more anonymous than traditional terrorist methods.
3. The variety and number of targets are enormous.
4. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.

5. Cyber terrorism has the potential to affect directly a larger number of people.

(vii) Banking/Credit card related crimes

In the corporate world, Internet hackers are continuously looking for opportunities to compromise company's security in order to gain access to confidential banking and financial information. Use of stolen card information or fake credit/debit cards are common.

(viii) E-commerce/ Investment Frauds

Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

(ix) Defamation

Defamation can be understood as the intentional infringement of another person's right to his good name. Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone.

(x) Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

(xi) Breach of Privacy and Confidentiality

Privacy

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

Confidentiality

It means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for

business and leakage of such information to other persons may cause damage to business or person, such information should be protected. Generally for protecting secrecy of such information, parties while sharing information forms an agreement about procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

6.3 COMPUTER VIRUSES

Computer viruses are computer programs that, when opened, put copies of themselves into other computers' hard drives without the users' consent. Creating a computer virus and disseminating it is a cyber crime. The virus may steal disk space, access personal information, ruin data on the computer or send information out to the other computer user's personal contacts. The most common way for a virus to infect a computer is by way of an email attachment. An example would be if you received an email with an attachment. You open this attachment, and the virus immediately spreads through your computer system. In some cases, if the virus is opened by a computer on a system network, such as your place of employment, the virus can immediately be spread throughout the network without needing to be sent via email. There are numerous reasons that a person would create a virus to send out to another computer or computers. It may be to steal information or money, or to demonstrate the flaws that the other computer system has.

6.4 SOCIAL ENGINEERING

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with. When to trust that a website is or isn’t legitimate, when to trust that the person on

the phone is or isn't legitimate; when providing your information is or isn't a good idea.

6.5 PHISHING

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. Typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details. Phishing is popular with cyber criminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email than trying to break through a computer's defences. Although some phishing emails are poorly written and clearly fake, sophisticated cybercriminals employ the techniques of professional marketers to identify the most effective types of messages. To make phishing messages look like they are genuinely from a well-known company, they include logos and other identifying information taken directly from that company's website. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization. The use of subdomains and misspelled URLs (typo squatting) are common tricks, as is homograph spoofing. URLs created using different logical characters to read exactly like a trusted domain.

6.6 SOFTWARE PIRACY

Software piracy is the unauthorized copying, reproduction, use, or manufacture of software products. On average, for every authorized copy of computer software in use, at least one unauthorized or "pirated" copy is made. Software piracy harms everyone in the software community including you, the end user. Piracy results in higher prices for duly licensed users, reduced levels of support, and delays in the funding and development of new products, causing the overall selection and quality of software to suffer. Piracy harms all software publishers, regardless of their size. Software publishers spend years developing software for the public to use.

Software piracy also harms the local and national economies. Fewer legitimate software sales result in lost tax revenue and decreased employment. Software piracy greatly hinders the development of local software communities. If software publishers cannot sell their products in the legitimate market, they have no

incentive to continue developing programs. Many software publishers won't enter markets where the piracy rates are too high, because they will not be able to recover their development costs.

Types of Software Piracy

It seems that illegal software is available anywhere, to anyone, at any time. The following are some of the methods by which illegal copies of software circulate among computer users.

SOFTLIFTING

The most common type of piracy, softlifting, (also called softloading), means sharing a program with someone who is not authorized by the license agreement to use it. A common form of softlifting involves purchasing a single licensed copy of software and then loading the software onto several computers, in violation of licensing terms. On college campuses, it is rare to find a software program that has *not* been softloaded. People regularly lend programs to their roommates and friends, either not realizing it's wrong, or not thinking that it's a big deal. Softlifting is common in both businesses and homes.

HARD DISK LOADING

Often committed by hardware dealers, this form of piracy involves loading an unauthorized copy of software onto a computer being sold to the end user. This makes the deal more attractive to the buyer, at virtually no cost to the dealer. The dealer usually does not provide the buyer with manuals or the original CDs of the software.

RENTING

Renting involves someone renting out a copy of software for temporary use, without the permission of the copyright holder. The practice, similar to that of renting a video from Blockbuster, violates the license agreement of software.

OEM UNBUNDLING

Often just called "unbundling," this form of piracy means selling stand-alone software originally meant to be included with a specific accompanying product. An example of this form of piracy is someone providing drivers to a specific printer without authorization.

COUNTERFEITING

Counterfeiting means producing fake copies of software, making it look authentic. This involves providing the box, CDs, and manuals, all designed to look as much like the original product as possible. Microsoft products are the ones most commonly counterfeited, because of their widespread use. Most commonly, a

copy of a CD is made with a CD-burner, and a photocopy of the manual is made. Counterfeit software is sold on street corners, and sometimes unknowingly sold even in retail stores. Counterfeit software is sold at prices far below the actual retail price.

ONLINE PIRACY

The fastest-growing form of piracy is Internet piracy. With the growing number of users online, and with the rapidly increasing connection speeds, the exchange of software on the Internet has attracted an extensive following.

6.7 INTELLECTUAL PROPERTY

Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs and symbols, names and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

TYPES OF INTELLECTUAL PROPERTY

COPYRIGHT

Copyright is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture and films, to computer programs, databases, advertisements, maps and technical drawings.

PATENTS

A patent is an exclusive right granted for an invention. Generally speaking, a patent provides the patent owner with the right to decide how - or whether - the invention can be used by others. In exchange for this right, the patent owner makes technical information about the invention publicly available in the published patent document.

TRADEMARKS

A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises. Trademarks date back to ancient times when craftsmen used to put their signature or "mark" on their products.

INDUSTRIAL DESIGNS

An industrial design constitutes the ornamental or aesthetic aspect of an article. A

design may consist of three-dimensional features, such as the shape or surface of an article, or of two-dimensional features, such as patterns, lines or color.

GEOGRAPHICAL INDICATIONS

Geographical indications and appellations of origin are signs used on goods that have a specific geographical origin and possess qualities, a reputation or characteristics that are essentially attributable to that place of origin. Most commonly, a geographical indication includes the name of the place of origin of the goods.

6.8 MAIL BOMBS

A mail bomb is the sending of a massive amount of e-mail to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. Mail bombs not only inconvenience the intended target but they are also likely to inconvenience everybody using the server. Senders of mail bombs should be wary of exposing themselves to reciprocal mail bombs or to legal actions.

Important Points:

- Cyber crime encompasses any criminal act dealing with computers and networks
- Cyber Crime that are addressed by the Information Technology Act, 2000.
- Cyber crimes is of two types.(i) The Computer as a Target (ii) The computer as a weapon
- DDOS stands for Distributed Denial of Service.
- Confidentiality means non disclosure of information to unauthorized or unwanted persons.
- Virus is a computer program file capable of attaching to disks or other files and replicating itself repeatedly.
- Social engineering is the art of manipulating people so they give up confidential information
- Phishing is a form of fraud in which the attacker tries to learn confidential information
- Software piracy is the unauthorized copying, reproduction, use, or manufacture of software products.
- Apatent is an exclusive right granted for an invention.
- A mail bomb is the sending of a massive amount of e-mail to a specific person or system.

Practice Questions

Objective type questions:

Q1. Firstly cyber crime Information Technology Act associated with which year

a. 1999
b. 2000
c. 2001
d. 1998

Q2. What are the method of software piracy

a. Softlifting
b. Hard Disk Loading
c. Counterfeiting
d. All of these

Q3.DoS stands for

a. Distributed Denial of Service
b. Denial of Service
c. Denial Denial of Service
d. None

Q4.Computer Virus infects

a. Human Being
b. Animals
c. Computer
d.None of these

Very short answer type questions:

Q1. What is the Full form of DDoS?
Q2. Define copyright.
Q3. Define Softlifting**.**
Q4. Define Identity Theft.
Q5. Define Exploit**.**

Short answer type questions:

Q1. What is Cyber Crime?
Q2. Define Virus.
Q3. Name some Antivirus Software**.**
Q4. What is Intellectual Property?
Q5. What is patent?
Q6. What is online piracy?

Q7. What is Cyber Terrorism?
Q8 Explain Denial of Service attack.

Essay type questions:
Q1. Explain Phishing in details.
Q2.Explain the different types of Software Piracy.
Q3. Explain the different types of Intellectual property.

Answers key for objective questions

Q1: b
Q2: d
Q3: b
Q4: c