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.