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>.