ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

Master of Science (Cyber Security)

Cyber law and Regulation of Cyberspace

(CSP-19)

BLOCK 2

Introduction to Python

UNIT-6
INTRODUCTION TO COMPUTER WRONGS

UNIT-7
CONVENTIONAL CRIMES THROUGH COMPUTER

UNIT-8
CRIMES AND TORTS

UNIT-9
CRIMES RELATING TO DATA ALTERATION/DESTRUCTION

EXPERT COMMITTEE

Dr. Sarojananda Mishra Professor & Head, Dept. of CSE, IGIT, Sarang	**(Chairman)**
Dr. Manas Ranjan Patra Professor & Head, Dept. of CSE Berhampur University, Bhanja Vihar	**(Member)**
Dr. P K Behera Reader, Dept. of CSE, Utkal University, Vani Vihar, Bhubaneswar	**(Member)**
Sri Malaya Kumar Das Scientist-E, NIC Bhubaneswar, Odisha	**(Member)**
Sh. Pabitrananda Patnaik Scientist-E, NIC, Bhubaneswar, Odiaha	**(Member)**
Dr. Manas Ranjan Senapati Associate Professor, Dept. of Information technology, VSSUT, Burla	**(Member)**
Sh. Girija Prasad Nanda Lead, ETA (Education, Training and Assessment), Infosys, Bhubaneswar	**(Member)**
Sri ChandrakantMallick Consultant (Academic) OSOU, Sambalpur, Odisha	**(Convener)**

M.Sc. in Cyber Security (MSCS)

Course Writer

Mr. Aseem Kumar Patel
Academic Consultant
Odisha State Open University, Sambalpur

Material Production

Dr. Manas Ranjan Pujari
Registrar
Odisha State Open University, Sambalpur

UNIT 6 INTRODUCTION TO COMPUTER WRONGS

Structure

6.1 INTRODUCTION

In this unit which is the first unit of this block, attempt has been made to give an overview of the computer wrongs. In the subsequent units we shall discuss various classes of computer wrongs.

With new mediums of communication, business and societal activities, growth of newer and varied kinds of crime is inevitable. Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The Internet is at once several shopping malls, libraries, universities, news paper, television, movie theatre, post office, courier service and an extension of government and business. It is like life in the real world being extended and carried on in another medium that cuts across boundaries, space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. The Internet, with all the benefits of anonymity, reliability, and convenience has become an appropriate breeding place for persons interested in making use of the Net for illegal purposes, either monetary or otherwise.

6.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the concepts of computer wrong and how the civil wrongs can be distinguished from the computer crimes, how the computer crimes are classified;
- distinguish between the concept of technology based and technology neutral laws;
- examine the issues involved in the regulation of cyberspace; and
- discuss how the matter has been dealt by the I.T. Act, 2000.

6.3 COMPUTER WRONGS

Computer wrongs includes both civil wrongs and crimes. 'Cyber crimes' is used in a generic sense which tends to cover all kinds of civil and criminal wrongs related to a computer. However, the phrase 'cyber crimes' has two limitations to it: (a) 'cyber' generally tends to convey the feeling of 'internet' or being 'online' and hence, does not cover other computer related activities; (b) 'crimes' restricts the application of the phrase to criminal wrongs. It would not include civil wrongs. Thus, it would be preferable to understand the concept of any wrong related to computer as being a 'computer wrong'. It would include any tort or civil wrong done which relates to a computer as also any criminal activity relatable to a computer. One must also keep in mind that it is the statute on a particular subject which informs us as to: (a) whether a particular act is a wrong; and, (b) if it is, whether such wrong is a civil wrong or a crime. The Information Technology Act, as would be seen in the subsequent units, divides various computer-related wrongs into computer torts and computer crimes. Computer torts lead to penalty and compensation whereas computer crimes lead to imprisonment, fine and confiscation.

6.4 CLASSIFICATION OF COMPUTER CRIMES

Technology-aided crimes can essentially be classified under two headings:

A) Where computer is used a *tool* to commit the crime: The computer is a tool for an unlawful act where the offence reflects a modification of a conventional crime by making use of information technology and modern communication tools.

B) Where the computer is the *target* for the crime: There are certain crimes where the computer itself is the target, that is, to say such crimes which have evolved due to the advancement in information technology itself.

There might be instances where the computer is a tool as well as the target of a crime. This kind of activity involves sophisticated crimes usually out of the purview of conventional criminal law. There is a third category as well, where computers are considered as *incidental* to a crime. The use of a computer is not necessary but is used to make the offender more efficient in the commission of the crime. This includes use of computers in bookmaking or drug-dealing.

6.5 COMMISSION OF MULTIPLE COMPUTER WRONGS

Another concern in computer crimes is the possibility of and ease with which an offender can commit multiple crimes at one goes. It is very possible and in fact, quite likely that an offender in the process of committing one computer crime commits other crimes as well. We can take a few instances to illustrate the point:

A) In case of data theft, one has to hack (unauthorized access) the computer or any other electronic storage medium and only then can be commit theft. Thus data theft includes hacking and theft.

B) To initiate a Distributed Denial-of-service, installation of virus, and Trojan horses on the 'slave'/compromised systems would be needed. The date of 'target' computer may also be altered or destroyed in the process. Thus, DDoS includes hacking, introduction of virus and data alteration.

C) Web defacing can be achieved by first hacking into the computer system.

The Indian statutory regulation, specifically Section 66 of the Indian Information Technology Act, 2000, in the area of computer crimes is quite comprehensive and concise. It is noticeable that most of the computer crimes culminate into section 66. Subsequent units on specific computer crimes would make the point clear.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are computer wrongs? How they are classified into civil wrongs and crimes?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6.6 CHALLENGES TO LAWS

India is today re-discovering itself – technologically. Being a developing country, it realises that the Internet and the use of computers are powerful tools for its economic development. Economic development presupposes existence of an appropriate regulatory regime. The biggest challenge to the law is to keep pace with technology.

6.6.1 Technology-neutral and Technology-based Laws

So far as law with respect to computer crimes is concerned, we have to have in place two sets of well-developed law: (1) technology-neutral criminal law; (2) technology-based laws. While talking about crimes relating to the Internet, most traditional crimes like fraud, defamation when committed using the Internet, would be governed by the existing technology neutral criminal laws. These are crimes with all elements of offline crimes, the only difference being that the Internet was used as aid in their commission. The other type of crime, and more disturbing requiring legal innovations, is the one directed at computers, networks, data etc. They include unauthorized disruption of computers and networks.

One of the challenges of making technology-based laws is that there is a chance of such laws being soon outdated. Again, it is against equity and fairness if offline conduct is governed differently from online conduct. This gives rise to the possibility of crime shifting from one medium to the other if there is an inconsistency in laws. Consistency between the two sets of law is, therefore, desirable. Laws must also cater to the need of prevention and investigation of crimes. For instance, with the advent of telephones, wire-tapping laws were introduced; similar laws to deal with unlawful conduct in the Internet would become necessary.

Clearly, with the development of new technology and with the realisation that such technology affects human life and relations and the peace, order and proprietary rights in society, laws must be framed to regulate conduct accordingly. Let’s take for instance theft of passwords. Passwords are a combination of alphabets and numbers and are central to the operation of computers. These are nothing but keys to gain entry into computer systems. Stealing a password or unauthorized access using someone else’s password must be recognised as merely the first step to committing a crime. Similarly, networks need to be recognised as highways for movement of information and communication and not for cranks to dig holes or put up impediments. One can enter into a private computer network only when one is authorized to enter much the same way as to enter into a private physical space. Web pages as private property can be considered as displays in shops. One can watch but cannot break the glass of the shop. Similarly, one can browse, but not tamper with or destroy.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is technology based law and technology neutral law?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6.6.2 Regulation Versus Freedom on the Internet

Talking of laws to control criminal behaviour on the Net brings one to the debate of regulation versus freedom on the Net. There are some who argue that the Net should not be regulated by governments.[1] They argue that, the Net grew because of its free environment, inviting people to contribute. Freedom and space for adventure, a new and different and an almost unrestricted and seemingly anonymous travelling experience has made the Net such an exciting media. Self governance is what they advocate for the Net. But this has several problems like, some groups taking law into their own hands. As Laurence Lessig, in *The Spam Wars*[2] says, "Vigilantes and network service providers (unaccountable groups) deciding fundamental policy questions about how the network will work – each group from its own perspective." This led to the argument that cyberspace transactions are no different from "real space" transnational transactions[3] that require government regulations in the ordinary way. The debate in the world between regulation and freedom on the Net has now more or less been settled in favour of the need for regulation. More and more governments have begun taking steps to regulate the Net.

6.6.3 Internet Crime Different from other Technology Crimes

It is important to note the difference between crime on the Internet and a crime with another modern technology. While crimes are rarely directed against

a telephone as an instrument, computers often become the victims of attack. Nature of crime on the computer is challenging and requires new definitions and understanding and a restatement of accepted norms of criminal conduct and punishment because of several reasons. Computers, apart from being comparatively more expensive, are also the repository of immense amount of data. This data can sometime contain valuable scientific inputs, purely personal matter, study works, e-mails, and official work. Tampering with this data or stealing it is much more harmful than stealing the computer. This requires recognition of data as a special form of property, as a privacy right.

6.7 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act seeks to protect a common man from the ill effects of the advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and appointing regulatory authorities. Many electronic crimes have been bought within the definition of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891 too have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes.

In the following units, common computer crimes have been discussed. Wherever possible, not only the meaning and scope of the crime but also its coverage under the Indian Information Technology Act, 2000, the Indian Penal code and other minor criminal Acts have been discussed. The computer crimes can be classified into the following categories:

A) Conventional crimes through computer: cyber defamation, digital forgery, cyber pornography, cyber stalking/harassment, Internet fraud, financial crimes, online gambling, and sale of illegal articles.

B) Crimes committed on a computer network: hacking/unauthorized access, denial of service.

C) Crimes relating to data alteration/destruction: virus/worms/Trojan horses/ logic bomb, theft of Internet hours, data diddling, salami attacks, steganography

6.8 OFFENCES UNDER THE IT ACT

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences (including offences under other sections) can be better understood in the form of a table:

Section	Offence	Punishment
33(2)	Failure of any Certifying Authority to surrender a licence under Section 33(1) after such licence has been suspended or revoked [Section 25(1)].	Person in whose favour the licence is issued shall be punished with imprisonment which may extend upto six months or a fine which may extend upto Rs.10,000 or both.
65 (Tampering)	Knowingly or intentionally concealing, destroying or altering or intentionally or knowingly causing another to conceal, destroy, or alter any computer source code use for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Punishable with imprisonment upto three years, or with fine which may extend up to Rs. 2,00,000/-, or with both.
66 (Hacking)	Destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously be any means with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any person.	Punishable with imprisonment up to three years, or with fine which may extend up to Rs. 2,00,000/-, or with both.
67	Publishing or transmitting or causing to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, or read, see or hear the matter contained or embodies in it that is hacking as defined under Section 67(1)	First conviction: punishable with imprisonment of either description of a term which may extend to five years and with fine which may extend to Rs. 1,00,000/-. Second or subsequent conviction: imprisonment of either description of a term which may extend to ten years and with fine which may extend to Rs. 2,00,000/-.
68(2)	Failure to comply with the order of Controller under section 68(1) which empowers the Controller to direct, by order, a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rule or any regulations made thereunder.	Punishable with imprisonment for a term not exceeding three years or to a fine not exceeding Rs. 2,00,000/- or to both.
69(3)	Failure to assist an agency [referred in section 69(2)] which is required to intercept any information as required by an order of the Controller [under section 69(1)]	Punishable with imprisonment for a term which may extend to seven years.
70(3)	Securing access or attempting to secure access to a protected system [as declared by the	Punishable with imprisonment of either description for a term which

	appropriate Government vide a notification under section 70(1)] in contravention of the provisions of this section [that is such person is not authorized by the appropriate Government under section 70(2) to access the protected system].	may extend to ten years and shall also be liable to fine.
71	Making any misrepresentation to, or suppressing any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs. 1,00,000/-, or with both.
72	Securing access to any electronic record, book, register, correspondence, information, document or other material by any person in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder without the consent of the person concerned and thereafter, disclosing such electronic record, etc. to any other person.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one Rs. 1,00,000/- or with both.
73	Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that- (a) the Certifying Authority listed in the certificate has not issued it; or, (b) the subscriber listed in the certificate has not accepted it; or, (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
74	Knowingly creating, publishing or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.	Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible, to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, he shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other office of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. ‘Company’, for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. ‘Director’, in relation to a firm, would mean a partner in the firm.

Section 7[4] prohibits immunity against any punishment under any other law to which a person might be liable to in spite of any penalty imposed or confiscation made under the IT Act.

6.9 INVESTIGATION UNDER THE IT ACT

The procedure for investigation for compute crimes is no different from the investigation for conventional crimes and Code of Criminal Procedure, subject to the provisions of the IT Act, would apply.

Investigation, for the purposes of the Code of Criminal Procedure, 1973, has been held by the Supreme Court [*State of Maharashtra* v. *Rajendra*, (1997) 3 Crimes 285] to consist generally of the following steps:

1) Proceeding to the spot
2) Ascertaining all the facts and circumstances of the case
3) Discovery and arrest of the suspected offender
4) Collection of evidence relating to the commission of the offence which may consist of,
    a) the examination of various persons (including, the accused) and the reduction of their statement into writing, if the officer thinks fit,
    b) the search of places and seizure of things considered necessary for the investigation and to be produced at the trial, and
5) Formation of the opinion as to whether on the materials collected, there is a case to place the accused before a Magistrate for trial and if so, taking the necessary steps for the same by filing a charge-sheet under section 173.

Section 78 of the IT Act places the powers of investigation to a police officer not below the rank of Deputy Superintendent of Police. This provision overrides anything contrary in the Code of Criminal Procedure.

Section 80 enumerates the powers of police officers to enter and search premises. Sub-section (1) of section 80 provides that any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Act. For the purposes of sub-section (1), the expression ‘public place’ has been explained to include any conveyance, any hotel, any shop or any other place intended for use by, or accessible by the public.

Where any person is arrested under sub-section (1), then sub-section (2) requires that such person should, without unnecessary delay, is taken or sent before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station. The provisions of the Code of Criminal Procedure are to apply in relation to any entry, search or arrest made under section 80, subject of course to the provisions of the section itself.

6.10 CONVENTION ON CYBERCRIME – COUNCIL OF EUROPE[5]

The Convention on Cyber Crimes is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. The possibility of computer networks and electronic information being used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, was the underlying concern during the preparation of the Convention. The Convention was deemed necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in the Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cyber crime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organization. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

References to the Convention would be made in subsequence units dealing with specific cyber/computer crimes alongside the Indian Information Technology Act.

6.11 SUMMARY

Computer wrongs include both civil wrongs and crimes. The Information Technology Act, 2000 covers both– civil wrongs and crimes. For the purposes of committing a crime, a computer can be used both as a tool as well as a target. Sometimes, it is used to make the offender more efficient in the commission of the crime. It is very possible and in fact, quite likely that an offender in the process of committing one computer crime commits other crimes as well. One of the challenges of making technology-based laws is that there is a chance of such laws being outdated soon. The debate in the world between regulation and freedom on the Net has now more or less been settled in favour of the need for regulation. Governments have begun taking steps to regulate the Net.

Chapter XI of the Information Technology Act enumerates the various acts which constitute an offence under the Act along with the punishment of either imprisonment or fine or both. The procedure for investigation for computer

crimes is no different than the investigation for conventional crimes and Code of Criminal Procedure, subject to the provisions of the IT Act, would apply.

The Convention on Cyber crime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

6.12 TERMINAL QUESTIONS

1) What are computer wrongs? Discuss the concepts of technology based and technology neutral wrongs.

2) Discuss the arguments in favour and against of the regulation of cyberspace. What are your views on this issue?

3) Discuss the challenges faced by the investigating agencies in investigating computer crime?

6.13 ANSWERS AND HINTS

1) Computer wrongs includes both civil wrongs and crimes. ‘Cyber crimes’ is used in a generic sense which tends to cover all kinds of civil and criminal wrongs related to a computer. However, the phrase ‘cyber crimes’ has two limitations to it: (a) ‘cyber’ generally tends to convey the feeling of ‘internet’ or being ‘online’ and hence, does not cover other computer related activities; (b) ‘crimes’ restricts the application of the phrase to criminal wrongs. It would not include civil wrongs. Thus, it would be preferable to understand the concept of any wrong related to computer as being a ‘computer wrong’. It would include any tort or civil wrong done which relates to a computer as also any criminal activity relatable to a computer. One must also keep in mind that it is the statute on a particular subject which informs us as to: (a) whether a particular act is a wrong; and, (b) if it is, whether such wrong is a civil wrong or a crime. The Information Technology Act, as would be seen in the subsequent units, divides various computer-related wrongs into computer torts and computer crimes. Computer torts lead to penalty and compensation whereas computer crimes lead to imprisonment, fine and confiscation.

2) Technology based laws are those in which computer is the means or the target of the crime such as hacking etc. While technology neutral laws are ordinary laws and it is immaterial whether computer is used or not such as defamation etc.

6.14 REFERENCES AND SUGGESTED READINGS

1. See, for example, David R. Johnson & David Post. “Law and Borders—

The Rise of Law in Cyberspace”. Stan L Rev 48 (1996): 1367,1372-75.

2. Lawrence Lessig. “The Spam Wars”. Opinion. 31 Dec.1998. 9 Feb. 05 <http://www.lessig.org/content/standard/0,1902,3006,00.html>.

3. Jack L. Goldsmith. “Against Cyber Anarchy”. U Chi L Rev 65 (1998): 1199-1250.

4. S. 77. Penalties or confiscation not to interfere with other punishments. No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

5. Budapest. 23.XI.2001. Council of Europe. 8 Feb.06 < http://conventions. coe.int/Treaty/en/Treaties/html/185.htm>.

UNIT 7 CONVENTIONAL CRIMES THROUGH COMPUTER

Structure

7.1 INTRODUCTION

In the previous unit we have tried to give the general introduction of the computer wrongs. In this unit we shall discuss the offences which are known as the technologically neutral offences. These offences do not depend on computer for their commission although their quantitative and qualitative impact changes when committed on the cyberspace.

Many of the wrongful acts enlisted as an offence under the Indian Penal Code, 1860 are capable of being committed with the use or aid of or through computers and technology. The technology acts only as a new medium to commit such

crimes. With the ease of use and anonymity available on the Internet, many of the crimes like defamation, forgery, pornography, etc. are being committed online.

While studying this unit you should keep the copy of the IPC for the quick references of the definitions of the offences discussed in this unit.

7.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the offences defined under Indian Penal Code which are capable of being committed on the internet;
- examine the new dimensions that have been added to these offences by the use of information and communication technology (ICT); and
- analyse whether the provisions of Indian Penal Code dealing with these offences are capable enough to address the challenges posed by the information and communication technology with regard to these offences.

7.3 CYBER DEFAMATION

Every individual has a private right to protect his reputation. Every individual has a right to its own personal space and he would not want others to interfere in that 'space'. However, a public right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India makes enforcement of our private right a challenge. A delicate balance has to be maintained. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages. Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking).

In the good old days, slander was more popular and possible. After the popularity of the printing press, one witnessed the increase in libel. With the advent of information technology and the Internet, libel has become much more common and of course, easier. In this context, arises cyber defamation. In simple words, it implies defamation by anything which can be read, seen or heard with the help of computers/technology. Since the Internet has been described as having some or all of the characteristics of a newspaper, a television station, a magazine, a telephone system, an electronic library and a publishing house, there are certain noticeable differences between online and offline attempt of defamation which makes the online defamation more vigorous and effective.

In *SMC Pneumatics Ltd.* v *Jogesh Kwatra*,[1] defamatory e-mails were allegedly sent to the top management of SMC Numatics by the defendant, who has since been restrained by the Delhi High Court from sending any form of communication to the plaintiff. The High Court granted an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene e-mails either to the plaintiffs or their subsidiaries. [*Avinash Bajaj* v *State (NCT) of Delhi*. Bail Appl. no. 2284 of 2004 decided on 21 Dec. 2004 [116 (2005) DLT 427].

7.3.1 Quantitative Impact of Cyber Defamation

Quantitatively, a comment defaming a person can be sent to a large number of persons through e-mail by a click of the mouse. Much easier would be to publish it on a discussion board known to be visited by thousands of persons every day. On the number game, it is still more convenient to make available the defamatory sentence to millions of people by merely publishing it on the website. The number of people a comment defaming a person might reach is gigantic and hence would effect the reputation of the defamed person much more than would an ordinary publication. Of course, there is a rider to it. In as much as there is a possibility of a large number of people reading the defamatory sentence on a website, unless such website is known, it might not even reach a single person at all. Thus, a defamatory sentence published on a newspaper website would have a bigger impact than being published on a website hardly known to the world at large.

7.3.2 Qualitative Impact of Cyber Defamation

Qualitatively, the impact of an online comment defaming a person would again depend upon the fact as to where it has been published. Putting a defaming message in specific a newsgroups (for example, a lawyer's group in case one wants to defame a lawyer) would necessarily have a more effective negative impact on the reputation of the person being defamed rather putting the same on a ladies' kitty party group.

7.3.3 Corporate Cyber Smear

Harmful and defamatory online message has been termed as *Corporate cyber smear*. It is a false and disparaging rumour about a company, its management or its stock that is posted on the Internet. This kind of criminal activity has been a concern especially in stock market and financial sectors where knowledge and information are the key factors for businessmen. Persons indulging in corporate cyber smear include disgruntled employees or insiders, ex-employees, envious ex-colleagues, impostors, competitors, creditors, and even those seeking a forum when they are denied employment or former shareholders.

False and defamatory statements made against Amazon Natural Treasures, Inc. led to a stock price decline from an April 1997, 52-week high of $3.56 per share to approximately 12 cents per share. The low stock price led to a de-listing from the OTCBB to the pink sheets. It transpired that the statements were made by the owner of Demonte & Associates, a New York public relations firm, who claimed that a collection agency was suing Amazon for about $7,000.

7.3.4 Indian Law

Cyber defamation is covered under section 499 of Indian Penal Code (IPC) read with section 4 of the IT Act. Section 499 of the IPC *inter alia* reads as under:

499. Defamation.Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

Explanation 1 — It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2 — It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3 — An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4 — No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

A bare perusal of the section above makes it clear that no specific mention has been made with regard to any electronic publication. Section 4 of the IT Act, however, gives legal recognition to electronic records. It reads as under:

4) **Legal recognition of electronic records.**

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

a) rendered or made available in an electronic form; and

b) accessible so as to be usable for a subsequent reference.

Keeping in mind the legal fiction being created by section 4 of the IT Act, if any defamatory information is posted on the Internet either through e-mails or chat rooms or chat boards, such posting would be covered under the section 499 requirement of 'publication' and would amount to cyber defamation. That is the legal position of cyber defamation in India.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What is defamation? Discuss its quantitative and qualitative impact when it is committed on the cyberspace.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7.4 DIGITAL FORGERY

Forgery is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. In common parlance, it is used more in terms of affixing somebody else's signature on a document. Digital forgery implies making use of digital technology to forge a document. Desktop publishing systems, colour laser and ink-jet printers, colour copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

7.4.1 Indian Law

Section 91 of the IT Act (read with the Second Schedule) amended the provisions of the IPC in relation to 'forgery' to include 'electronic records' as well. Section 29A has been inserted in the Indian Penal Code to provide for a definition of 'electronic record'. The words 'electronic record' will have the same meaning which is assigned to it in section 2(1)(t)[2] of the IT Act.

Section 464 of the IPC was amended by section 91 of the IT Act to include a false electronic record. Under section 464, a person is said to make a false electronic record:

1) Who dishonestly or fraudulently makes or transmits any electronic record or part of any electronic record, or, affixes any digital signature on any electronic record, or, makes any mark denoting the authenticity of the digital signature, with the intention of causing it to be believed that such electronic record or part of electronic record or digital signature was made, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, executed or affixed; or

2) Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

3) Who dishonestly or fraudulently causes any person to sign, execute or alter an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the electronic record or the nature of the alteration.

Explanation 3 to section 464 has also been inserted which, for the purpose of this section, provides for the expression 'affixing digital signature' to have the same meaning as assigned to it in section 2(1)(d)[3] of the IT Act.

Section 463 of the IPC, after amendment, defines forgery, in relation to electronic records, as making of any false electronic record or part thereof with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed. Section 466 (forgery of record of Court or of Public register, etc.), section 468 (forgery for purpose of cheating), section 469 (forger for purpose of harming reputation), section 470 (forged document or electronic record), section 471 (using as genuine a forged document), section 474 (having possession of document described in section 466 or 467, knowing it to be forged and intending to use it as genuine) and section 476 (counterfeiting device or mark used for authenticating documents other than those described in section 467, or possessing counterfeit marked material) have also been suitably amended to include 'electronic records'. It may, however, be noticed that section 467 which pertains to forgery of valuable security, will, etc., has not been amended for the reason that section 1(4) bars the applicability of IT Act to certain documents including will, trust, power-of-attorney, contract for sale or conveyance of immovable property, etc. Therefore, digital forgery and offences related to it are now covered under the IPC pursuant to the amendments made by the IT Act.

7.4.2 Convention on Cyber Crime – Council of Europe

The Convention on Cyber crime, Article 7 requires the member-States to make laws to establish as criminal offences, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is digital forgery? How the technology has made its detection sometimes very difficult?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7.5 CYBER PORNOGRAPHY

Pornography literally means, “Writings, pictures or films designed to be sexually exciting”. Developing, distributing and propagating the same over the Internet is termed as cyber pornography. This would include pornographic Web sites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, writings, etc. In recent times, there have been innumerable instances of promotion of pornography through the use of computers. Information technology has made it much easier to create and distribute pornographic materials through the Internet; such materials can be transmitted all over the world in a matter of seconds. The geographical restrictions, which hitherto prevented, to a certain extent, foreign publications to enter into local territories, have disappeared.

7.5.1 Increase in Cyber Pornography

Two primary reasons why cyber pornography has, in recent years, gathered much attention of both the offender and user, are: (a) Easy accessibility; (b) Anonymity.

Individuals can easily view thousands of pornographic images day and night within the privacy of the four walls of their homes. The Internet has decreased the hurdle of shame that comes with purchasing pornographic materials in a shop or the embarrassment of being caught with physical hard copies of porno

materials. The consumer of such publications is more comfortable in opening a website and viewing/watching. With availability of broadband connections and high downloading speeds, the demand, though privately, seems to have risen.

On the other hand, anonymity has encouraged the offender to come out with more explicit and real material with higher degrees of inducement. Anybody can upload information onto a website from anywhere with the entire world as its market/consumer. It is extremely difficult to pinpoint persons responsible for such activities. It is also important to note that in countries where certain degree of pornographic material is permitted to be published and distributed, offenders quite often publish their information online from such countries though knowing well that the online market extends well beyond the geographical boundaries.

7.5.2 Child Pornography

What has, however, been most disturbing is the increase in child pornography. Child pornography is different from other pornography, and consequently receives more stringent legal treatment. It is distinguished as an issue of child abuse — in its production and/or in the way it is used by pedophiles to desensitise their victims. The growth of the Internet has provided child pornographers with a distribution vehicle which is perceived to be relatively anonymous.

In February 2006, Mark S. Proctor was sentenced by U.S. District Court Judge to a total of 151 months' imprisonment after pleading guilty to possession and distribution of child pornography. Proctor's arrest was part of "Operation Clean-Sweep". an undercover operation initiated by the Miami Electronic Crimes Task Force. A Secret Service agent met Proctor in a 'Preteen' Internet chat room on 'Yahoo'. Proctor, who believed the undercover agent was the parent of a pre-teen girl, engaged the agent in sexually explicit chats about minors and sent the undercover agent images of child pornography. A search warrant of his residence and seizure of his computers revealed additional images of child pornography. Proctor pled guilty.[4]

7.5.3 Indian Law

The issue of cyber pornography has been dealt with in section 67 of the IT Act where publishing of information which is obscene in electronic form has been made an offence. Section 67 reads as under:

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

The section provides that any material which is published, or transmitted or caused to be published in the electronic form shall be an offence in the following situations:

a) The material so published or transmitted is lascivious;

b) The material appeals to the prurient interest;

c) If the effect of the material is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

In case one is found committing an offence under section 67, he shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. It is worth noticing that the obscenity test in section 67 is the same as that in section 292 of the IPC which deals with sale of obscene books, etc.

Other enactments having a bearing on the issue of cyber pornography are Indecent Representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950. Persons dealing in cyber pornography that is accessible to persons under the age of twenty years are also liable to be prosecuted under section 293 of the IPC.

7.5.4 Cyber Crime Convention

The Convention on Cyber Crime has, under Article 9, dealt with child pornography and corresponds to an international trend that seeks to ban child pornography. It defines 'child pornography' as inclusive of such pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

c) realistic images representing a minor engaged in sexually explicit conduct.

The article requires the member countries to adopt laws which establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

1) Producing child pornography for the purpose of its distribution through a computer system;

2) Offering or making available child pornography through a computer system;

3) Distributing or transmitting child pornography through a computer system;

4) Procuring child pornography through a computer system for oneself or for another person;

5) Possessing child pornography in a computer system or on a computer-data storage medium.

It is worth noticing that 'online pornography' by itself has not been brought within the four corners of the Convention. It is only the child pornography which has been condemned in the Convention.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

How the term pornography has been defined in Indian law?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7.6 CYBER STALKING / HARASSMENT

To stalk is to follow quietly and secretly. Cyber stalking is an electronic extension of stalking. The electronic medium is used to pursue, harass or contact another in an unsolicited fashion. The term is used to refer to the use of the Internet, e-mail, or other electronic communication devices to stalk another person. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

7.6.1 Preferred Mode of Harassment

Five reasons why cyber stalking today is a preferred mode of harassment are:

a) Ease of communication

b) Access to personal information: With a bit hacking expertise, one might easily be able to access personal information of a person which would help in further harassment.

c) Anonymity: The cyber stalker can easily use an identity mask thereby safeguarding his real identity.

d) Geographical location: In online cyber stalking the cyber stalker can be geographically located anywhere.

e) Ease of indirect harassment: The cyber stalker does not directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

In the first successful prosecution under California's new cyber stalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999.[5]

Similar problem arose in *State of Tamil Nadu* v *Suhar Katti*,[6] where a family friend who wanted to marry a widow, on her refusal, started posting online messages in her name as if she is soliciting. These messages resulted in annoying phone calls. On a police complaint made in February 2004, the accused was traced, put to trial and was ultimately found guilty of offences under sections 469, 509 of the Indian Penal Code and section 67 of the IT Act.

7.6.2 Indian Law

Chapter 22 of the Indian Penal Code deals with criminal intimidation, insult and annoyance. Section 503 provides that whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, such person commits criminal intimidation. Cyber stalking in effect is committing criminal intimidation with the help of computers. The offender might be causing alarm by sending messages via the Internet to the victim threatening injury to him, his property or reputation. The computer is merely used as a tool for committing the offence or rather improving upon the act of committing the offence and to be able to more effectively threaten his victim. The anonymity over the Internet gives the offender a suitable shield to commit the offence without being easily detected. However, the end-result being the same, cyber stalking is merely criminal intimidation under section 503 of the IPC.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

Discusses the new dimensions added by the cyberspace to the concept of stalking and harassment.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7.7 ONLINE GAMBLING

Gambling is in many countries illegal. Computer is a medium for the purposes of online gambling. The act of gambling is categorised as an offence in some countries and has a legal sanctity in others. The main concern with online gambling is that most virtual casinos are based offshore making them difficult to regulate. This means that people offer gambling services on the Internet from countries where gambling is permitted where players, from such countries where gambling is illegal, play and bet. It is in this situation that the Internet helps the gamblers to evade the law. Anyone with access to a personal computer and an Internet connection can purchase lottery tickets or visit gambling sites anywhere in the world. The world of online gambling, due to its anonymity, unfortunately has many other hazards like danger of illegal use of credit card or illegal access to bank account.

In an interesting case, the managers and owners of six Internet sports betting companies that operated offshore and allowed bettors in the United States to gamble on football, basketball and other sports were charged with illegally using the wires and telephone to transmit bets. The 14 individuals accused of running the illegal betting operations were set up offshore in Caribbean or Central American locations where sports betting is legal. Though the owners contended that they are beyond the law because they are located in countries where gambling is legal, the prosecution was of the view that so long as money is wired or telephone calls are made from the United States, it doesn't matter where the company is set up.[7]

7.7.1 Indian Law

The Public Gambling Act, 1867 prohibits gambling. Section 3 of the Act imposes a fine on the person opening a common gaming-house for others. However, it is also worth noting that the Act presumes a physical place where gambling will take place. The interpretation clause of the Act defined 'common gaming-house' as any house, walled enclosure, room or place in which card, dice, tables or other instruments of gaming are kept or used for the profit or gain of the person owning, occupying, using or keeping such place.

Relevant provisions of the IPC dealing with cheating, criminal misappropriation or criminal breach of trust could be applied in cases of online gambling. However, there is no direct law on this point.

7.8 ONLINE SALE OF ILLEGAL ARTICLES

There are certain articles like drugs, guns, pirated software or music that might not be permitted to be sold under the law of a particular country. However, those who would want to sell such articles find Internet a safe zone to open up online shops. There are specific concerns with regard to increase in online sale of drugs. A simple Internet search will turn up dozens of Web sites that let anyone order drug-of-choice for home-delivery.

The sale of illegal articles on the Internet is also one of those computer crimes where the computer is merely a tool to commit the crime. The traditional crime is already not permissible under various statutes. However, it is being committed by using computer and through the Internet where one gets a better and bigger market along with the benefit of anonymity.

In December 2004, the CEO of Bazee.com was arrested in connection with sale of a CD with objectionable material on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail by the Delhi High Court.[8] This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider.

7.8.1 Indian Law

Under the Indian law, many articles are prohibited for sale. For instance, with regard to sale of arms and ammunition, section 7 of the Arms Act, 1959 specifically prohibits sale of any prohibited arms or prohibited ammunition by any person. Section 9B of the Indian Explosive Act, 1884 makes sale of any explosive an offence if it is done in contravention of the rules. Likewise, section 8 of the Narcotic Drugs and Psychotropic Substances Act, 1985 prohibits sale or purchase of any narcotic drug or psychotropic substance. As regards drugs, sections 18, 27, 27A, 28B and 33I of the Drugs and Cosmetics Act, 1940 prohibit sale of certain drugs or cosmetics. Similarly the sale of banned animal products would be covered under the Wild Life (Protection) Act, 1972. Dealing illegally in antiques is covered by the Antiques and Art Treasures Act, 1972.

Therefore, as far as the issue of legality of sale of any article on the Internet is concerned, it would be governed by a specific statute. Merely because it is being sold through the Internet would not change the character of sale and would still be within the ambit of the prohibitory provision of the enactment.

7.9 SUMMARY

This unit discusses the crimes enumerated in the IPC which can be committed with the aid of the Information Communication Technology (ICT) with more ease and some times with more impunity.

Defamation law – aims at protecting the reputation of the injured person and giving him the right to sue if his reputation is damaged. If a defamatory statement is published on the website, it may have more quantitive and qualitative impact as compared to the publication in a newspaper etc. for instance e-mailing a defamatory statement to a large number of persons or posting it on a discussion board or newsgroups of a profession e.g. lawyers etc. may prove to be very injurious.

Similarly, corporate cyber smearing i.e. injurious or defamatory statement about a company or its officials may be more harmful than the other medium of publication.

Forgery – forgery is a creation of a document which the person knows to be not genuine and yet he projects it to be genuine. With the use of the desk top publishing system, laser and ink-jet printers, colour copier, image scanner etc forged documents such as birth certificates, passports etc can be made and it is more difficult to test the genuineness of such documents.

Pornography – means writings, pictures and films which are sexually exciting. Pornographic material on the Internet can be accessed by any one any where in the world in privacy and without feeling shame irrespective of whether the law of such country permits it or not.

The most disturbing aspect is the increase in the child pornography.

Cyber stalking/harassment – stalking means to follow quietly and secretly. It refers to the use of Internet, e-mail and other communication devices harass or intimidate etc. with a bit expertise in hacking, a person may have access to the personal information stored in the computer and use in stalking and while doing it, he may conceal his identity also.

Gambling – online gambling websites can be operated from the country where it is not illegal. In such types of virtual casinos, it is not necessary to be present in the country from where the site is being operated. A person can be engaged in gambling while sitting in his home even if it is illegal in his country.

Online illegal sale of articles – such as drugs, arms, pirated copies of software’s etc. Internet provides a bigger market and privacy to the seller. Through online shopping, these goods can be sold even if their sale is prohibited by law.

7.10 TERMINAL QUESTIONS

1) Discuss how the information and communication technology have added new dimensions to many of the technology neutral offences as defined in the Indian Penal Code of 1860.

7.11 ANSWERS AND HINTS

1) Every individual has a private right to protect his reputation. Every individual has a right to its own personal space and he would not want others to interfere in that 'space'. However, a public right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India makes enforcement of our private right a challenge. A delicate balance has to be maintained. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages. Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking).

   Quantitative impact of Cyber Defamation

   Quantitatively, a comment defaming a person can be sent to a large number of persons through e-mail by a click of the mouse. Much easier would be to publish it on a discussion board known to be visited by thousands of persons every day.

   Qualitative impact of Cyber Defamation

   Qualitatively, the impact of an online comment defaming a person would again depend upon the fact as to where it has been published. Putting a defaming message in specific a newsgroups (for example, a lawyer's group in case one wants to defame a lawyer) would necessarily have a more effective negative impact on the reputation of the person being defamed rather putting the same on a ladies' kitty party group.

2) Forgery is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. In common parlance, it is used more in terms of affixing somebody else's signature on a document. Digital forgery implies making use of digital technology to forge a document. Desktop publishing systems, colour laser and ink-jet printers, colour copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

3) Pornography literally means, "Writings, pictures or films designed to be sexually exciting". Developing, distributing and propagating the same over the Internet is termed as cyber pornography. This would include pornographic Web sites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, writings, etc. In recent times, there have been innumerable instances of promotion of pornography through the use of computers. Information technology has made it much easier to create and distribute pornographic materials through the Internet;

such materials can be transmitted all over the world in a matter of seconds. The geographical restrictions, which hitherto prevented, to a certain extent, foreign publications to enter into local territories, have disappeared.

4) To stalk is to follow quietly and secretly. Cyber stalking is an electronic extension of stalking. The electronic medium is used to pursue, harass or contact another in an unsolicited fashion. The term is used to refer to the use of the Internet, e-mail, or other electronic communication devices to stalk another person. .

Preferred mode of harassment

Five reasons why cyber stalking today is a preferred mode of harassment are:

a) Ease of communication

b) Access to personal information: With a bit hacking expertise, one might easily be able to access personal information of a person which would help in further harassment.

c) Anonymity: The cyber stalker can easily use an identity mask thereby safeguarding his real identity.

d) Geographical location: In online cyber stalking the cyber stalker can be geographically located anywhere.

e) Ease of indirect harassment: The cyber stalker does not directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

Internet knows no boundaries. Communication has begun faster and easier. It has become easy to conceal his identity and commit offences. Internet gives access to a large number of persons irrespective of geographical boundaries through e-mail, newsgroups, online shopping etc.

Study the offences discussed in the unit and see how ICT has provided the technology which can be used in the commission of these offences.

7.12 REFERENCES AND SUGGESTED READINGS

1. Sharon Walsh. Washington Post Staff Writer. “14 Charged in Internet Betting. The Washington Post”. <http://www.washingtonpost.com/wp-srv/national/longterm/intgambling/stories/charged.htm.>.

2. Judgment delivered by Ld. Additional Chief Metropolitan Magistrate. Egmore on 05.11.2004.

3. <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>.

4. 6 No. 6 Cyber Crime Law Reporter 6 <http://www.usdoj.gov/usao/fls/060210-03.html>.

5. S. 2(1)(t).- 'electronic record' means, data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

6. S. 2(1)(d).- 'affixing digital signature', with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

7. <http://www.legalservicesindia.com/articles/defcy.htm>.

8. Suit no. 1279 of 2001, Delhi High Court.

UNIT 8 CRIMES AND TORTS COMMITTED ON A COMPUTER NETWORK AND RELATING TO ELECTRONIC MAIL

Structure

8.1 INTRODUCTION

In the previous unit we have discussed that the information and communication technology has added new dimentions to traditional crimes. Computer and cyberspace has given rise to many of the wrongs which were hitherto unknown to the mankind. These crimes are of very complicated nature and highly sophisticated technology is applied in committing these crimes. This unit discusses some of them. In this unit we shall also discuss how these offences have been dealt with in the Indian law and Cyber Crime Convention of the Council of Europe.

It is recomended that you should read chapter IX and XI of the IT Act, 2000 which defines these offences. Sub-section 3 of the Unit 3 of the Block 1 may be referred to in this connection.

8.2 OBJECTIVES

After studying this unit, you should be able to:

- analyse the concept of hacking and what is Indian law on the issue?;
- discuss various forms of denyal of service and legal provisions dealing with the issue; and
- discuss how the unsolicited e-mail spanning and e-spoofing has caused problems to the user and service providers and is Indian law sufficient to deal with this menace?

8.3 HACKING/UNAUTHORIZED ACCESS

Trespassing is a word known to us. Simply put, it means entering upon or into a property owned by someone else without his or her permission. In the offline world, 'entering' would imply physical entry into the property. Trespassing has both civil and criminal consequences.

Trespassing has a digital counterpart which is referred to as hacking. Hacking means unauthorized access to a computer system. The computer serves as a tool to commit the crime as also necessarily is the target of such crimes. It is one of the most popular and fastest growing computer crimes and has been escalated with the aid of the Internet.

8.3.1 Hacker Ethics

Hacking has generally been understood as interacting with a computer in a playful and exploratory rather than goal-directed way. The word 'hack' at the Massachusetts Institute of Technology (MIT) usually refers to a clever, benign, and "ethical" prank or practical joke, which is both challenging for the perpetrators and amusing to the MIT community (and sometimes even the rest of the world!). Those who hack also concern themselves with hack ethic (belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism or breach of confidentiality). At the basic level, hackers are considered to be learners and explorers who want to help rather than cause damage, and who often have very high standards. Many call those who break into (crack) computer systems, "crackers". A "hacker" is someone who does some sort of interesting and creative work at a high intensity level. This applies to anything from writing computer programs to pulling a clever prank that amuses and delights everyone. According to the "hacker ethic", a hack must:

- be safe;
- not damage anything;
- not damage anyone, either physically, mentally or emotionally;
- be funny, at least to most of the people who experience it.

However, trouble arises when these hackers go overboard and start prying into protected system and data for personal gain or mischief. There have been attempts to hack into remote computer systems for multiple purposes like data

theft, fraud, destruction of data, causing damage to computer systems, etc. It should be noted that hacking *per se* might not be injurious unless the hacker does something beyond the act of hacking like even reading through data/ information stored on the hacked computer. For instance, hacking to Internet and telephone service providers' computer systems and stealing personal information and making bomb threats.

In March 2005, one Mr. Lyttle, who is known as one of the members of the self-titled hacking group called 'The Deceptive Duo', pleaded guilty and admitted that he unlawfully accessed computer systems of various American federal agencies in April 2002, including the Department of Defense's Defense Logistic Information Service (DLIS), the Office of Health Affairs (OHA), and NASA's Ames Research Center (ARC). In particular, Mr. Lyttle admitted that he gained unauthorized accessed to DLIS computers in Battle Creek, Michigan, for the purpose of obtaining files that he later used to deface an OHA website hosted on computers in San Antonio, Texas.[1]

In April 2005, a person by name Mr. Heckenkamp was sentenced to imprisonment for gaining unauthorized access to eBay computers during February and March 1999. Using this unauthorized access, Mr. Heckenkamp defaced an eBay Web page using the name "MagicFX". He also installed "trojan" computer programs – or programs containing malicious code masked inside apparently harmless programs – on the eBay computers that secretly captured usernames and passwords that Mr. Heckenkamp later used to gain unauthorized access into other eBay computers. He also gained unauthorized access to Qualcomm computers in San Diego in late 1999 and installed multiple "trojans" programs which captured usernames and passwords used to gain unauthorized access into more Qualcomm computers.[2]

8.3.2 Indian Law

Under the Indian law, however, 'hacking' has been given a wider dimension then mere 'illegal access' as contemplated under the Cyber Crime Convention. Hacking simpliciter entails civil consequences whereas hacking along with commission of other act like downloading information or lodging a virus results in criminal charges.

The definition provided under the Indian law surpasses the generally accepted meaning of hacking. Section 66(1) of the IT Act requires hacking to mean:

"(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack."

A plain reading makes it amply clear that the pre-requisite for 'hacking' is not plain unauthorized access to a computer, whether intentional or not, but further requires: (a) destruction or deletion or alteration of any information residing in a computer resource; (b) such activity has lead to the diminishing of the value or utility of the information or affects it injuriously by any means; and, (c) such activity was done to cause or knowing that it is likely to cause

wrongful loss or damage to the public or any person. We will revert to further discussion on this a bit later in this unit.

The Indian law provides for damages in case mere hacking or unauthorized access into a computer system. A person might just gain access, without authorization, into a computer system and do nothing else. The IT Act provides for payment of compensation in case of such illegal intrusion. Section 43 (a) provides that:

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

a) accesses or secures access to such computer, computer system or computer network;

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

Thus, any access to a computer without the permission of the owner or any other person who is in-charge would entail civil consequences. There is no requirement of any actual damage, either data or information damage or computer damage, for liability under section 43(a). Mere unauthorized access is enough.

Hacking coupled with some other act would lead to criminal charges. If an act done comes within the definition of hacking provided in Section 66(1) reproduced above, it would be punishable in accordance with sub-section (2) of Section 66:

"Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both."

A reading of sub-section (1) makes it clear that the emphasis for committing 'hacking' under the IT Act is on the effect i.e. on the information residing in the computer and any subsequent wrongful loss due to access rather than mere access to a computer itself. For instance, if somebody needs to steal credit card numbers and passwords from a computer system, he has to necessarily access the computer and then download the information. Such access might be authorized or unauthorized. The emphasis of 'hacking', under Section 66, is not on the nature of access but rather on the act done subsequent to such access. Generally, 'hacking' concerns access to a computer. Further acts are categorised under different cyber crimes. However, as we move ahead and deal with different kinds of cyber crimes, it would be clear that most, if not all, of the cyber crimes emanate from section 66(1). The Indian law, for the purposes of cyber crimes, is almost condensed into section 66.

Special provisions have been framed under the IT Act for protection of 'protected systems'. Section 70 deals with declaration of a system to be a protected system, persons authorized to access such system and further provides for punishment in case unauthorized access into protected system. It reads thus:

"**70. Protected system.**

1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine."

The appropriate Government has been defined under clause (3) of sub-section (1) of Section 2 as:

"appropriate Government" means as respects any matter,—

i) enumerated in List II of the Seventh Schedule to the Constitution;

ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

Instances of a 'protected system' could be computer systems belonging to the defence, income tax department computer systems, atomic and nuclear energy systems, computer systems of educational institutions of national importance like the Super Computer Centre at the Indian Institute of Sciences, Bangalore. It is noticeable that where the maximum punishment for hacking under section 66 is three years imprisonment, the same can go upto ten years in case of access or attempt to access to a protected system under section 70.

8.3.3 Cyber Crime Convention of the Council of Europe

Under the Convention for Cyber crime by the Council of Europe, hacking has been termed as 'illegal access' in Article 2. It refers to access to the whole or any part of a computer system without right. Such access should be committed intentionally and might be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. The scope of 'illegal access' under the Convention is somewhat broader than mere 'hacking'. It would also include 'cracking' and any other access made without authorization, by whatever name it might be called. The requirements are two fold: (a) access without right; (b) intentional access.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What is hacking and when it is punishable under Indian law?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8.4 DENIAL OF SERVICE

A ‘denial-of-service’ attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service. As the name suggests, the purpose is to deny someone from using a service.

Examples include:

- 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.

Denial-of-service attacks can essentially disable one’s computer or one’s network. Depending on the nature of the enterprise, this can effectively disable an organization. The term can be applied to any situation where an attacker attempts to prevent the use or delivery of a valued resource to its intended audience or customer. It can be implemented via multiple methods, physically and digitally.

For example, an attacker can deny access to telephone systems by physically cutting the telephone lines. Another way could be by calling a person continuously so that any other trying to contact the ‘attacked person’ finds such person’s phone line busy all the time.

In the online world, denial-of-service would include blocking the computer systems of, for example, a bank. It can have devastating effects where a bank’s website is blocked so that its customers are unable to avail the online services, unable to open their accounts or transact online.

In what was described as the most devastating assault on the World Wide Web in the history of the Internet, a teenager by name ‘Mafiaboy’ was, on 07.02.2000, able to deny legitimate users the services of Yahoo.com by propelling an encyclopaedia’s worth of electronic information every second. By using various university computers as ‘zombies’, he was able to attack the Web site from various virtual locations. On second day, Buy.com, eBay.com, CNN.com and Amazon.com could not be reached by the online customers. On the third day, stock traders of E*TRADE Financial were stymied when its Internet servers were felled by a barrage of data. This particular DDoS led to a loss of millions in revenue because shoppers were blocked from each company’s Internet home page. After a thorough investigation, Mafiaboy, a 15-year old boy, was traced in Montreal, Canada.

8.4.1 Distributed Denial of Service

Where denial-of-service is referred to a single computer disabling another computer or network, a distributed denial-of-service is one where a number of compromised systems attack a single target. The attacker identifies a ‘master’ system and ‘slave’ systems (which might be thousands depending upon the availability), and with the use of viruses and Trojan horse programs, controls such systems and initiates a sustained attack on the target system. The purpose is to flood the target system with incoming messages coming from all the compromised systems thereby forcing it to shut down, and denying service to the system to legitimate users. With enough such slave systems, the services of even the largest and most well-connected websites can be denied.

In December 2005, one Mr. Clark admitted to have accumulated approximately 20,000 ‘bots’ by using a worm program that took advantage of a computer vulnerability in the Windows Operating System – the ‘Remote Procedure Call for Distributed Component Object Model’, or RPC-DCOM vulnerability. The ‘bots’ were then directed to a password-protected Internet Relay Chat (IRC) server, where they connected, logged in, and waited for instructions. When instructed to do so by Mr. Clark, the ‘bots’ launched DDoS attacks at computers or computer networks connected to the Internet. Mr. Clark personally commanded the ‘bots’ to launch DDoS attacks on the name server for eBay.com. As a result of these commands, Mr. Clark intentionally impaired the infected computers and eBay.com.[3]

8.4.2 Indian law

Section 43(f) of the IT Act specifically provides for penalty in case anyone is found guilty of causing denial of access. It reads as under:

“If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(b) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.”

8.4.3 Convention on Cyber Crime of the Council of Europe

The Convention on Cyber crime covers denial-of-service under Article 5. It states that:

"Article 5 – System interference: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

The attacker interferes with the system while it, without right, transmits and/ or inputs data which seriously hinders the functioning of a computer system. The Convention requires every member-country to make domestic laws which establishes such acts as criminal offences.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What are the ways by which the legitimate users are denied access to the network?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8.5 CRIMES RELATING TO ELECTRONIC MAIL: E-MAIL SPAMMING/E-MAIL BOMBING

Spam refers to sending of unsolicited messages in bulk. Technically, it overflows the limited-sized memory by excessively large input data. In relation to e-mail accounts, it means bombing an e-mail account with a large number of messages maybe the same or different messages. The contents of the message are not

relevant. Neither does it refer to ‘abuse’ messages or ‘advertisements’. It necessarily is measured by the number of messages which are sent across as to have the tendency of blocking the e-mail account. Instead of sending huge volumes of data at one go (as in denial-of-service), the general practice seems to be of sending a few messages everyday, regularly and constantly. The economic costs are generally unrecoverable in terms of user’s time, attention and effort to go through each and every message and disposing them. The MSN Hotmail and Yahoo accounts presently are the most sought for places for sending regular spam e-mails.

Interestingly, there is a company by name SPAM selling primarily food products. On their website, www.spam.com, there is an interesting history on ‘spam’. As the story goes, in Monty Python skit, a group of Vikings sang a chorus of “spam, spam, spam...” in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because all unsolicited mails are drowning out normal communication on the Internet.

In March 2006, one Clason from New Hampshire (USA) with two more associates pleaded guilty of transmission of spam e-mails containing graphic pornographic images. They conspired to engage in the business of sending spam e-mails for their own personal gain. America Online, Inc. received more than 600,000 complaints between Jan. 30, 2004 and June 9, 2004 from its users regarding spam e-mails that had allegedly been sent by the defendants’ spamming operation. The e-mails sent by the accused advertised pornographic Internet Web sites in order to earn commissions for directing Internet traffic to these Web sites.[4]

In *EarthLink Inc.* v. *Smith*,[5] the court awarded an Atlanta-based Internet service provider EarthLink Inc. $24.8 million against the defendant, a junk e-mailer based in Johnson City, Tenn, for bombarding its network with more than one billion e-mails over a 12-month period. It was found that the defendant was engaged in a massive scheme of illegal acts, including spamming. He would pose as someone with a legitimate need for passwords and credit card numbers, including the ISP of the victim, or a retail merchant trying to complete a sale, to obtain them. He would then use the accounts of EarthLink customers to send out more fraudulent e-mails, or open accounts and sell them to other spammers for the same purpose, opening over 1,000 accounts in all.

8.5.1 Problem for ISPs

For Internet service providers (ISP), spam e-mails present a big threat because of its enormity and anonymity. A spammer can very well send hundreds of messages to a particular ISP server thereby blocking the genuine messages to reach the ISP at all. The disgruntled consumers would prefer shifting over to another ISP service. In terms of infrastructure, these spam mails also put an enormous pressure on the computer systems and networks.

8.5.2 ‘False’ Spam Messages

It is also noticed that most of the ‘spam’ messages clogging online mailboxes probably are ‘false’ in some way. The US Federal Trade Commission is of the

view that spam e-mails involving investment and business opportunities are especially dubious, with an estimated 96 per cent containing information that probably is false or misleading. In a study of random sample of 1,000 unsolicited e-mails taken from a pool of more than 11 million pieces of spam collected, the agency looked for deceptive claims in a message's text or the 'from' or 'subject' lines. Twenty percent of the spam studied involved business opportunities such as work-at-home and franchise offers. Offers for pornography or dating services accounted for another 18 per cent. Spam involving pitches for credit cards, mortgages and insurance was the third largest category at 17 per cent.

8.5.3 Indian Law

The issue of spamming has not been directly dealt with in any Indian statute. However, the law of nuisance under tort law can be employed, for the present, for bringing the spammer to books. Under the law of torts, nuisance is supposed to have been caused by an act or omission, whereby a person is unlawfully annoyed, prejudiced or disturbed in the enjoyment of property. The feature that gives it unity is the interest invaded. The emphasis is more on the harm to the plaintiff rather than the conduct of the defendant.

Spam is an unsolicited message requiring one's time and effort to get rid off. A regular supply of such spam messages would naturally result in considerable annoyance. It would also directly hamper the interest of the user in his electronic mailbox where he does not expect any interference and encroachment. The result, apart from loss of Internet working hours and thwarting one's regular e-mail stream, could be one of mental agony and distress.

In case an Internet service provider is receiving a voluminous, regular supply of spam messages that is disrupting its entire network and consuming its disk space, section 43(e) of the IT Act can be a good refuge. Section 43(e) requires that a person should have disrupted or caused the disruption of any computer, computer system or computer network. A constant barraging of unwanted messages causing non-delivery of genuine messages to and from its users would be enough for an ISP for claiming disruption of a computer network. However, since there are related concerns of availability of 'opt-in' and 'opt-out' options with spam messages, it is desirable that a law directly relates to spamming and its punishment be introduced.

8.5.4 Cyber Crime Convention of the Council of Europe

Since the unsolicited bulk emails have the capability of interference with regular flow of data also hamper the regular working of a system, they can be categories under Articles 4 and 5 of the Convention. Article 4 requires every member-State to adopt such laws so as to make every act of damaging, deletion, deterioration, alteration or suppression of computer data without right an offence. Similarly, Article 5 of the Convention requires the member-States to take legislative steps to declare such act as an offence which, when intentionally committed, seriously hinders without right the functioning of a system by *inputting, transmitting,* damaging, deleting, deteriorating, altering or suppressing computer data.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What is e-mail spanning or bombing? Discuss how it affects the user of e-mail service as well as the service provider.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8.6 CRIMES RELATING TO ELECTRONIC MAIL: E-MAIL SPOOFING

E-mail spoofing is electronic disguising. A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. It is the process of electronically covering one's electronic communication in the name of another. It is the practice of disguising an e-mail to make the e-mail appear to come from an address from which it actually did not originate. It involves placing in the "From" or "Reply-to" lines, or in other portions of e-mail messages, an e-mail address other than the actual sender's address, without the consent or authorization of the user of the e-mail address whose address is spoofed.

E-mail spoofing may occur in different forms, but all have a similar result: a user receives e-mail that appears to have originated from an ostensible source. It is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). The purpose is make one reveal such information which otherwise would not be revealed by the person himself or by an organization constrained by privacy laws. Examples of spoofed e-mail that could compromise one's information:

- E-mail claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this;

- E-mail claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information;
- E-mail from your credit card company asking again for your personal details, credit card number and password to access online account, etc.

In *Federal Trade Commission* v. *Brian D. Westby* [2004 WL 1175047 (N.D.I11.), Case No.03 C 2540, judgment on 4 Mar. 2004.] et al, the US District Court of Illinois found the defendants guilty of spoofing and passed an order of injunction restraining and enjoining them from the practice of spoofing in connection with the advertising, promotion, offering or sale of goods in commerce. Since May 2002, the defendant has been engaged in the activity of sending unsolicited bulk commercial emails with e-mail addresses of un-related third parties as the "reply-to" or "from" address. As a result, third parties whose e-mail addresses or domain names were spoofed suffered injury to their reputations by having themselves wrongfully affiliated with the sending of bulk unsolicited e-mail.

8.6.1 Indian Law

E-mail spoofing is a variation of digital forgery where one attempts to impersonate another person by sending a false electronic record which though purported to be have been made and/or signed by the latter person, but in fact is not. This kind of computer crime is also covered by the provisions under the IPC relating to forgery under Chapter XVIII of the Indian Penal Code. Particularly, Section 463 dealing with forgery needs proper interpretation. Section 463 reads as under:

"463. Forgery.-Whoever makes any false documents or part of a document with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery."

Since the primary objective of e-mail spoofing is to induce the receiver of e-mail to part with certain information by making a false document purportedly sent by a person from whom it is not actually sent, it would be covered within the offence of forgery. However, it is desirable that a law directly relating to e-mail spoofing and punishment thereof be framed.

8.6.2 Cyber Crime Convention of the Council of Europe

Under the Convention on Cyber crime, Article 7 requires the member-States to make laws to establish as criminal offences, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. The scope of this Article is wide and would also include e-mail spoofing since it involves input of data (an e-mail address in the 'From' column of an e-mail) resulting in inauthentic data (a false 'From' e-mail address) for the purpose of being acted upon and divulge information which otherwise the receiver of the e-mail would not.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

What is e-mail spoofing.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8.7 SUMMARY

Computer and cyberspace has given rise to many of the wrongs which were hitherto unknown to the mankind. These crimes are of very complicated nature and highly sophisticated technology is applied in committing these crimes.

Indian IT Act has made adequate provisions for punishing these crimes. Some of the examples of this crimes are –

Hacking/Unauthorized Access

- Hacker Ethics
- Indian Law
- Cyber Crime Convention

Denial of Service

- Distributed Denial of Service
- Crimes relating to Electronic Mail: E-mail Spamming/E-mail Bombing
- Problem for ISPs
- 'False' spam messages
- Indian Law
- Cyber Crime Convention

Crimes relating to Electronic Mail

- E-mail Spoofing
- Indian Law
- Cyber Crime Convention

8.8 TERMINAL QUESTIONS

1) Discuss in brief the various forms of computer and cyberspace related crimes. Does the Indian law adequately deal with them?

8.9 ANSWERS AND HINTS

1) Trespassing is a word known to us. Simply put, it means entering upon or into a property owned by someone else without his or her permission. In the offline world, 'entering' would imply physical entry into the property. Trespassing has both civil and criminal consequences. Trespassing has a digital counterpart which is referred to as hacking. Hacking means unauthorized access to a computer system. The computer serves as a tool to commit the crime as also necessarily is the target of such crimes. It is one of the most popular and fastest growing computer crimes and has been escalated with the aid of the Internet.

2) A 'denial-of-service' attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service. As the name suggests, the purpose is to deny someone from using a service

   Denial-of-service attacks can essentially disable one's computer or one's network. Depending on the nature of the enterprise, this can effectively disable an organization. The term can be applied to any situation where an attacker attempts to prevent the use or delivery of a valued resource to its intended audience or customer. It can be implemented via multiple methods, physically and digitally.

3) Spam refers to sending of unsolicited messages in bulk. Technically, it overflows the limited-sized memory by excessively large input data. In relation to e-mail accounts, it means bombing an e-mail account with a large number of messages maybe the same or different messages. The contents of the message are not relevant. Neither does it refer to 'abuse' messages or 'advertisements'. It necessarily is measured by the number of messages which are sent across as to have the tendency of blocking the e-mail account. Instead of sending huge volumes of data at one go (as in denial-of-service), the general practice seems to be of sending a few messages everyday, regularly and constantly. The economic costs are generally unrecoverable in terms of user's time, attention and effort to go through each and every message and disposing them. The MSN Hotmail and Yahoo accounts presently are the most sought for places for sending regular spam e-mails.

4) E-mail spoofing is electronic disguising. A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. It is the process of electronically covering one's electronic communication in the name of another. It is the practice of disguising an e-mail to make the e-mail appear to come from an address from which it actually did not originate. It involves placing in the "From" or "Reply-to" lines, or in other portions of e-mail messages, an e-mail address other than the actual sender's address, without the consent or authorization of the user of the e-mail address whose address is spoofed.

8.10 REFERENCES AND SUGGESTED READINGS

1. <http://www.usdoj.gov/criminal/cybercrime/lyttlePlea.htm>.

2. <http://www.usdoj.gov/usao/can/press/html/2005_04_25_ heckenkamp.html>.

3. <http://www.usdoj.gov/usao/can/press/html/2005_12_28_ Clarkbotplea.htm>.

4. 6 No. 7 Cyber crime L. Rep. 4 Mar. 2006 <http://www.usdoj.gov/opa/ pr/2006/March/06_crm_123.html>.

5. 2 No. 15 Cyber crime L. Rep. 4; N.D. Ga., No. 1:01-CV-2099. 7 Sep.2002.

UNIT 9 CRIMES RELATING TO DATA ALTERATION/DESTRUCTION

Structure

9.1 INTRODUCTION

Like the previous unit, this unit also discusses the the crimes which are committed on the cyberspace. These crimes are commonly called as the crimes relating to the data alteration and destruction.

Crimes relating to data alteration and data destruction are increasing day-by-day. As the use of computer and Internet is increasing, more and more people are finding it benificial in their day-to-day life many of the transactions of various types are being conducted on the Internet. This has provided opportunity to unscruplous people who are indulging in all sorts of activities to defraud and cheat innocent people using Internet.

This unit tries to discuss some of the comman types of such crimes on the Internet and laws to prevent such crimes.

9.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss what internet fraud is and what its various forms are;
- analyse and distinguish amongst the various types of viruses, worms, trojan horses, and logic bombs etc and discuss how they are harmful to the computer and computer-networks; and
- analyse other forms of Internet fraud such as theft of Internet hours, salami attacks, data diddling, steganography etc.

9.3 INTERNET FRAUD AND FINANCIAL CRIMES

The term 'Internet fraud' refers generally to any type of fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mail, message boards, or Web sites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or others connected with the scheme. With anonymity and speed, Internet is a haven for fraudsters. There are various fraudulent schemes envisaged over the Internet from which the criminals benefit financially. Some of them are as follows:

9.3.1 Auction and Retail Schemes Online

According to the 2005 statistics of Internet Fraud Watch (www.fraud.org), 72% of the complaints made on Internet fraud relates to schemes appearing on online auction and retail sites. These schemes typically purport to offer high-value items – ranging from Cartier watches to computers to collectibles such as Beanie Babies – that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods).

9.3.2 Business Opportunity/Work-at-home Schemes Online

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

9.3.3 Identity Theft and Fraud

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Unlike one's fingerprints, which are unique to oneself and cannot be given to someone else for their use, one's personal data like bank account number or credit card number, telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at other's expense.

9.3.4 Credit Card Fraud

Credit card fraud, as the name suggests, involves misusing someone else's credit cards for one's own benefit. This risk of credit card fraud has increased manifold especially after the advent of e-commerce. People purchase products online through their credit cards. The Web sites offering products for purchase require the credit card details of the online buyer so that the price can be credited to the card. In the process, the details of the credit cards are stored on the server of the online retailer. If one is able to access the servers containing the credit cards details of the online consumer, it is easy to collect those details and then use for one's own benefit in online transactions. One can also sell the credit card information to someone else. For instance, the one-stop online marketplace, "Shadowcrew.com" website, was taken down in October 2004 by the U.S. Secret Service, closing an illicit business that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million.

The California Department of Corporations (Internet Compliance and Enforcement), a regulator of securities trading, won an August 2000 settlement ordering Victor Idrovo to post a retraction (under the new alias of Retraction) of earlier posts to the Yahoo message board. Under the original alias, "frankgmancuso", Idrovo attempted to manipulate the price of Metro-Goldwyn-Mayer, Inc., (MGM) stock when he posed as an insider/former executive of MGM. He was also fined $4,500.[1]

9.3.5 Online Investment Schemes

9.3.5.1 Issuance of False Stocks

This in another variation of online investment schemes where the person, either authorizedly or unauthorized, gains access to the computer systems of a company and is able to issue stocks to themselves or any other person. For instance, two employees of Cisco Systems, Inc. a US company, illegally issued almost $8 million in Cisco stock to themselves. The total value of the Cisco stock that they took (at the time that they transferred the stock) was approximately $7,868,637. Both were sentenced to 34 months each in federal prison, restitution of $7,868,637 and a three year's period of supervised release.

9.3.5.2 Market Manipulation Schemes

Enforcement actions by the US Securities and Exchange Commission and criminal prosecutions indicate that the basic method for criminals to manipulate

securities markets for their personal profit is the so-called “pump-and-dump” schemes. In this scheme, they typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly traded stocks or stocks of shell companies (the ‘pump’), then immediately sell off their holdings of those stocks (the ‘dump’) to realise substantial profits before the stock price falls back to its usual low level. Any other buyers of the stock who are unaware of the falsity of the information become victims of the scheme once the price falls.

9.3.5.3 Pyramid or Ponzi Schemes

Pyramid or Ponzi Schemes and chain letters are well suited to the Internet because they entice investors with the promise of quick profits using a home computer. Investors make money by recruiting new investors. The programme soon runs out of new investors and most of the players lose their money they invested. Chain letter schemes ask participants to send money to the name at the top of a list with the promise that they will eventually receive thousands of dollars when their name comes to the top.

9.3.6 Fraudulent Financial Solicitation

Due to its ease and anonymity, there have been instances of people soliciting money online for charitable purposes. One might seek financial contribution via credit card online to certain public purpose funds or schemes for the benefit of certain classes or down-trodden people of society. Many a time, fiscal statutes[2] provide for income tax exemption for such contributions and online promises are made to provide a tax exemption certificate in case such contributions are made. The website may even provide for a printout of a fake certificate.

On January 30, 2006, Gary S. Kraser pleaded guilty in the United States District Court for the Southern District of Florida to online fraud in connection with his fraudulent solicitation of charitable donations supposedly intended for Hurricane Katrina relief. According to the indictment, the defendant falsely claimed in conversations on the Internet, and ultimately via the website www.AirKatrina.com, that he was piloting flights to Louisiana to provide medical supplies to the areas affected by Hurricane Katrina and to evacuate children and others in critical medical condition. He further claimed that he had organized a group of Florida pilots to assist him in his supposed relief efforts. In just two days, the defendant received almost $40,000 in donations from 48 different victims from around the world.

9.3.7 Phishing

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

The Delhi High Court in the case of *NASSCOM* v. *Ajay Sood*[3] elaborated upon the concept of 'phishing'. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of NASSCOM. The plaintiff had filed the suit inter alia praying for a decree of permanent injunction restraining the defendants from circulating fraudulent e-mails purportedly originating from the plaintiff. The court declared 'phishing' on the Internet to be a form of Internet fraud and hence, an illegal act. The court stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details. This case had a unique bend since it was filed not by the one who was cheated but by the organization, who was being wrongly represented that is NASSCOM. In this regard, the court was of the view that even though there is no specific legislation in India to penalize phishing, it is illegal being "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even the person whose name, identity or password is misused". The court held the act of phishing as passing off and tarnishing the plaintiff's image, thereby bringing it within the realm of trademark law.

In February 2006, the Federal Bureau of Investigation, USA, become aware of a spam e-mail which claimed that the recipient is eligible to receive a tax refund for $571.94. The e-mail claimed to be from tax-returns@irs.gov with the subject line of "IRS [119(2005)DLT596. 2005(30)PTC437(Del). judgment delivered on 23 Mar. 2005] Tax Refund". A link was provided in the e-mail to access a form required to be completed in order to receive the refund. The link appeared to connect to the true IRS website. However, the recipient was redirected to http://www.porterfam.org/2005/, where personal data, including credit card information, was captured[4].

9.3.7.1 Indian Law

The IT Act deals with the crimes relating to Internet fraud and online investment fraud in sections 43(d), 65 and 66.

"**43.** If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(a) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

"**65. Tampering with computer source documents.**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program computer system or computer network, when the computer source code is required to be kept or maintained

by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—for the purposes of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form."

"**66. Hacking with computer system.**

1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both."

Section 43(d) penalizes a person who damages or causes damage to data. 'Damage', under clause (IV) of the Explanation, means to destroy, alter, add, modify or rearrange any computer resource by any means. Therefore, unauthorized alteration of data would come within the ambit of section 43(d) which is sufficient to cover computer crimes like issuance of false stocks or market manipulation schemes since they essentially involve alteration and/or addition of data.

Section 65 makes tampering with computer source code an offence. 'Computer source code' has been defined as the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Internet fraud would also come within the scope of section 66 of the IT Act dealing with wrongful loss or damage to the public or any person due to destruction or alteration of any data residing in a computer resource or due to diminishing its value or utility or affecting it injuriously by any means.

Under the Indian Penal Code, Internet fraud would be covered by sections 415 to 420 which relates to 'cheating'. One is said to 'cheat' when he, fraudulently or dishonestly, induces another person to deliver any property to him by deceiving such person and which act causes damages or harm to the person deceived in body, mind, reputation or property. If on the Internet, one is, by any of the numerous fraud schemes enumerated above, able to deceive a person so as to induce him to deliver any sum of money, it would be a case of 'cheating'. Section 416 deals with 'cheating by personation' that is inter alia cheating by pretending to be some other person. This covers 'phishing' as well. For example, in the NASSCOM case above, the defendant could well be held up for an offence committed under section 416 for pretending that he is representing NASSCOM while communicating with third parties.

9.3.8 Convention on Cyber – Crime Council of Europe

Article 8 of the Convention on Cyber Crime covers Internet fraud and requires the member-states to suitably alter their legislations so as to make the following an offence in their countries:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data,

b) any interference with the functioning of a computer system,

With fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Discuss the various forms of Internet fraud. What are the legal provisions dealing with them?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

9.4 VIRUS, WORMS, TROJAN HORSES AND LOGIC BOMBS

This set of attacks onto the computer/computer data is by way of transmitting programs designed to destroy, alter, damage, or even send across data residing in the computer. The transfer of data through floppy was considered to be of potential danger in transmitting such programs. With the growth of the Internet, the threat has multiplied many-fold. Quite easily can one knowingly/ unknowingly transfer such programs via e-mail? There have been innumerable instances in the last few years where such programs have been sent across e-mails through an innocent looking attachment. There are primarily four kinds of such programs available: virus, worms, Trojan horses and logic bombs.

9.4.1 Virus & Worms

A virus is a program that searches out other programs and 'infects' them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the 'infection'. This normally happens invisibly to the user. However, unlike a worm, a virus cannot infect other computers without assistance. The virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things like writing messages on the terminal or playing strange tricks with the display. Certain viruses, written by particularly perversely minded crackers, do irreversible damage, like deleting all the user's files. On the other hand, a worm is a program that propagates itself over a network, reproducing itself as it goes. Therefore, worm, unlike a virus, does not require a medium to propagate itself and infect others.

One Smith was involved in unleashing the "Melissa" computer virus in 1999, causing millions of dollars in damage and infecting untold numbers of computers and computer networks. He posted an infected document on the Internet newsgroup "Alt.Sex". The posting contained a message enticing readers to download and open the document with the hope of finding passcodes to adult-content websites. Opening and downloading the message caused the Melissa virus to infect victim computers. The virus altered Microsoft word processing programs such that any document created using the programs would then be infected with the Melissa virus. The virus also lowered macro security settings in the word processing programs. The virus then proliferated via the Microsoft Outlook program, causing computers to send electronic e-mail to the first 50 addresses in the computer user's address book. Because each infected computer could infect 50 additional computers, which in turn could infect another 50 computers, the virus proliferated rapidly and exponentially, resulting in substantial interruption or impairment of public communications or services. According to reports from business and government following the spread of the virus, its rapid distribution disrupted computer networks by overloading e-mail servers, resulting in the shutdown of networks and significant costs to repair or cleanse computer systems. Smith was eventually sentenced to prison after pleading guilty.[5]

9.4.2 Trojan Horses

Trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or a program to find and destroy viruses. It portrays itself as something other than what it is at the point of execution. The malicious functionality of a Trojan horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

A special case of Trojan Horses is the *mockingbird* — software that intercepts communications (especially login transactions) between users and hosts and provides system-like responses to the users while saving their responses (especially account IDs and passwords).

9.4.3 Logic Bombs

A logic bomb is a code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met. In an instance of logic bomb, a computer systems administrator for UBS PaineWebber was charged with using a 'logic bomb' to cause more than $3 million in damage to the company's computer network. It was alleged that from November 2001 to February 2002, the accused constructed the logic bomb computer program. On March 4, as planned, his program activated and began deleting files on over 1,000 of PaineWebber's computers [*U.S.* v *Smith*][6].

9.4.4 Back Door

Another way to enter into a computer is by creating a back door. It is a hole in the system's security deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. Historically, back doors have often lurked in systems longer than anyone expected or planned, and a few have become widely known.

9.4.5 Indian Law

Section 43(c) of the IT Act covers the area of introduction of viruses, etc. The relevant portion reads as under:

"**43.** If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

He shall be liable to pay damages by way of compensation not exceeding one core rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i)"computer contaminant" means any set of computer instructions that are designed—

a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or

b) by any means to usurp the normal operation of the computer, computer system, or computer network;

iii) "computer virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;"

The law pertaining to viruses, worms, Trojan horses and logic bombs have all been culminated into the above provision. The explanations to the words 'computer contaminant' and 'computer virus' are wide enough to cover all the above.

In cases where the purpose of introduction of virus, worms, etc. in a computer is to destroy or alter or delete the information residing in such computer system, the offender would also be liable for criminal charges under section 66 of the IT Act, 2000.

9.4.6 Cyber Crime Convention of the Council of Europe

Both Articles 4 and 5 of the Convention can be employed, depending upon the extent of damage caused due to introduction of virus, worms, etc. in a given computer system. Article 4 covers such offences which, committed intentionally, damages, deletes, deteriorates, alters or suppresses computer data without right. On the other hand, Article 5 deals with system interference that is hindrance to the functioning of the computer system itself, when committed intentionally by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. Since viruses, worms, etc. are basically computer programs designed to alter information/data/programs on a computer so as to cause calculated damage, introduction of such destructive programs amounts to data and system interference envisaged within Articles 4 and 5 of the Convention.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What do you understand by the terms—virus, worm, Trojan horse and logic bombs? What are the legal provisions for punishing people engaged in harming the computers through them?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

9.5 THEFT OF INTERNET HOURS

Theft of Internet hours refers to using up or utilizing of somebody else's Internet services. In many cases, when a person takes up the services of any Internet service provider, he utilizes the services in terms of number of hours consumed and makes the payment on a per hour basis. However, in case a third person is able to identify the username and password of the Internet service user, he can easily consume those Internet hours.

9.5.1 Indian Law

Section 43(h) of the IT Act addresses the issue of theft of Internet hours.

"**43.** If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one core rupees to the person so affected.

9.6 SALAMI ATTACKS

This attack is 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 the bank's servers, that deducts a small amount of money (say 10p. a month) from the account of every customer. No single account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month. The classic story about a salami attack is the old "collect-the-round off" trick. In this scam, a programmer modifies arithmetic routines, such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary two or three kept for financial records. For example, when currency is in rupees, the round off goes up to the nearest paisa about half the time and down the rest of the time. If a programmer arranges to collect these fractions of paisa in a separate account, a sizable fund can grow with no warning to the financial institution.

9.6.1 Indian Law

'Salami Attacks' would be covered by section 477A of the IPC relating to falsification of accounts and section 66 of the IT Act.

Section 477A of the IPC makes it an offence for any clerk, officer or servant to wilfully and with an intend to defraud, to destroy, alter, mutilate or falsify any electronic record or making or abetting the making of any false entry in any such electronic record. Therefore, making alterations in and additions of any electronic entry in the bank's computers would bring the offender within the ambit of section 477A of the IPC.

This is also covered by section 66 of the IT Act whereunder any destruction or deletion or alteration of any information residing in computer resource or diminishing its value or utility or affecting it injuriously so as to cause wrongful loss or damage to the public or any person would be an offence.

9.7 DATA DIDDLING

This computer crime relates to operation security and is minimized through strengthening of internal security controls. 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. This is a simple and common computer related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data.[7]

9.7.1 Indian Law

Alteration of data residing in computer resource or diminishing its value or utility or affecting it injuriously so as to cause wrongful loss or damage to the public or any person would be an offence under section 66 of the IT Act. Such kind of computer crime would also be covered by section 43(d) of the IT Act.

9.8 STEGANOGRAPHY

Steganography is the process of hiding one message or file inside another message or file. According to Dictionary.com, steganography (also known as ‘steg’ or ‘stego’) is “the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key”. It has been used in ancient times as well.[8] In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file.[9] For instance, steganographers can hide an image inside another image, an audio file, or a video file, or they can hide an audio or video file inside another media file or even inside a large graphic file. Steganography differs from cryptography in that while cryptography works to mask the content of a message, steganography works to mask the very existence of the message.[10]

Following steps are generally followed to achieve the desired result:

a) Locating a data/video/audio file which requires being hidden and transmitted.

b) Locating a carrier file which will carry the data/video/audio file.

c) Using appropriate steganography software which will permit embedding of the data/video/audio file into the carrier file and at the receiver’s end, permit extraction thereof. A few softwares even permit password protection.

d) E-mailing the carrier file to the receiver.

e) Decryption of the message by the receiver.

There have been reports of Osama bin Laden and others hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.[11]

Though steganography can be used for quite a many legitimate purposes like watermarking images for copyright protection or secure confidentiality of information, it is used equally or rather more for illegitimate goals. It requires mention that mere use of steganography is not illegal in itself. It is a misconception that steganography is a computer crime. At the most, it can be a tool for committing another crime but cannot be a crime in itself. For example, one might send a military secret message hidden in a picture file, and then such act would be an offence under the Official Secrets Act. However, it is to be noted that it was not the use of steganography but rather sending of the military secret that is punishable. Likewise, if one is distributing pornographic pictures by hiding it in another picture with the help of steganography, such distribution would be punishable under section 67 of the IT Act. Therefore, mere use of steganography is not an offence. It merely assists a person in commission of some other offence.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What is steganography? When it becomes punishable?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

9.9 SUMMARY

With the increase in the use of computers and Internet, the crimes relating to data alteration and destruction are increasing. These crimes have manifested

in various forms in which either a person has to loose money etc or data stored on the computer is damaged or destroyed. Law has tried to keep pace with it and has made many of such acts punishable.

9.10 TERMINAL QUESTIONS

1) Discuss various forms of financial crimes. What is their effect on the individuals and the companies?

2) Discuss the concepts of virus, worm, Trojan horse, and logic bombs. What is the distinction amongst them?

9.11 ANSWERS AND HINTS

1) The term 'Internet fraud' refers generally to any type of fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mail, message boards, or Web sites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or others connected with the scheme. With anonymity and speed, Internet is a haven for fraudsters. There are various fraudulent schemes envisaged over the Internet from which the criminals benefit financially.

2) A virus is a program that searches out other programs and 'infects' them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the 'infection'. This normally happens invisibly to the user. However, unlike a worm, a virus cannot infect other computers without assistance. The virus may do nothing but propagate itself and then allow the program to run normally. Trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or a program to find and destroy viruses. It portrays itself as something other than what it is at the point of execution. The malicious functionality of a Trojan horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls. A logic bomb is a code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met. In an instance of logic bomb, a computer systems administrator for UBS PaineWebber was charged with using a 'logic bomb' to cause more than $3 million in damage to the company's computer network. It was alleged that from November 2001 to February 2002, the accused constructed the logic bomb computer program. On March 4, as planned, his program activated and began deleting files on over 1,000 of PaineWebber's computers.

   Steganography is the process of hiding one message or file inside another message or file. According to Dictionary.com, steganography (also known as 'steg' or 'stego') is "the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key".

9.12 REFERENCES AND SUGGESTED READINGS

1. <http://security.iia.net.au/downloads/doznalrt-ftc.pdf>.
2. <http://www.corp.ca.gov/pressrel/nr0011.htm>.
3. For instance, contributions made to funds listed under Section 80G of the Income Tax Act, 1961 are, to some extent, exempted from income tax.
4. Internal Revenue Service. the income tax wing of the US government.
5. No. 3 Cyber crime L. Rep. 7
6. May 2. 2002 < http://www.cybercrime.gov/melissaSent.htm>.
7. < http://www.usdoj.gov/criminal/cybercrime/duronioIndict.htm>.
8. Computer Crime Prevention, Royal Canadian Mounted Police <http://www.rcmp.ca/scams/ccprev_e.htm>.
9. For example, in ancient Rome and Greece, text was traditionally written on wax that was poured on top of stone tablets. If the sender of the information wanted to obscure the message – for purposes of military intelligence, for instance – they would use steganography: the wax would be scraped off and the message would be inscribed or written directly on the tablet, wax would then be poured on top of the message, thereby obscuring not just its meaning but its very existence. See, Kristy Westphal, "Stenography Revealed", Computer Crime Research Center <http://www.crime-research.org/eng/library/Steganography.html>.
10. *Ibid.*
11. Jack Karp. A Novice Tries Steganography. Computer Crime Research Center <http://www.crime-research.org/eng/library/Jack2.htm>.