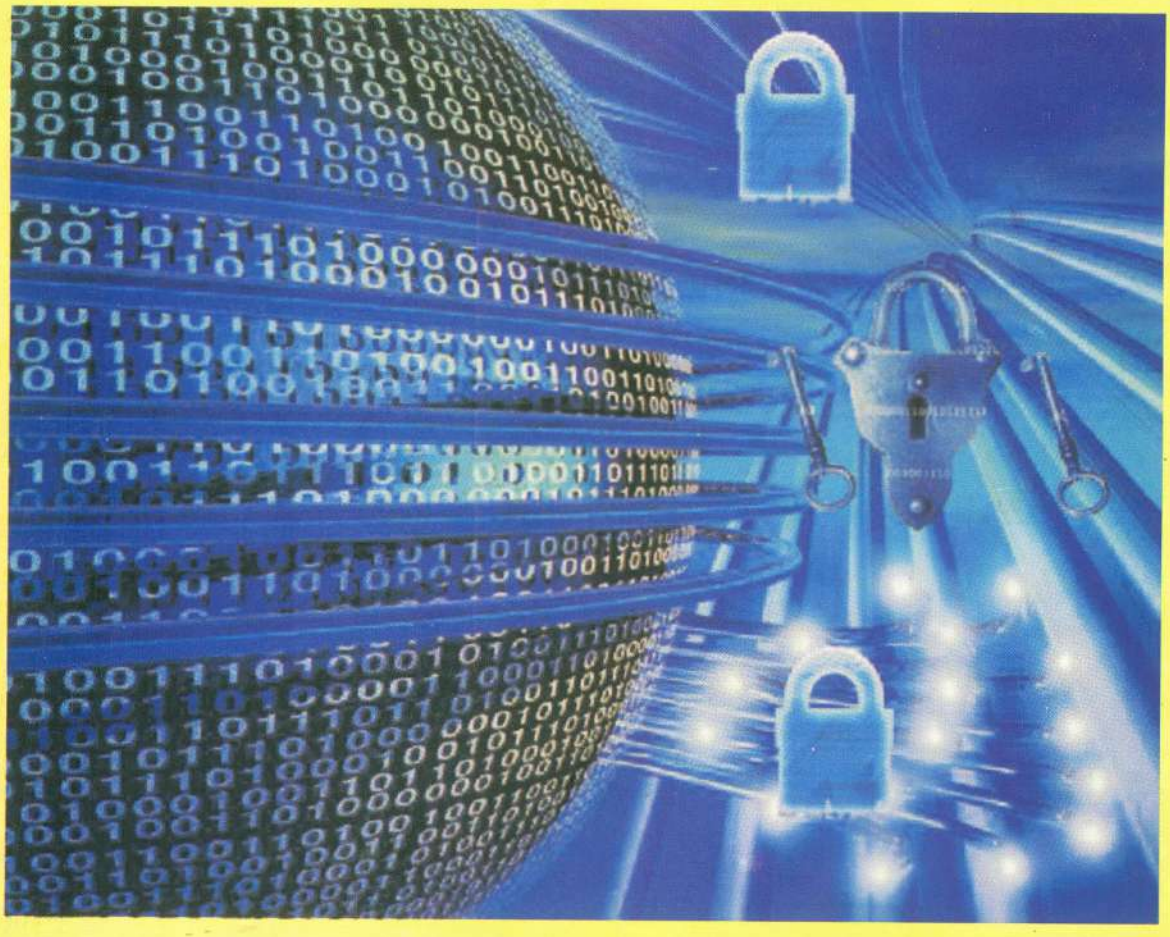
ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics



Cyber Crime and Cyber Forensics

1

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

– इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

—Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-027
Digital Forensics

Block

1

CYBER CRIME AND CYBER FORENSICS

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writer

Mr. S. Balasubramony
Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell, Delhi
(Unit 1, 2, 3 & 4)

Block Editors

Prof. Ajith Kumar R, Professor
Indian Institute of Information Technology and Management-Kerala (IIITM-K), Trivandrum, Kerala

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

February,2012

ISBN-978-81-266-5922-7

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed at: Berry Art Press A-9, Mayapuri, Phase-I New Delhi-64

COURSE INTRODUCTION

This course deals with the digital forensics. It is s a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. It is the art and science of applying computer science to aid the legal process. It is more than the technological, systematic inspection of the computer system and its contents for evidence or supportive evidence of a civil wrong or a criminal act. Computer forensics requires specialized expertise and tools that goes above and beyond the normal data collection and preservation techniques available to end-users or system support personnel.

This course stresses for the forensics team to have a solid understanding of the level of sophistication of the cyber suspect(s). If insufficient information is available to form this opinion, the suspects must be considered to be experts, and should be presumed to have installed countermeasures against forensic techniques.

This course discusses about the various branches of cyber forensics science like digital, mobile and wireless technology forensics. It is important to control increasing cyber crimes with the help of forensic science. Today, the use of computer and phone as a means in the conduct of crimes has been increasing. At the same time, it is quite difficult to detect such crimes or prevent them due to the lack of technical knowledge. Such ignorance is dangerous. Hence, this course helps in spreading awareness about the tools and mechanism for detecting such cyber crimes.

This discipline holds large relevance in this computer age. For proper cyber crime patrolling, it is necessary to know the technology needed for prevention of such crimes. Moreover, it is quite more necessary to note that technical skills should not be misused for any reason. Else, it would lead to more serious offences. Infact, the skills should be used in such a way that it helps in reducing the happening of any kind of cyber crime. This course makes the students vigilant towards the use of computer technology and makes them more responsible towards the society.

This course includes the following blocks:

Block 1 – Cyber Crime and Cyber Forensics

Block 2 – Digital Forensics: Tools and Techniques

Block 3 – Mobile Forensics

Block 4 – Security Issues in Wireless Technologies

BLOCK INTRODUCTION

This block deals with the cyber crime and cyber forensics. In common parlance all crimes committed or resorted by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system are known as cyber crime. This type of crime involves a computer and a network, where the computer may or may not have played an instrumental part in the commission of the crime. The knowledge of a computer by the subject is essential to commit the crime. Computer crimes are perpetrated in the computer environment or any illegal, unethical, unauthorised behaviour relating to the automatic processing and the transmission of data. This block comprises of four units and is designed in the following way;

The **Unit one** deals with various types of cyber crimes. Due to constant development in the field of technology, Cyber crime is a rapidly growing field and problem area for law enforcing agencies. Now, with the advancement in technology this type of crime has lost boundaries. On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft and other cross-border crimes sometimes referred to as cyber warfare.

The **Unit two** provides an overview of the banking and financial crime. It is also known as White Collar crime. We cannot expect to reap full benefits of liberalization of economy, if we do not ensure white-collar criminals being dealt with sternly and severely. The strengthening of enforcement agencies such as CBI, DRI, the Directorate of enforcement etc. is also a sine qua non. The close coordination among these agencies is also essential if a dent is to be made on the emerging white-collar economic criminality. In respect of counterfeit currency also educative advertisements are issued by the RBI from time to time.

The **Unit three** covers various types of Identity theft and Data theft and various techniques for obtaining and exploiting personal information for identity theft. Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras.

The **Unit four** covers various types of spam and botnets. Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam. Botnet is a collection of infected computers or bots that have been taken over by hackers (also known as bot herders) and are used to perform malicious tasks or functions. A computer becomes a bot when it downloads a file (e.g. an e-mail attachment) that has bot software embedded in it. This unit also covers a case study on Nigerian Letter Fraud.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 VARIOUS TYPES OF CYBER CRIMES

Structure

1.0 INTRODUCTION

Computer Crime or Cybercrime

In common parlance all crimes committed or resorted by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system are known as cybercrime. This type of crime involves a computer and a network, where the computer may or may not have played an instrumental part in the commission of the crime. The knowledge of a computer by the subject is essential to commit the crime. Computer crimes are high-tech variations of conventional crimes. In another word it is crimes perpetrated in the computer environment or any illegal, unethical, unauthorised behaviour relating to the automatic processing and the transmission of data.

Net-crime is also a type of cybercrime which more precisely refers to criminal exploitation of the Internet. With the advancement of technology and use of computers and internet in every field of life (Banking, Telecommunication, Travel, medicine and education etc.) such crime has grown rapidly. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography and child grooming etc.

Now, with the advancement in technology this type of crime has lost boundaries. On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft and other cross-border crimes sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat. There are also problems of privacy when confidential information is lost, published or intercepted, lawfully or otherwise.

From the cases the usual profile of a Cyber Criminal has emerged as generally middle class male between 14 to 30 yrs of age, well educated having high I.Q. and good knowledge of computers and internet etc.

1.1 OBJECTIVES

After going through this Unit, you should be able to:

- define cyber crime;
- list and explain various types of cyber crime reported world wide;
- describe major areas of computer crime; and
- explain various computer frauds in India.

1.2 TOPOLOGY

Computer crime encompasses a broad range of potentially illegal activities. Broadly, it may be divided into following three types/ categories:

1) Crimes that Target Computer Networks or Devices Directly

Examples of such offences are sabotage of Computer and Computer systems, sabotage on Computer networks, operating systems and programmes, theft of data, theft of marketing information, unlawful access to criminal justice and other Government Records etc.

These crimes involved techno tresspass and unauthorised access to computer systems and data on programmes stored in the computer. The common targets are military and intelligence computer, business offices by competitors, commercial or industrial or trading companies by disgruntled employees, Research & Scientific Organisations etc. However, this may not amount crime always. Some of them are as under:

a) Virus *(Vital Information Resource Under Siege)*

It is computer programmes which can self replicate or make copies itself and spread from one computer to another without help of user. They can delete files, format hard drives and they are spread via infected floppy, CDs, E-mail attachments, downloaded from Internet etc.

b) Trojan Horses

They are apparently innocuous programme that contains code designed to surreptitiously access information or computer system without user's knowledge. They have a method to send information to the person who created or implanted the Trojan.

c) Spam

The unsolicited sending of bulk e-mail for commercial purposes is unlawful to varying degrees in different countries. As applied to e-mail, specific anti-spam laws are relatively new, however limits on unsolicited electronic communications have existed in some forms for some time.

d) Worms

A computer programme that copies itself across a network which runs independently and travels across network connection is called a worm. It makes the system unusable by self-replication. A virus is dependent upon a host file or boot sector and the transfer of files between machines to spread, while a worm can run completely independently and are spread of its own will through network connections. They mainly make the systems unusable by self-replication.

e) Logic Bombs

A logic bombs is computer instructions coded in a programme that triggers the execution of a malicious act, if and when certain criteria are made. It is also called slag code and it is a programming code added to the software of an application or operating system that lies dormant until a period of predetermined time or event occurs, triggering the code into action. It is malicious in intent, acting like a virus or a trojan once activated. It is time bomb of virus.

f) Hacking

Hacking is unauthorised access to computer network bypassing the security net systems. The hackers can get access to the information that does not belong to them and can copy, alter or erase the information.

g) Spoofing

IP(Internet Protocol) Spoofing is an attack in the Internet Provider where the attacker disguises himself or herself as another user by means of a false IP network address. Whereas Spoofing is the process of disguising one computer user as another.

2) Computer is Incidental to Crime

Where computer is used by the criminals to facilitate their criminal activities such as processing of data quickly to facilitate commission of crime or for e-mailing communication by the criminals. These are significant from forensic/evidence angle.

a) Use of e-mails for communication by terrorists/organised criminals.

b) Electronic money transfer of ill-gotten wealth.

c) Electronic trading in contraband.

d) **Illegal lotteries:** Nigerian lottery fraud and offer of 'Black Dollar' by certain criminals are very common. Lot of people including educated and well place have been cheated.

3) Computer as a tool in the commission of the offence

Here the computer is used for committing an offence. For example, Computers being used for pornography, gambling, stealing money by illegal money transfer etc. Some of the crimes are fraudulent use of ATM/Debit/Credit Cards and accounts, credit cards frauds, frauds involving electronic fund transfer, computer transactions such as stock transfers, sales invoicing, telecommunication frauds etc. Other examples are:

a) Pornography / Paedophaely: Obscene or Offensive Content

In such cases the content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.

The extent to which these communications are unlawful varies greatly between countries. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

b) Harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups and by sending hate e-mail to interested parties. Cyber bullying, cyber stalking, harassment by computer, hate crime, Online predator and

stalking etc. are the other examples. Any comment that may be found derogatory or offensive is considered harassment.

c) Intellectual Property theft

This includes software piracy which is on the rise, involving illegal duplication and distribution.

d) Hardware theft

This is normal theft related to hardware.

e) Denial of Service Attacks

An attack that causes the targeted system to be unable to fulfill its intended function because of sending so many useless information flooding the network.

f) Cyber Stalking

It is sending unwanted and distasteful mails in someone's machine from unauthorised persons who somehow got the password illegally. Some of the mails may be intimidating or obscene. Some times due to such mails and details gathered/ passed on during chatting people start getting obnoxious telephone calls during night time. Callers told that they have been invited to call on telephone at night on the chatting site.

1.3 TYPES OF CYBER CRIME

1.3.1 Common Types of Cyber Crime

- **Sale of prohibited goods through net.**
- **Phishing scams**

  In such cases personal information viz. Bank account number, log-in ID and passworld etc. is sought from the public by sending messages after creating false web-site of an organisation. The purpose behinf is to misuse the information so obtained. A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators.

- **Drug trafficking**

  Believe it or not, drug trafficking is happening over the Internet. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail or password-protected message boards to arrange drug deals. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills and swap recipes for amphetamines in restricted-access chat rooms.

  The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

- **Cyber terrorism**

  Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scams since

early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network and the information stored on them.

A simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

- **Cyber warfare**

  Cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance.

- **Spam**

  The most common type of cyber crime is spam. While e-mail spam laws are fairly new, there have been laws on the books regarding "unsolicited electronic communications" for many years.

- **Fraud**

  Credit fraud is another common form of cyber crime. Certain computer viruses can log keystrokes on your keyboard and send them to hackers, who can then take your Social Security number, credit card number and home address. This information will be used by the hacker for his own means.

- **Cyber Bullying**

  Harassment or cyber bullying, is a growing problem among teenagers Many countries in Europe and several states in the United States have laws to punish those who consistently harass somebody over the Internet. Drug Trafficking

- **Cyber terrorism**

  There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal.

- **Piracy**

  Far and away the most talked about form of cyber crime is Piracy. Yes, downloading music from peer-to-peer websites is illegal and therefore a form of cyber crime.

1.3.2 Common Types of Cyber Crime Cases Reported World Wide

- **Theft of Telecommunications Services**

  The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code or by using software available on the internet. Some sophisticated

offenders loop between PBX systems to evade detection. Additional forms of service theft include capturing "calling card" details and on-selling calls charged to the calling card account and counterfeiting or illicit reprogramming of stored value telephone cards.

- **Communications in Furtherance of Criminal Conspiracies**

  Just as legitimate organisations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organisations enhanced by technology.

  The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders at the speed of light

- **Telecommunications Piracy**

  Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price or indeed, for free distribution, has proven irresistible to many.

  This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement.

  When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss. This is one of the major cause of concerns for Indian Movie and Music industry.

- **Dissemination of Offensive Materials**

  Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda and instructions for the fabrication of incendiary and explosive devices. Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient.

- **Electronic Money Laundering and Tax Evasion**

  For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Legitimately derived income may also be more easily concealed from taxation authorities. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light. The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed, but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them. Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications.

  With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering and tax evasion may soon be of limited value.

- **Electronic Vandalism, Terrorism and Extortion**

  As never before, western industrial society is dependent upon complex data processing and telecommunications systems. Damage to or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness electronic intruders cause inconvenience at best and have the potential for inflicting massive harm

- **Sales and Investment Fraud**

  As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavours will be that much greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations or bogus investment overtures is increasingly common.

  Some time back investment in Plantation industry was very common in India. Lot of 'Fly by Night' operators came in the market and cheated lot of people.

- **Illegal Interception of Telecommunications**

  Developments in telecommunications provide new opportunities for electronic eavesdropping. From activities as time-honoured as surveillance of an unfaithful spouse, to the newest forms of political and industrial espionage, telecommunications interception has increasing applications.

- **Electronic Funds Transfer Fraud**

  Electronic funds transfer systems have begun to proliferate and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited.

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is spoofing?

.....

.....

.....

.....

.....

.....

.....

.....

1.4 GREY AREA AND INVESTIGATIVE ISSUES

i) Detection of cyber crime needs lot of expertise. In India we don't have adequate number of perosnnel to handle such cases.

ii) Paucity of resources is also a great impediment. To handle such crime we need Cyber Forensic Experts, dedicated computer network and Internet etc. In our country hands of our experts are full.

iii) Now such crime has no national boundry. Most of the Internet Service Providers (ISPs) are having their server outside the country. It becomes very difficult to get required information quickly. Some times even they do not cooperate.

iv) In our country Information Technology Act-2000 daels with such crime. This Act has got its own limitations relating to jurisdiction etc.

v) For successfull prosecution of such cases we need good, specially trained and qualified Prosecutors having domain knowledge.

vi) Special courts and Judges who can appreciate evidence properly are the next necessity.

vii) Electronic data under most jurisdictions is considered as being intangible. The law of some jurisdictions may only permit seizure of tangible material. In such cases, intangible data can only be obtained by seizing the physical medium (e.g. data on diskette or other storage medium) on which the data is stored and found. Proper search and seizure of stored data in a computer and the interception of data that is being communicated from one computer to another or within a computer system is also a grey area.

viii) In some cases, the precise location of electronic data within a computer system may not be apparent. In this situatio we need experts. They are very less in number. During the course of a search the shutting down of, an entire computer system may be extremely intrusive and particularly burdensome to an ongoing business.

ix) Retention period of data is also problomatic in certain cases. Which types of transaction data do telecommunications carriers retain? For how long do the carriers or ISPs retain such data? Are there any laws or regulations which require them to retain such data or to dispose of it after a certain period of time?.

x) Even when one is able to determine the location from which a communication originates, identifying the human source of the communication may prove to be challenging. What legal and/or technological tools are available for this purpose?.

xi) Legal, practical or technical means available to preserve the data seized or intercepted in order to ensure its presentation and admissibility in judicial proceedings are also not adequate.

xii) In case of the data seized are encrypted, again legal, practical and technical problems crop up regarding means available to allow law enforcement to decrypt data and admissibility there of.

xiii) In such cases some times it also very difficult to quantify loss sufferred.

xiv) Reluctance to report such crime is oftenly noticed.

xv) Lack of adequate international cooperation is one of the biggest problem area.

1.5 MAIN FEATURES OF IT ACT 2000

- After enactment in 2000, this act was substantially amended in the year 2008 and efforts were made to plug the loopholes.
- Hacking is the main offence under this act.

- A police officer not below the rank of Dy. S.P. can investigate (Section 78). Such Officer or any other officer authorized by central government is empowered to enter any public place for search and arrest.
- Such officer can arrest without warrant any person found therein, committed, committing or about to commit an offence punishable under this act.

1.6 COMPUTER FRAUDS IN INDIA

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering computer input data in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing or stealing output, usually to conceal unauthorized transactions: this is difficult to detect;
- Altering or deleting stored data;
- Altering or misusing existing system tools or software packages or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion and theft of classified information. A variety of Internet scams target consumers direct.

Some important computer related crimes unearthed in India are as follows:

Medical admission

The first reported computer fraud was in the manipulation of MBBS entrance exam of Delhi University which took place in 1984. In this case, the computer programme was manipulated to alter the marks of the candidate.

Bill Fraud

The NDMC Billing fraud case of 1996 investigated by CBI, is a typical example of a computer fraud which has taken place in India times where huge funds were misappropriated and NDMC cheated.

Railways

Computerized reservation records were allegedly manipulated to favour persons for monetary gains or otherwise. In one case, the booking clerk tampered with the computer entries to generate false closing summary reflecting upper class monthly and quarterly season tickets as second class season tickets and thereby misappropriated the funds.

Indian Airlines

In one case, open ended tickets were issued in fictitious names for shorter sectors and later the computer records were tampered with to show longer sectors and refunds obtained, thereby defrauding the airlines.

MTNL

Computerised records of telephone calls of subscribers allegedly were manipulated to favour subscribers by allowing them to make unrecorded/unbilled ISD calls to Saudi Arabia from Mumbai resulting in loss of revenue to MTNL.

Income Tax

Cases of illegal IT refunds have also been reported.

Stock Market

Cases of manipulating prices have also increased.

DTP Publishing

Counterfeiting of 500 rupee currency notes using DTP (Desk Top Publishing) systems have been reported especially in North-East India. Counterfeiting of Degree Certificate Registration Certificate of vehicles using DTP systems have also been reported.

- **Counterfeiting share certificates**

  In October, 1995, Economic Offences Wing of Crime Branch, Mumbai, seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs.34.47 crores. These were allegedly prepared using DTP systems.

- DTP systems were allegedly used for production nude photographs of celebrities for the purposes of blackmailing. Allegedly, porno sites on the internet were used for downloading offensive pictures.

Banks and Financial Institutions

Several cases of misappropriation of funds by manipulation of computer records have been reported in banks and financial institutions.

Other cases

- Several cases of SOFTWARE PIRACY have been booked by Delhi Police and others on the initiatives taken by NASSCOM, India.
- Cases of hawala transactions and money laundering over the internet have been reported regularly.
- The Purulla Arms Drop Case has revealed how the internet was being used extensively by organised criminals of communication, planning and logistics.
- In case of certain blasts carried out by the terrorists responsibility for the same was claimed through e-mails which were sent by hacking Wi-Fi connectivity of subscribers.
- By the accused persons involved in Mumbai blast VOIP (Voice Over Internet Protocol) facility was also used for communication to conceal their identity and interception.
- Modes of sending mails have been found constantly being improvised by the terrorists to avoid being caught and their plan is disclosed to police and other law enforcing agencies.

1.7 MAJOR AREAS OF COMPUTER CRIME

Major areas of computer crime can be divided into six major areas. Broadly the areas and their related percentages are.

- Trespass, 2%
- Theft of services, 10%
- Manipulation of data, 12%

- Damage to software, 16%
- Theft of information or programs, 16%
- Theft of money, 44%

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Give some example of important computer related crimes in India.

.....

.....

.....

.....

.....

.....

.....

1.8 LET US SUM UP

Due to constant development in the field of technology. Cyber crime is a rapidly growing field and problem area for law enforcing agencies. Broadly speaking Cyber crime and its investigation is like any other conventional case. However, there are certain differences also. Some of them are as under:

- Requires a multi disciplinary approach.
- The legal regime is still in the developing stage.
- Investigating Officer requires to work extra hard to convince the judiciary / prosecution of the authenticity and integrity of evidence.
- Requires quick reaction and sometimes also involves evidence collection abroad.

For investigation of such cases most of the time certain equipments viz. Still and Video cameras, Hand gloves, Permanent markers, Labelling materials, Sealing materials, Packing materials, Stationary and Finger Print Development Kit etc. are required.

This area of investigation also needs services of Cyber Forensics Experts to collect, analyse and present computer based information so that it is suitable for use as evidence in a Court of law. In this area lot of man power is needed. Some of the important aspects to be taken care of are as under:

- Inspection of computer systems and computer networks.
- Making non-functional computer systems operational.
- Examination of Audit trails.
- Hard Disk copying and imaging.
- Backing up data from computer systems at the search site.

Data recovery is another very important area.

- Examination of various storage media for data.
- Recovering erased data from disks.
- Duplicating or converting data files from multi user systems.
- Seized computer evidence recovery.
- Locating hidden files or disguised data.
- Decrypting encrypted data.
- Recovering data from virus infected files.

To prevent such crime and supplement law enforcement agencies we, also need good number of experts to conduct audit of IT system used by various financial institutions.

Now cases of identity theft, source code theft, cases relating to illegal transfer of money by manipulation of net-banking system and similar crimes are on the rise. The other evolving field having lot of potential for crime is Phone banking. Although simultaneous efforts are being made to secure the transactions but ingenious people are there to manipulate system to their benefit. We have to prepare ourselves to tackle theses emerging trends to reap the benefits of technology. Last but not the least prevention is much better which needs well informed public, who may not become prey to the nefarious design of criminals.

1.9 CHECK YOUR PROGRESS: THE KEY

1) Spoofing

IP(Internet Protocol) Spoofing is an attack in the internet Provider where the attacker disguises himself or herself as another user by means of a false IP network address. Whereas Spoofing is the process of disguising one computer user as another.

2) Railways

Computerized reservation records were allegedly manipulated to favour persons for monetary gains or otherwise. In one case, the booking clerk tampered with the computer entries to generate false closing summary reflecting upper class monthly and quarterly season tickets as second class season tickets and thereby misappropriated the funds.

Indian Airlines

In one case, open ended tickets were issued in fictitious names for shorter sectors and later the computer records were tampered with to show longer sectors and refunds obtained, thereby defrauding the airlines.

UNIT 2 BANKING AND FINANCIAL CRIMES

Structure

2.0 INTRODUCTION

In common parlance Banking and Financial crime is also known as White Collar crime and also economic crime. It is called White Collar crime because normally such crime is committed by a person of respectability and high social status, in the course of his occupation. In simple terminology we can say that white-collar crime is an illegal act or series of illegal acts or doing of legal act for achieving an illegal objective committed by any person normally by non-physical and/or non-violent means and by guile, to gain money or property wrongfully or to avoid payment of legal dues or retain money or property wrongfully or to obtain wrongful business of personal advantage.

Economic crime, which in its wide ambit also includes white-collar crimes because of the diverse nature of its component activities, is incapable of simple definition. However, it is for sure that it directly undermines the stability of society albeit in a subtle fashion and can lead to considerable political and social discord.

In Indian perspective Economic offences and public servants are closely interlinked. It is in common knowledge that most economic offences cannot be committed without the active connivance of the Public Servant. During earlier days of strict controls and licences/permits (Quota-Permit Raj) entrepreneur had to look up to the Public Servant in the shape of the Banker, the Insurer, the License-issuing authority and Inspectors of various departments viz- Factories and Boilers, Industries, Customs and Central Excise, Income-tax, Labour and D.R.I. etc. for the multifarious permissions which are required from the State to run his business. The unscrupulous among the entrepreneurs make the unscrupulous among the public servants their partners in crime.

To exemplify the Banking and Financial crime we may list irregularities like forgery of cheques, fraudulent withdrawal of money from financial institutions, fraudulent

credit/loans, filing of false Income-Tax Returns, evasion of Customs Duty, evasion of Excise Duty, evasion of Service Tax, undervaluation of immovable property to evade stamp duty, capital gains tax or municipal taxes, smuggling of Narcotic, antiques etc., showing lesser rental income to evade income-tax, concealing assets to subvert insolvency proceedings etc. Due to huge misappropriation and leakage various welfare activities launched by the Government is not able to bring desired result.

Huge money is involved in such crime. On the one hand this can be imagined from the fact that major terrorist activities world wide are financed by narco-money. On the other hand, its seriousness can be gauged from the fact that effect of even a few white-collar crimes on the economic fabric of society can be far more devastating than all the thefts, burglaries, robberies and dacoities put together. If we consider the infamous Security Scam case of 1992, for example, the net losses of one case would well take care of losses by conventional crimes for scores of years.

With the passage of time new forms of financial crime are emerging. To tackle this menace we need constant and painstaking efforts. As financial crime is very complex and require high level of knowledge lot of practical difficulties are being faced in investigation and prosecution of such cases. Extensive use of computers has further enhanced complexities of such crime. The remedy also lies in the technology. Now lot of information is available on line to promptly detect genuineness of a borrower and his past conduct etc. Long felt requirement of Law Enforcing Agencies have been addressed by enactment and implementation of Prevention of Money Laundering Act (PMLA) -2002. On going project "Aadhar' for providing tamper proof Unique Identity (UID) card having biometric data to all citizens is likely to further reduce menace of financial crime.

2.1 OBJECTIVES

After going through this Unit, you should be able to:

- define banking and financial crime;
- list and explain various characteristics of banking and financial crime;
- list and explain various types of banking and financial crime;
- describe problems of detection of banking and financial crime; and
- explain about various agencies in detection of banking and financial crime.

2.2 CHARACTERISTICS OF BANKING & FINANCIAL CRIME

Banking Crimes

Banking industry in India is very old and time tested. Presently in India we are having banks in different sectors viz. Nationalised Banks, Private sector banks, Co-operative banks an Regional Rural Banks. The main activities of commercial banks are to keep in custody depositors money and lending a part of it to make profit out of it. However, in due course, these functions have been extended and other activities viz. purchase/ discounting of bills, issue of bank guarantee, issue of Letter of Credit (LC), safe custody of valuables (Locker facility) and Portfolio Management etc. have been added. The dependence of commerce upon banking has increased manifold. In a modern money economy, the stoppage of banker's activities, completely paralyses the economic life of a nation.

The primary functions of commercial banks is defined in Sec. 5(b) of the Banking Regulations Act, 1949 as 'banking means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise and withdrawable by cheques, drafts, orders or otherwise. It is governed by Reserve Bank of India which declares bank rates (SLR & CRR) and other guidelines from time to time.

Recently after Sub-prime Crisis faced by the developed western world, Indian banking industry has received international acclaim/recognition. However, iincreasing population and unemployment have made people desperate and education makes such people aware of possibilities of gains through bank frauds which offer the quickest buck possible in no time. After Nationalization of Banks in 1969 activities of banks have changed/increased many fold and it became mass banking.

Banks have evolved detailed systems/procedures/rules, inter alia, taking into account the instructions issued by Reserve Bank of India from time to time on the various areas of their operations. If such rules /norms/procedures, as laid down, are strictly followed, the chances of malpractices can be avoided to great extent.

Main characteristics of Financial Crime are as under:

- Perpetrators of such crime are normally educated, intelligent and often well placed in society.
- They now the system well which they manipulate/intend to manipulate.
- Normally in such cases individual is not the victim rather whole society is at loss/ victim.
- Unlike conventional crime there is no social stigma attached to the offenders.
- Such types of offence are highly technical and complex in nature. Sometimes relate to evolving legislation.
- Most of the time not limited by geographical boundaries. Have got mostly international ramification.

2.3 DIFFERENT TYPES OF BANKING AND FINANCIAL CRIMES

An analysis of the fraud cases reported by banks to the Reserve Bank broadly indicates that frauds perpetrated on banks could be classified into the following types;

i) Misappropriation of cash deposited by the bank's constituents and misappropriation of cash in remittances;

ii) Withdrawals from deposit accounts through forged instruments;

iii) Fraudulent encashment of negotiable instruments (cheque) by opening an account in fake/fictitious name;

iv) Misappropriation through manipulation of books of accounts;

v) Perpetration of frauds through clearing transactions;

vi) Misutilisation/overstepping of lending/discretionary power, non-observance of prescribed norms/procedures in credit dispensation etc.;

vii) Opening/issue of letters of credit, bank guarantees, co-acceptance of bills without proper consideration and;

viii) Frauds in foreign exchange transactions, mainly through non-adherence to Exchange Control Manual Provisions.

From the point of players frauds committed on banks may be classified into following three groups:

a) Frauds committed by persons not directly connected with the banks.

b) Frauds committed by persons connected with the bank and collusion with the bank staff.

c) Frauds committed by the bank staff themselves.

Enormity of fund involved in such crime can be seen from the fact that approximately Rs.39749 Crores was there in the Non Performing Assets (NPA head/bad debt) during the year 2007-2008. Strong KYC (know your customer) norms, meticulous compliance and customer awareness is a must to minimize crime.

Computerisation of banks and introduction of CBS, Netbanking, RTGS, NEFT etc. further made detection of such crime more complex.The Bank frauds involving use of computers are discussed under the heading of computer frauds.

2.3.1 Certain Examples of Banking Frauds/Crimes

a) Banking, Commerce, Chit Fund

Bank frauds are likely to increase with the expansion of the economy. Integration of the economy with the global economy and removal of controls has also integrated the economy with international crime money. Removal of controls has removed opportunities for petty corruption. However, it has eased the commission of Money Laundering. Which needs to be tackled effectively.

b) Fictitious Loan Cases

In few cases certain Bank Officials have been found to have submitted several fictitious applications for loan and withdrew money for himself in an obvious attempt to become rich overnight.

c) Counterfeiting Cases

Circulation of counterfeit currency by anti social elements and also through banking channels is now rampant and posing threat to national security. Enormity of such cases and international ramification has forced government and RBI to address this problem on high priority basis.

d) Crime Committed by Non Banking Financial Institutions (NBFCs)

Initially cases under Import-Export Act (IMPEX Act) were forming major chunk of the cases. Cases relating to other fiscal laws impinging on the revenues of the Central Government, namely, the Essential Commodities Act, Customs Act, Central Excise Act, Income Tax Act, Insurance Act, Narcotic Drugs and Psychotropic Substances Act, Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, Antiquities and Art Treasures Act, besides various sections of the Indian Penal Code (IPC) relating to forgery, cheating, criminal misappropriation and criminal breach of trust, counterfeiting of currency and bank notes and coins and Govt. Stamps etc. also fall under this category.

A brief description of certain varieties of Financial Crime is discussed below to give an idea about the vastness of the subject:

1) Import & Export Frauds

Directorate General of Foreign Trade (DGFT) used to formulate Import-Export policy from time to time. Same are to be followed by every one concerned with

the trade. Import-Export frauds happens to be one of the most prevalent economic crime in earlier days. Long back Imports and Exports (Control) Act, 1947, was enacted to regulate this field. Import-export frauds included, in the past, obtaining of duty free licenses bases on forged and fictitious documents, not fulfilling the export obligations resulting in loss of revenue and misutilization of the imported material. In addition to this smuggling of contraband items was rampant leading to huge revenue loss to the government.

However, with liberalization of economy many items have been put under Open General Licence (OGL). Now on large number of items there is no tax or very minimal tax is there. The number of such cases has declined in the last few years with the rescinding of the IMPEX Act and the various Control orders. Increasingly, these days recourse is taken by unscrupulous operators to the value based advance licensing scheme (VABAL), to under-invoice the imports and over-invoice the exports in money laundering operations, many a time only junk is exported, paid for by the exporter through hawala and duty free import licences are obtained. Certain important categories are as under:

- False claim of Duty Drawback and DEPB (Duty Entitlement Passbook) /Duty Exemption Entitlement Certificate (DECC) etc. have ranged from outright diversion of duty free imported goods to the over-invoicing of export goods to fulfill export obligation and subsequent transfer of duty free licenses into open market.

- Mis-use of EPCG Scheme cases detected indicate outright diversion of duty free imported capital goods and cars and sale of the same in the local market to non-fulfillment of export obligations.

- **Misuse of DEPB Scheme**, Duty drawback scheme etc. has become one of the most favoured routes of money-laundering by black-marketers and those who have unaccounted wealth.

2) Human Trafficking

The offences relating to forgery of travel documents (Passport/visa) etc. are rampant. On the basis of forged documents job-racketeering/ human trafficking is thriving. Passport rackets also have clear security implications as they are required primarily by trans-border criminals, smugglers and drug traffickers. The usual modus-operandi adopted by the criminals in such cases are as under:

a) Photo-substitution on travel/ bank documents etc.

b) Substitution of a page in the Passport. Even forged/fake booklets are in circulation.

c) Fake endorsement of arrival/departure stamps on the Passport etc.

d) Issuance of Passports based on false/suppressed information.

These loopholes can be plugged by introducing features in the passport and visas which would make their forgery difficult e.g. Machine readable passports and visas, distinctive watermark, complicated printing technique, permanent inscription of biographical data, high quality of ink and seals and advance passenger information systems.

3) Insurance Frauds

Broadly Insurance frauds are of two types viz. within the Insurance industry and outside the industry. Under the first category frauds occur with the connivance of Insurance Officials by way of granting insurance cover without charging the premium and until claim is made by party, antedating the 'Cover Note' providing

after-accidental loss insurance cover, allowing inflated claim, not taking over and accounting the salvage and other recoveries to reduce the loss to the company, entertaining a totally fictitious claim etc. Examples of frauds under the second category are endless. Certain major illustrations are as under:

a) Fire in the godown/factory is the best example of insurance frauds. Fires have been known to be set up by respectable persons and businessmen for the purpose of defrauding the insurance company. Some times it is resorted to conceal the pilferage also.

b) Motor cars which are not damaged in an accident or which suffered a minor accident/damage but major repairs in the cars are carried out under cover of damage and the bills passed on to the insurance company.

c) Granting insurance covers after accidents and staging accidents are other methods adopted for committing frauds.

d) Making repeated claims on the basis of same accident.

e) Making claims based on false repair bills/invoices without conducting any repairs or without purchasing parts.

f) Submitting bogus lorry receipts as proof of goods sent and making claim of non-delivery.

g) Getting certain eventualities added after incident. This point can be elaborated from the incident that in a particular dry area no cover from 'flood' was taken by business establishments. However, in the particular year due to unusual heavy rain fall large area got submerged and caused huge loss. After this incident interpolation of 'flood' in many cover notes was reported. This was got done with a malafide intention to obtain false claim.

4) Cases relating to Narcotic Drugs

We all have heard about Heroin, Brown Sugar, Charas and Marijuana etc. Normally drugs are Opium based, Canabis based and also synthetic one. Drug related crime is spread world wide and huge money is involved in this. Lot of Mafia and Terrorists survive on this trade only. Illegal farming of Opium is very common in certain countries. Abuse of drugs is a social problem also. Large numbers of young people are addicted to drugs. They commit further crime to meet their drug requirement. Lot of people visit drug havens to enjoy the same. The legal framework for unearthing drug-trafficking rackets is provided by the NDPS Act and the PIT-NDPS Act.

5) Counterfeit Currency Cases

Counterfeiting rackets and has notched remarkable successes in detecting not only counterfeit Indian Currency but also US Dollars, the Bangladeshi Taka as well as counterfeit stamps, judicial and non-judicial stamp papers, National Savings Certificates and certificates of School Examination Boards.It is noticed that even cases of counterfeiting affect our financial stability also.

6) Art and Antiquity Smuggling Cases

India is a treasure house of cultural heritage. Most of her objects of art and artifacts are priceless but undocumented and are located either in places vulnerable to theft or are owned by individuals as family heirlooms.

Archaeological Survey of India (ASI) is the chief custodian of the cultural wealth of the country. It protects over 5000 individual monuments of national importance, 16 World Heritage Sites including, The Taj Mahal, Ajanta and Ellora, Halebid etc.

The ASI also has 33 museums located at sites of historical and archaeological importance, such as Sanchi, Lothal, Badami and others. Certain important Indian sites have been declared as 'World Heritage' by UNESCO.

Now a days various means are being adopted to smuggle such items out of the country such as by concealment in cargo and diplomatic baggage apart from mis-declaration with respect to their vintage. These antiques of Indian origin are thereafter being sold abroad for substantial profits. This amounts to onslaught against the rich cultural heritage of our country .It has taken up a number of cases relating to the smuggling of priceless antique idols, manuscripts, paintings and artifacts stolen from various museums, temples, monuments and private collections.

Now Antiquities and Art Treasure Act, 1972 is not found adequate to address this problem.

7) Tax & Duty Evasion and Smuggling (Custom Offences)

These fall into two categories:

i) Smuggling offences which involve outright smuggling.

ii) Manipulation of documents.

8) **Hoarding and Black Marketing**

Most common device to cause artificial scarcity of commodities of daily use to earn quick buck.

9) Adulteration of Food, Drugs, Cosmetics etc

These are very common in our country. Adulteration of food items, spices, milk, medicines, sweets even vegetables/ fruits & fertilizer is very common in our country. It is very difficult to find out the fake one. Essential commodities Act, Drugs & Cosmetics Act etc. are their to deal with such menace. Looking to the enormity of such crime now these provisions appear to be inadequate.

10) Stamp Paper Fraud and Postal Frauds

In the recent past we have heard a lot about Stamp paper scam popularly known as 'Telgi Scam'. The stamp paper scam and fraud relating to fraudulent encashment of stolen National Savings Certificates (NSCs) and Kisan Vikas Patra (KVPs) was spread all over the country and run in a organised manner. This fraud caused huge loss to the Govt. Exchequer.

11) Lottery Frauds

Now a days 'Nigerian Lottery Fraud' is very common. In such cases people without participation in any scheme receive mails regarding different lotteries won by them. They are advised to deposit money for processing in some account. Due to greed they do so and fall prey to the designs of scamsters. Another version of this fraud is offer of 'Black Dollars'.

In domestic scenario indulgence of public in excessive purchase of lottery tickets and lottery ticket frauds even resulted in commission of suicide by certain people. Due to its social impact certain State Govt. have stopped such activity in their state.

12) Finger-Print Frauds

In certain cases it has been noticed that finger-print impression of dead persons are taken on documents indicating the will of the deceased. Even this will amount to a forgery as there can be no activity of person after his death. With the help of Forensic expert it is possible in some cases to indicate that the finger-prints have been taken after the death and not while the person was living.

13) Construction Frauds

Buildings, tanks and bridges are constructed according to specifications indicated in the tender. Sometime inferior quality of bricks/stones is used whose strength is apparently less than asked for.

14) Railway Frauds

Used railway tickets over short distances are put to use on the same day again or after several days by changing the dates on the earlier dated tickets. Even instances of counterfeit sale of tickets have also been found in certain sectors.

Fake circular tickets and fake Extra Fare Tickets (EFTs) were common feature. Now with the computerization of ticketing system such incidents have come down. However, certain new dimensions have emerged. Online ticketing frauds have come to fore. Further, by manipulating the system touts used to grab huge number of reserved tickets.

15) Frauds Related To Petrol Pumps/ LPG Stores

- Dispensing less petrol/ diesel by petrol pumps who keep faulty meters.
- Adulteration of Petroleum Products.
- Black marketing of LPG Cylinders.

16) Meter Related Frauds

- Electricity/ water meters are tampered for less reading than actual consumption. Even instances of electricity thefts are very common. Unauthorized connections are also obtained without meters with the connivance of concerned staff.
- Certain taxi/ autorickshaw drivers keep a faulty meter which will read larger amounts (than actual) for collection from the travelers.
- Other weight and measure related offences.

17) Telephone Frauds

Telephone frauds can be very small involving just rupee one or may be very large involving millions of rupees. Certain prevalent instances are as under:

- **Fraud by Diversion of Telecom Lines**

  The diversion of telecom lines is resorted to by unauthorizedly connecting the lines of telephones having STD/ISD into the lines of telephones which are STD/ISD bar or otherwise.

- **Use of Conference-Creating a Parallel Exchange for providing International Trunk Service**

  In a case recently done by CBI, Delhi, it was found that almost a mini exchange was being run from the premises of the fraudster for providing International calls to subscribers by means of conference instrument.

- **Fraud by Meter Tampering**
- **Diverting the Service Telephone Line to some Premises**

18) Wild Life Crime (Flora & Fauna)

Unscrupulous elements are also engaged in smuggling out prohibited items such as sandal wood, red Sandal wood, snake skin etc. apart from shahtoosh wool/ shawls. Intelligence available also suggests organized smuggling of body parts of

endangered species through Indo-Nepal border for the purpose of being smuggled out to China and countries in South-East and East Asia. Certain items specially, rare herbs and micro-organisms which are found only in the upper reaches of the mountains of north-eastern India and the Himalayas which is one of the 12 mega-biodiversity centres in the, world. The smuggled bio-material can be easily replicated abroad thereby affecting the rights of Indian farmers, researches and plant breeders. Legislation to prevent this is reported to be on the anvil.

Enormity of such offences can be assessed from the fact that now 'Tigers' are on the verge of extinction. To protect them lot of money is being spent by the Government under 'Project Tiger'.

19) Arms and Ammunition

To mint easy money lot of people are indulging in trade relating to supply of illegal arms and ammunition. These weapons are subsequently used for conventional crime and also as an aid to economic crime.

20) Intellectual Property and Related Crime

Intellectual Property infringement is a Crime only in the case of trademark & copyright infringement. In respect of Designs & Patents there is provision of Civil Remedy only. Infringement of Copyright has further posed new challenges to enforcement as thrown up by digital age. Film Industry, Music Industry and traditional Book Publishing Industry are facing lot of loss and problems.

Enforcement personnel need to become technically and technologically aware and the law enforcement authorities must be geared to meet challenges. In the absence of effective enforcement, IPR will cease to be rights.

The Patents Act 1970, The Indian Designs Act 2000, The Copyright Act 1957, The Trade and Merchandise Marks Act 1958 and Geographical Indications Act 1999 etc. enacted by govt. apparently need drastic changes.

21) Money Laundering

This is the biggest threat international community is facing right now. This provides finance to criminals. Even after detection of crime it is very difficult to control criminal activity unless supply of money is stopped. If we seriously consider a co-ordinated strategy to combat white-collar economic crime we have to take into account the various facets of money laundering which is nothing but profitable investments of proceeds from crime. The scope is vast keeping in view the enormous potentials of money inflow both from narcotic trafficking as well as from other white-collar crime. To begin with, we may define this as a process by which assets, primarily cash assets, which derived from illegal activities are manipulated so as to make them look as if they were derived from legitimate sources. It would not be exaggeration in saying that perhaps prevalence of successful money laundering is the back-bone and sustaining force of all white-collar crimes.

Many a technique for money laundering are adopted by white-collar criminals some of which can find special mention. viz. currency smuggling, use of front or shell companies, fictitious cash business, private/surreptitious banking systems, use of inflated invoicing etc. The ingenuity of white-collar criminal can only be thwarted by a co-ordinated effort by all the enforcement agencies police set ups, strict Bank customer identification system, international harmonization of money transfer clause, uncomplicated procedures for blocking and freezing of foreign accounts, uniform regime of infusing transparency in transactions and loosening of Bank secrecy norms and last but not the least enhanced and better co-operation/ co- ordination in investigation of asset-related matters both nationally and internationally.

22) Electronic Frauds/Computer Frauds (Cyber Crime)

We are presently living in Computer Era. Now every aspect (banking, travel, communication etc.) is affected by computer system. With the development of technological resources, extensive use of computers in day to day life, particularly electronic data processing used in the business world, a new type of fraud has arisen i.e. Computer Fraud. Though computer came into India around 1960, cases involving computer frauds have started appearing on the scene in last decade. It is time that we start working against computer frauds right now before it is too late.

To defraud the public, therefore, all the criminal has to do is to alter the instructions given to a computer. This is a relatively easy matter for computer programmers whose job is to feed instruction to the computer. Now a days computer frauds are fairly widespread. For new generation white-collar criminal the computer is thus an ideal tool which not only accepts everything they feed into it, but also forgets everything that is deleted.

Law enforcement has had its own problems in dealing with the complexity of computer criminality. The complexity of computer crime is based on two major differences, it has vis-a-vis the ordinary crime. First, that the criminal does not have to be at the scene of crime to commit the act. The second is the computer crimes have no boundary limitations.

Now in India serious efforts are being made to curb this menace. Information Technology Act was enacted in the year 2000 and was amended recently. Cyber Crime Cells have been opened by the Police organizations. However, we still need adequate resources, Cyber Forensic Experts and training to deal with this problem.

23) Trafficking in Human Organs

This is latest and fast emerging crime scene. Normally poor and hapless people are targeted by scamsters for removal of their body parts which is transplanted to rich patients after charging huge money. Lot of money is involved in this trade. This needs to be adequately addressed to safeguard poor people from becoming source of spare parts for rich and wealthy people. To address this problem, in India Transplantation of Human Organs Act was enacted in the year 1994. However, this needs lot of changes.

24) Fraud Relating to Capital Market

Crime relating to stock market are now very common and cause huge loss. In India this type of crime came in prominence after securities scam of 1992 popularly known as 'Harshad Mehta Scam'. Main modus operandi adopted are as under:

- Fictitious applications submitted for cornering Retail Individual Investor (RII) category in respect of allotment of shares by companies through Initial Public Offers (IPO). Multiple D-mat accounts are also used for this purpose.
- Allotted shares purchased by forging Delivery Instruction Slips (DIS) in off market deals.
- After listing in stock exchanges, shares sold at premium.
    - Rigging of Share price.
    - Insider trading.
    - Placement of over priced shares with public sector undertakings etc.

After formation of SEBI now such types of cases are under constant watch. Now trading in derivatives and 'Future and option' are evolving phenomenon.

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Give main characteristics of financial crime.

.....

.....

.....

.....

.....

2.4 SOME CATEGORIES OF FORGED DOCUMENTS

To commit economic offence relevant documents need to be created, forged and fabricated. Some of the important documents as under:

i) Bank documents – Demand drafts, cheques etc.

ii) Licences, permits, orders issued by Government or other statutory authorities.

iii) Invoices, bills, receipts etc.

iv) Educational certificates.

v) Birth certificates.

vi) Passports – Generally photo is changed. Full passport may also be forged.

2.5 PROBLEMS OF DETECTION OF WHITE-COLLAR CRIMES AT POLICE LEVEL

The white-collar crime has always presented enormous problems to the investigators in all the aspects of the investigation and a brief reference to these problems would be in order. Some broader issues which include the question of priority in the application of limited police resources.

i) The first difficulty in white-collar crime investigation arises often from the absence of a complainant. In a number of frauds cases the investigation is commenced following a complaint made to the police by a victim, potential victim or other organization which has reason to suspect fraudulent activity. However, in a large number of white-collar/economic crimes there may be no readily identifiable loser and the loss may be evenly distributed in the community. The task of identifying losers in such cases can be very taxing and time-consuming particularly when they are spread throughout the country or even overseas. The first task of the Investigating Officer, therefore, is to trace the complainant and trace the exact dimensions of the crime committed which is extremely arduous. In recent past we have seen 'Satyam Computers' case which gave a big jolt to even our auditing system also.

ii) The second difficulty in investigation relates to reporting of white-collar/ economic crime. Some times reporting of such crimes gives an adverse publicity which can have disastrous effect on commercial reputation, share values, economic viability, of a company or even a Government.

iii) The other aspect relating to difficulty in investigation is the question of specialized knowledge, training and experience. It is necessary to stress that because highly diverse areas of commercial activity upon which mostly white-collar crime investigations are centered to speak of general specialization in white-collar crime is somewhat misleading.

iv) The difficulty which relates to accessibility of Bank accounts of suspect persons and secrecy thereof is great. Multi - national and private Banks or banks abroad are often found to be extremely jealous of their customer's right to secrecy and this leads to a great deal of hindrance in investigation.

v) Economic Laws in India are enforced by separate departments. The role of the police in this regard, except in respect of the CBI and the Economic Offences Wings created in certain States is, therefore, very limited. In fact, almost all the economic offences so declared created by the special status are non-cognizable, that is the police cannot investigate such cases without the permission of the Magistrate.

vi) Another distinguishing feature of most of the economic offences is that for prosecuting the accused, complaints have to be filed by the designated authorities. The police cannot file charge-sheets. Notable exceptions are property offences under the IPC, offences of bribery and corruption and trafficking in narcotics.

vii) Difficulty in obtaining documents from foreign countries and the testimony of the person who has to prove the document necessitates recourse to the time-consuming process of issuing of Letters Rogatory (LR) and awaiting their replies.

viii) Since most economic offenders extremely rich and powerful, the legal loopholes are fully exploited and sometimes, even investigation is stayed by the Superior Courts for many years.

ix) There is also reluctance in private sector to report such crimes to enforcement agencies because in the opinion of some, private firms fear a worse loss because of business disruption by law enforcement investigators than by criminals.

x) Lack of specialized Courts in many States, shortage of prosecutors and technical officers.

2.6 CHALLENGES DUE TO RECENT ECONOMIC LIBERALISATION

The economy has witnessed epochal reforms over the past few years in the sphere of industrial policy. We have seen bureaucratic controls being either totally dismantled or substantially reduced. Far-reaching changes have taken place in trade and exchange-rate policies, foreign investment policy, tax structure, financial sector and the public sector. The processes of deregulation and de-bureaucratization have reduced areas of choice and, to that extent, the scope for corruption in enforcement of laws. Now import licensing is virtually abolished, import duties have been substantially lowered and gold and silver imports have been liberalized. The rupee is now partially convertible and this has resulted in a reduction of the premium on foreign exchange in the hawala market also.

The Foreign Investment policy has simplified the procedure for obtaining foreign investment approvals and streamlined the procedure for Indian private investment abroad and a number of constraints under the FERA have been removed. With more liberal provisions FEMA has been brought in. Similarly, tax reforms have resulted in reduction of the maximum marginal rate of Income tax, abolition of

wealth tax on productive assets, the concept of presumptive taxation for small businesses, reduction of customs duties and, albeit to a slightly lesser degree, excise duties. The financial sector - banking system and the capital market and the public sector also have witnessed liberalization to a great extent. In the coming years the pace of the reforms is likely to further increase. Regulatory Authorities (SEBI, TRAI, IRDA and PFRDA etc.) are now taking over the control earlier exercised by the government.

In the financial sector, unless responsive and fraud-resistant trading mechanisms are formulated, such as those contemplated for National Stock Exchange, another security scam cannot be ruled out. In other words, economic offences will exists in all these areas as long as vestiges of control remains and decision making processes lack transparency.

It is widely suspected that some of the foreign exchange coming into the country as foreign direct investment is, in fact, black money generated through import and export frauds or crimes, converted into clandestine foreign exchange and routed back into the country through investment and banking channels in clear cut money laundering operation. Similarly most of the legal gold and silver import into the country is also being widely done by conversion of black money into hard currency through hawala channels.

The integration of our economy with the global economy has also integrated it with global crime and 'hot' money from international narco-racketeering, illegal arms sales and funding of terrorist outfits gets laundered through various 'shell' companies over several countries, thereby, seriously endangering our sovereignty and integrity as a nation. Therefore, the need for monitoring imports and exports and foreign exchange inflows is perhaps much more than ever in the past and the only way in which integration with the world economy and the increasing threat of international crime can be reconciled is by enacting a potent Money Laundering Act.

Last but not the least the greatest problem is that of the "Front Man" probably one of the most worrying aspects of white-collar crime investigation is that even when investigator has detected the persons responsible for perpetration of the majority of criminal acts, he has no idea of the identity of the individual who formulated the fraud, supervised it from a distance and then slipped away to dodge the police. The man who is put as 'The Front Man' is mostly a poor/illiterate man prepared to accept responsibility for the operation and to be punished for it which in any case are not very stringent. The king-pin always eludes the dragnet of the police.

2.7 ENFORCEMENT AGENCIES

Mainly following agencies are involved in detection of Banking and Financial crime in India.

i) Local Police – In view of rapid increase in economic crime some of the states separate Economic Offences Wing/ Cyber crime wing have been created.

ii) Reserve Bank of India (RBI) – Regular inspection of Banks is carried out by RBI. Certain big cases came out during such inspections.

iii) Central Bureau of Investigation (CBI) – Looking the importance of this aspect since long cases of Banking and Financial crime are investigated by CBI. After registration of Bank Security Scam cases in the CBI in June, 1992, a full fledged Economic Offences Division was created. Under this division 'Banking Securities & Fraud Cell' was established, which is specifically meant for investigation and prosecution of Bank Scam Cases, along with other major financial frauds committed on Nationalized Banks throughout the country.

iv) Department of Company Affairs.

v) Serious Fraud Investigation Office (SFIO).

vi) Income Tax Department.

vii) Customs Department.

viii) Enforcement Directorate (ED).

ix) Department of Revenue Intelligence (DRI) and

x) National Investigative Agency (NIA).

2.8 RELEVANT LEGISLATION TO DISCOURAGE AND CURB THE MENACE

To deprive persons of the proceeds and benefits derived from the commission of economic offence including confiscation and forfeiture of such property including parked abroad some of the provisions as given below may prove to be useful.

i) Section 105 of IPC.

ii) Prevention of Money Laundering Act, 2002.

iii) Narcotic Drugs & Psychotropic Substances Act, 1985.

iv) Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976.

v) Foreign Exchange Management Act, etc.

vi) Maharashtra Organised Crime Control Act – In respect of 'Telgi Scam', this act was invoked to adequately address the problem and punish the guilty expeditiously.

2.9 TECHNICAL SUPPORT

To deal with this menace in effective manner many steps have been taken. Now following facilities are available to render assistance in the detection.

- Central Forensic Science Laboratory (CFSL) and State Forensic Science Laboratories (FSL) and Government Examiner of Questioned Documents (GEQD):

  Importance of documents cannot be overstressed. We have the first important document bearing date of birth which is very important and cases involving age forgeries are very common. The last document is the death certificate which is equally important. Forgeries are mostly committed through documents whether it is a will, driving license, import license; foreign exchange clearance or transfer vouchers agreement, cheque, receipt, account book, ledger books, insurance papers, registration papers, pay-in-slips or passport, degrees, tickets of airlines or railways, fraudulent TA/DA or medical bills. Now a days specialized technical Forensic Science Laboratories are equipped very well and provided adequate facilities to render immediate assistance in the early detection of frauds. For examination of documents to detect alteration/addition/ obliteration services of these Laboratories and Government Examiner of Questioned Documents (GEQD) have been made available.

In addition to above services of following experts are also available for assistance.

- Finger-Prints Experts;
- Building materials (where use of less cement is alleged or inferior material below specification is used);
- Voices (where speakers tried to disguise their voice);
- Chemical frauds (where adulteration in petrol/oils has been suspected);
- Computer frauds (Cyber Forensic Experts) - This branch is emerging and needs lot of experts in coming days.
- Information System Auditors.
- Chartered Accountants.
- Experts of Security Printing Press and the Bank Note Press.
- Financial Action Task Force (FATF).*
- INTERPOL*

(* For international cooperation)

2.10 GREY AREAS

Delay in investigation or prosecution is biggest grey area of white-collar crime. The investigations because of technicalities involved, requirements of scientific examination of documents, miscellaneous preoccupation gets delayed.

Secondly, in cases of white-collar offences, it is often seen that even when laws are available many of the enforcement agencies suffer from lethargy and feel that the well-placed white-collar criminal would retaliate against their actions.

In India, a majority of economic crimes sentences imposed by courts are very mild, even a case involving violation of import laws to the tune of hundreds of millions of rupees, the sentence could be imprisonment for few days or fines as little as Rs. 50,000/- . The irony of the fact is that against this, a poor thief who steals Rs. 100/- would be sent to a jail most certainly for at least 6 months.

Further absence of expertise to investigate such technical crime and adequate infrastructure are great impediments in curbing this menace.

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What agencies are involved in detection of Banking and Financial crime in India?

.....

.....

.....

.....

.....

.....

2.11 LET US SUM UP

It is always true that 'prevention is better than cure'. To minimize this menace, awareness of common man is a must. To achieve this objective many advertisements / campaigns through Audio- Visual media have been launched by the government. In this regard steps have been taken by SEBI, Banks and Consumer Forums also.

We cannot expect to reap full benefits of liberalization of economy if we do not ensure white-collar criminals being dealt with sternly and severely. The strengthening of enforcement agencies such as CBI, DRI, the Directorate of enforcement etc. is also a sine qua non. The close coordination among these agencies is also essential if a dent is to be made on the emerging white-collar economic criminality. In respect of counterfeit currency also educative advertisements are issued by the RBI from time to time.

To minimize the instances of forgery travel documents and other valuable documents should be printed with the highest level security features e.g. machine readability, distinctive water mark, high quality seals, more than one printing technique, intaglio printing, on internationally accepted lines.

Corporate frauds have assumed serious dimensions and are posing threats to the health of organizations whether in the industrial sector, services sector or any other sector. The menace of fraud is serious problem which is continuously growing number-wise, variety-wise and extent of losses wise. This needs to be curbed by enacting provisions in the Corporate Law.

The longstanding desirability of a separate and comprehensive legislation on money laundering has been addressed by enacting Prevention of Money Laundering Act (PMLA), which has been notified in the year 2005. Provision of highly sophisticated and modern infrastructure for monitoring of inter-country commercial transactions, high-tech interception devices for electronic transfers, faster mobility and better training and orientation in computerized banking and accounting procedures adopted internationally has to be adopted in our country also.

The menace of money laundering has attracted international attention and one organization 'FATF' has been created. India is also in the process of joining this organization to reap the benefits of international cooperation.

Now INTERPOL also renders assistance to member countries in cases of serious nature having international ramification. In India CBI is the Nodal Agency for such cooperation.

2.12 CHECK YOUR PROGRESS: THE KEY

1) Main characteristics of Financial Crime are as under

- Perpetrators of such crime are normally educated, intelligent and often well placed in society.
- They now the system weii which they manipulate/ intend to manipulate.
- Normally in such cases individual is not the victim rather whole society is at loss/ victim.
- Unlike conventional crime there is no social stigma attached to the offenders.
- Such types of offence are highly technical and complex in nature. Sometimes relate to evolving legislation.

- Most of the time not limited by geographical boundaries. Have got mostly international ramification.

2) **Mainly following agencies are involved in detection of Banking and Financial crime in India.**

- Local Police – In view of rapid increase in economic crime some of the states separate Economic Offences Wing/ Cyber crime wing have been created.
- Reserve Bank of India (RBI) – Regular inspection of Banks is carried out by RBI. Certain big cases came out during such inspections.
- Central Bureau of Investigation (CBI) – Looking the importance of this aspect since long cases of Banking and Financial crime are investigated by CBI. After registration of Bank Security Scam cases in the CBI in June, 1992, a full fledged Economic Offences Division was created. Under this division 'Banking Securities & Fraud Cell' was established, which is specifically meant for investigation and prosecution of Bank Scam Cases, along with other major financial frauds committed on Nationalized Banks throughout the country.
- Department of Company Affairs.
- Serious Fraud Investigation Office (SFIO).
- Income Tax Department
- Customs Department.
- Enforcement Directorate (ED).
- Department of Revenue Intelligence (DRI) and
- National Investigative Agency (NIA).

UNIT 3 IDENTIFY THEFTS AND DATA THEFTS/SOURCE CODE THEFTS

Structure

3.0 INTRODUCTION

Identity Theft

Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Organizations and individuals who are duped or defrauded by the identity thief can also suffer adverse consequences and losses and to that extent are also victims.

The term identity theft was coined in 1964 and is actually a misnomer, since it is not literally possible to steal an identity as such – more accurate terms would be identity fraud or impersonation or identity cloning but identity theft has become common place.

Data theft

Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras. Since employees often spend a considerable amount of time developing contacts and confidential and copyrighted information for the company they work for they often

feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company or misuse it while they are still in employment.

While most organizations have implemented firewalls and intrusion-detection systems very few take into account the threat from the average employee that copies proprietary data for personal gain or use by another company. A common scenario is where a sales person makes a copy of the contact database for use in their next job. Typically this is a clear violation of their terms of employment.

The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. Removable media devices are getting smaller with increased hard drive capacity and activities such as podslurping are becoming more and more common. It is now possible to store more than 160 GB of data on a device that will fit in an employee's pocket, data that could contribute to the downfall of a business.

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- define identity theft and data theft;
- list and explain various types of identity thefts and data thefts;
- list and explain various techniques for obtaining and exploiting personal information for identity theft; and
- describe source code theft and the law.

3.2 TOPOLOGY

3.2.1 Types of Identity Thefts

- Identity cloning and concealment
- Criminal identity theft
- Synthetic identity theft
- Medical identity theft
- Business/commercial identity theft (using another's business name to obtain credit)
- Criminal identity theft (posing as another person when apprehended for a crime)
- Financial identity theft (using another's identity to obtain credit, goods and services)
- Identity cloning (using another's information to assume his or her identity in daily life)
- Medical identity theft (using another's identity to obtain medical care or drugs)

Identity theft may be used to facilitate or fund other crimes including illegal immigration, terrorism and espionage. There are cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

Identity thieves occasionally impersonate others for non-financial reasons-for instance, to receive praise or attention for the victim's achievements.

3.2.1.1 Identity Cloning and Concealment

In this situation, the identity thief impersonates someone else in order to conceal their own true identity. Examples might be illegal immigrants, people hiding from creditors or other individuals or those who simply want to become "anonymous" for personal reasons. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life.

3.2.1.2 Criminal Identity Theft

When a criminal fraudulently identifies himself to police as another individual at the point of arrest, it is sometimes referred to as "Criminal Identity Theft." In some cases criminals have previously obtained state-issued identity documents using credentials stolen from others or have simply presented fake ID. Provided the subterfuge works, charges may be placed under the victim's name, letting the criminal off the hook. Victims might only learn of such incidents by chance, for example by receiving court summons, discovering their drivers licenses are suspended when stopped for minor traffic violations or through background checks performed for employment purposes.

It can be difficult for the victim of a criminal identity theft to clear their record. The steps required to clear the victim's incorrect criminal record depend on what jurisdiction the crime occurred in and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers and prove their own identity by some reliable means such as fingerprinting or DNA fingerprinting and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. Authorities might permanently maintain the victim's name as an alias for the criminal's true identity in their criminal records databases. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it is possible that a future background check will return the incorrect criminal records. This is just one example of the kinds of impact that may continue to affect the victims of identity theft for some months or even years after the crime, aside from the psychological trauma that being 'cloned' typically engenders.

3.2.1.3 Synthetic Identity Theft

A variation of identity theft which has recently become more common is synthetic identity theft, in which identities are completely or partially fabricated. The most common technique involves combining a real social security number with a name and birthdate other than the ones associated with the number. Synthetic identity theft is more difficult to track as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit bureau or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Individual victims can be affected if their names become confused with the synthetic identities or if negative information in their subfiles impacts their credit ratings.

3.2.1.4 Medical Identity Theft

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity-such as insurance information-without the person's knowledge or consent to obtain medical services or goods or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, which may in turn lead to inappropriate and potentially life-threatening decisions by medical staff.

3.3 TECHNIQUES FOR OBTAINING AND EXPLOITING PERSONAL INFORMATION FOR IDENTITY THEFT

Identity thieves typically obtain and exploit personally identifiable information about individuals or various credentials they use to authenticate themselves, in order to impersonate them. Examples include:

- Rummaging through rubbish for personal information (dumpster diving)
- Retrieving personal data from redundant IT equipment and storage media including PCs, servers, PDAs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold on without having been properly sanitized.
- Using public records about individual citizens, published in official registers such as electoral rolls.
- Stealing bank or credit cards, identification cards, passports, authentication tokens typically by pickpocketing, housebreaking or mail theft.
- Skimming information from bank or credit cards using compromised or hand-held card readers and creating clone cards.
- Using 'contactless' credit card readers to acquire data wirelessly from RFID-enabled passports.
- Observing users typing their login credentials, credit/calling card numbers etc. into IT equipment located in public places (shoulder surfing).
- Stealing personal information from computers using malware, particularly Trojan horse keylogging programs or other forms of spyware.
- Hacking computer networks, systems and databases to obtain personal data, often in large quantities.
- Exploiting breaches that result in the publication or more limited disclosure of personal information such as names, addresses, Social Security number or credit card numbers.
- Advertising bogus job offers in order to accumulate resumes and applications typically disclosing applicants' names, home and e-mail addresses, telephone numbers and sometimes their banking details.
- Exploiting insider access and abusing the rights of privileged IT users to access personal data on their employers' systems.
- Infiltrating organizations that store and process large amounts or particularly valuable personal information
- Impersonating trusted organizations in e-mails, SMS text messages, phone calls or other forms of communication in order to dupe victims into disclosing their personal information or login credentials, typically on a fake corporate website or data collection form (phishing)
- Brute-force attacking weak passwords and using inspired guesswork to compromise weak password reset questions
- Obtaining castings of fingers for falsifying fingerprint identification ... or famously using gummy bears to fool low quality fingerprint scanners[12]
- Browsing social networking websites for personal details published by users,

often using this information to appear more credible in subsequent social engineering activities

- Diverting victims' e-mail or post in order to obtain personal information and credentials such as credit cards, billing and bank/credit card statements or to delay the discovery of new accounts and credit agreements opened by the identity thieves in the victims' names
- Using false pretenses to trick individuals, customer service representatives and help desk workers into disclosing personal information and login details or changing user passwords/access rights (pretexting)
- Stealing checks to acquire banking information, including account numbers and bank routing numbers
- Guessing Social Security numbers by using information found on Internet social networks such as Facebook and MySpace.

3.4 METHODS TO PROTECT ONESELF FROM IDENTITY THEFT

Methods to protect oneself from identity theft

The acquisition of personal identifiers is made possible through serious breaches of privacy. For consumers, this is usually a result of them naively providing their personal information or login credentials to the identity thieves as a result of being duped but identity-related documents such as credit cards, bank statements, utility bills, checkbooks etc. may also be physically stolen from vehicles, homes and offices or directly from victims by pickpockets and bag snatchers. Guardianship of personal identifiers by consumers is the most common intervention strategy recommended by the US Federal Trade Commission, Canadian Phone Busters and most sites that address identity theft. Such organizations offer recommendations on how individuals can prevent their information falling into the wrong hands. Identity theft can be partially mitigated by not identifying oneself unnecessarily (a form of information security control known as risk avoidance). This implies that organizations, IT systems and procedures should not demand excessive amounts of personal information or credentials for identification and authentication. Requiring, storing and processing personal identifiers {such as Social Security number, national identification number, drivers license number, credit card number, etc.) increases the risks of identity theft unless this valuable personal information is adequately secured at all times.

To protect themselves against electronic identity theft by phishing, hacking or malware, individual are well advised to maintain computer security, for example by keeping their operating systems fully patched against known security vulnerabilities, running antivirus software and being cautious in their use of IT.

Identity thieves sometimes impersonate dead people, using personal information obtained from death notices, gravestones and other sources to exploit delays between the death and the closure of the person's accounts, the inattentiveness of grieving families and weaknesses in the processes for credit-checking. Such crimes may continue for some time until the deceased's families or the authorities notice and react to anomalies. In recent years, commercial identity theft protection/insurance services have become available in many countries. These services purport to help protect the individual from identity theft or help detect that identity theft has occurred in exchange for a monthly or annual membership fee or premium.The services typically work either by setting fraud alerts on the individual's credit files with the three major credit bureaus or by setting up credit report monitoring with

the credit bureaux. While identity theft protection/insurance services have been heavily marketed, their value has been called into question.

3.5 PROBLEM AREA

3.5.1 Identity Protection by Organizations

In their May 1998 testimony before the United States Senate, the Federal Trade Commission (FTC) discussed the sale of Social Security numbers and other personal identifiers by credit-raters and data miners. The FTC agreed to the industry's self-regulating principles restricting access to information on credit reports. According to the industry, the restrictions vary according to the category of customer. Credit reporting agencies gather and disclose personal and credit information to a wide business client base.

Poor stewardship of personal data by organizations, resulting in unauthorized access to sensitive data, can expose individuals to the risk of identity theft. The Privacy Rights Clearinghouse has documented over 900 individual data breaches by US companies and government agencies since January 2005, which together have involved over 200 million total records containing sensitive personal information, many containing social security numbers. Poor corporate diligence standards which can result in data breaches include:

- failure to shred confidential information before throwing it into dumpsters.
- failure to ensure adequate network security.
- the theft of laptop computers or portable media being carried off-site containing vast amounts of personal information. The use of strong encryption on these devices can reduce the chance of data being misused should a criminal obtain them.
- the brokerage of personal information to other businesses without ensuring that the purchaser maintains adequate security controls.
- Failure of governments, when registering sole proprietorships, partnerships and corporations, to determine if the officers listed in the Articles of Incorporation are who they say they are. This potentially allows criminals access to personal information through credit-rating and data mining services.

The failure of corporate or government organizations to protect consumer privacy, client confidentiality and political privacy has been criticized for facilitating the acquisition of personal identifiers by criminals.

Using various types of biometric information, such as fingerprints, for identification and authentication has been cited as a way to thwart identity thieves, however there are technological limitations and privacy concerns associated with these methods as well.

3.5.2 Regional Legal Responses

Australia

In Australia, each state has enacted laws that dealt with different aspects of identity or fraud issues. Some States have now amended relevant criminal laws to reflect crimes of identity theft, such as the Criminal Law Consolidation Act 1935 (SA), Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 and also in Queensland under the Criminal Code 1899 (QLD). Other States and Territories are in states of development in respect of regulatory frameworks relating to identity theft such as Western Australia in respect of Criminal Code Amendment (Identity Crime) Bill 2009.

On the Commonwealth level, under the *Criminal Code Amendment (Theft, Fraud, Bribery & Related Offences) Act 2000* which amended certain provisions within the *Criminal Code Act 1995*,

> " **135.1 General dishonesty**
>
> (3) A person is guilty of an offence if: a) the person does anything with the intention of dishonestly **causing a loss to another person**; and b) the other person is a Commonwealth entity. Penalty: **Imprisonment for 5 years.**"

Likewise, each state has enacted their own privacy laws to prevent misuse of personal information and data. The Commonwealth *Privacy Act* is applicable only to Commonwealth and territory agencies and to certain private sector bodies (where for example they deal with sensitive records, such as medical records or they have more than $3 million turnover PA).

Canada

Under section 402.2 of the *Criminal Code of Canada*,

> "Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
>
> is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or is guilty of an offence punishable on summary conviction."

Under section 403 of the *Criminal Code of Canada*,

> " (1) Everyone commits an offence who fraudulently personates another person, living or dead,
>
> (a) with intent to gain advantage for themselves or another person; (b) with intent to obtain any property or an interest in any property; (c) with intent to cause disadvantage to the person being personated or another person; or (d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice. is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or guilty of an offence punishable on summary conviction."

In Canada, *Privacy Act* (federal legislation) covers only federal government, agencies and crown corporations. Each province and territory has its own privacy law and privacy commissioners to limit the storage and use of personal data. For the private sector, the purpose of the Personal Information Protection and Electronic Documents Act (2000, c. 5) (known as PIPEDA) is to establish rules to govern the collection, use and disclosure of personal information; except for the provinces of Quebec, Ontario, Alberta and British Columbia were provincial laws have been deemed substantially similar.

France

In France, a person convicted of identity theft can be sentenced up to five years in prison and fined up to £75,000.

Hong Kong

Under HK Laws. Chap 210 *Theft Ordinance*, sec. 16A Fraud

" (1) If any person by any deceit (whether or not the deceit is the sole or main inducement) and with **intent to defraud** induces another person to commit an act or make an omission, which results either–

(a) in **benefit to any person** other than the second-mentioned person; or (b) in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person, the first-mentioned person commits the offense of fraud and is liable on conviction upon indictment to **imprisonment for 14 years.** "

Under the *Personal Data (Privacy) Ordinance*, it established the post of Privacy Commissioner for Personal Data and mandate how much personal information one can collect, retain and destruction. This legislation also provides citizens the right to request information held by businesses and government to the extent provided by this law.

India

Under the Information Technology Act 2000 Chapter IX Sec 43 (b)

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

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

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

Sweden

Sweden have had relatively little problems with identity theft. This is because only Swedish identity documents have been accepted for identity verification. Stolen documents are traceable by banks and some other institutions. The banks have the duty to check the identity of people withdrawing money or getting loans. If a bank gives money to someone using an identity document reported as stolen, the bank must take the loss. From 2008 any EU passport are valid in Sweden for identity check and Swedish passports are valid all over the EU. This makes it harder to detect stolen documents, but still banks in Sweden must ensure that stolen documents are not accepted.

Other types of identity theft than over the bank desk have become more common in Sweden. One common example is ordering a credit card to someone who has an unlocked letterbox and is not home on daytime. The thief steals the letter with the credit card and then the letter with the code which typically arrives a few days later. Usage of a stolen credit card is hard in Sweden, since an identity document or a PIN code it is normally demanded. If the shop does not demand that, it must take the loss from stolen credit cards. The method of observing someone using the credit card PIN code, stealing the card or skimming it and then use the card, has become more common.

Legally, Sweden is an open society. The Principle of Public Access says that all information kept by public authorities must be available for anyone except in certain cases. Specificially anyone's address, income, taxes etc. are available to anyone. This makes fraud easier (the address is protected for certain people needing it).

To impersonate someone else and gain money from it is a kind of fraud, which is described in the Criminal Code (Swedish:Brottsbalken).

United Kingdom

In the United Kingdom personal data is protected by the Data Protection Act 1998.

The Act covers all personal data which an organization may hold, including names, birthday and anniversary dates, addresses, telephone numbers, etc.

Under English law (which extends to Wales but not necessarily to Northern Ireland or Scotland), the deception offences under the Theft Act 1968 increasingly contend with identity theft situations. In *R v Seward* (2005) EWCA Crim 1941, the defendant was acting as the "front man" in the use of stolen credit cards and other documents to obtain goods. He obtained goods to the value of £10,000 for others who are unlikely ever to be identified. The Court of Appeal considered sentencing policy for deception offenses involving "identity theft" and concluded that a prison sentence was required. Henriques J. said at para 14:"Identity fraud is a particularly pernicious and prevalent form of dishonesty calling for, in our judgment, deterrent sentences."

Increasingly, organizations, including Government bodies will be forced to take steps to better protect their users' data.

United States

The increase in crimes of identity theft lead to the drafting of the Identity Theft and Assumption Deterrence Act. In 1998, The Federal Trade Commission appeared before the United States Senate. The FTC discussed crimes which exploit consumer credit to commit loan fraud, mortgage fraud, lines-of-credit fraud, credit card fraud, commodities and services frauds. The Identity Theft Deterrence Act (2003)[ITADA] amended U.S. Code Title 18, § 1028 ("Fraud related to activity in connection with identification documents, authentication features and information"). The statute now makes the possession of any "means of identification" to "knowingly transfer, possess or use without lawful authority" a federal crime, alongside unlawful possession of identification documents. However, for federal jurisdiction to prosecute, the crime must include an "identification document" that either: (a) is purportedly issued by the United States, (b) is used or intended to defraud the United States, (c) is sent through the mail or (d) is used in a manner that affects interstate or foreign commerce. See 18 U.S.C. § 1028(c). Punishment can be up to 5, 15, 20 or 30 years in federal prison, plus fines, depending on the underlying crime per 18 U.S.C. § 1028(b). In addition, punishments for the unlawful use of a "means of identification" were strengthened in § 1028A ("Aggravated Identity Theft"), allowing for a consecutive sentence under specific enumerated felony violations as defined in § 1028A(c)(1) through (11).

The Act also provides the Federal Trade Commission with authority to track the number of incidents and the dollar value of losses. Their figures relate mainly to consumer financial crimes and not the broader range of all identification-based crimes.

If charges are brought by state or local law enforcement agencies, different penalties apply depending on the state.

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Give some techniques for obtaining and exploiting personal information for identity theft.

.....

.....

.....

.....

.....

.....

3.6 TYPES OF DATA THEFTS

- **Thumbsucking**

  Thumbsucking, similar to podslurping, is the intentional or unintentional use of a portable USB mass storage device, such as a USB flash drive (or "thumbdrive"), to illicitly download confidential data from a network endpoint.

  The moniker is derived from the act of downloading or "sucking", data from a network endpoint onto a USB flash drive or similar storage device.

  A USB flash drive was allegedly used to remove without authorization highly classified documents about the design of U.S. nuclearweapons from a vault at Los Alamos.

  The threat of thumbsucking has been amplified for a number of reasons, including the following:

  - The storage capacity of portable USB storage devices has increased.
  - The cost of high-capacity portable USB storage devices has decreased.
  - Networks have grown more dispersed, the number of remote network access points has increased and methods of network connection have expanded, increasing the number of vectors for network infiltration.

- **Carder**

  A Person who is engaged in online credit card fraud.

- **Hacker**

  Person gaining illicit uses to approach any other system.

- **Pod slurping**

  The use of iPods etc. to download information illegally.

- **Bluesnafing**

  Use of bluetooth devices to approach and stole information.

3.7 SOURCE CODE THEFT AND THE LAW

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies.

As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations that get original software developed for their use.

Scenario 1

The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

Modus Operandi

If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then contact potential buyers to make the sale.

Usual motives

Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the Information Technology Act and section 63 of Copyright Act	Sections 43, 65, 66 & 66B of the Information Technology Act and section 63 of Copyright Act

Scenario 2

The suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software.

Modus Operandi

If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code.

He would then modify the source code (either himself or in association with other programmers) and launch his own software.

Usual motives

Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the Information Technology Act and section 63 of Copyright Act	Sections 43, 65, 66 & 66B of the Information Technology Act and section 63 of Copyright Act

Section 65 of the Information Technology Act is titled "Tampering with computer source documents" and is the most important legal provisions relating to source code theft in India.

3.8 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 programme, 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 both.

Explanation. – For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Comments

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application). Let us understand this using some illustrations.

Illustration: Ms X has created a simple computer program. When a user double-clicks on the hello.exe file created by Ms X, the following small screen opens up:

Hello World

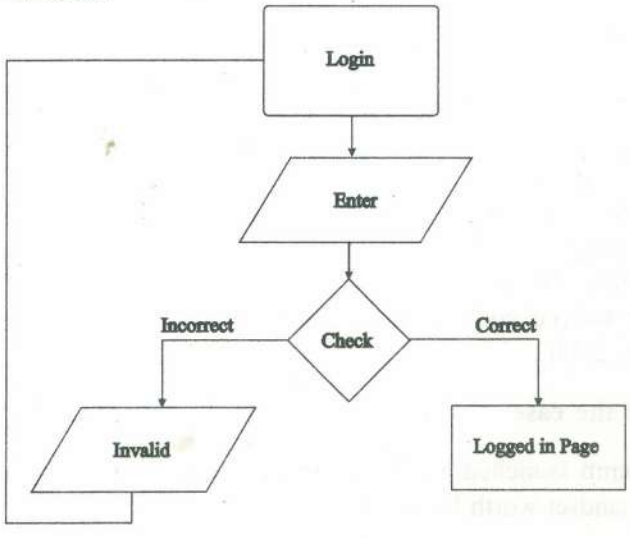
The hello.exe file created by Ms X is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Ms X. Ms X has created the executable file using the programming language called "C". Using this programming language, she created the following lines of code:

```
main()
{  printf("Hello, ");
printf("World");
}
```

These lines of code are referred to as the source code.

Illustration: Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration: Ms X is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either: (1) required to be kept (e.g. in a cell phone, hard disk, server etc) or (2) required to be maintained by law.

The following acts are prohibited in respect of the source code (1) knowingly concealing or destroying or altering (2) intentionally concealing or destroying or altering (3) knowingly causing another to conceal or destroy or alter (4) intentionally causing another to conceal or destroy or alter. Let us discuss the relevant terms and issues in detail.

Conceal simply means "to hide".

Illustration: Ms X has created a software program. The source code files of the program are contained in a folder on Ms X's laptop. Mr X changes the properties of the folder and makes it a "hidden" folder. Although the source code folder still exists on Ms X's computer, she can no longer see it. Mr X has concealed the source code.

Destroy means "to make useless", "cause to cease to exist", "nullify", "to demolish" or "reduce to nothing".

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Illustration: Ms X has created a software program. The source code files of the program are contained in a folder on Ms X's laptop. Mr X deletes the folder. He has destroyed the source code.

Illustration: Ms X has created a software program. The source code files of the program are contained in a folder on Ms X's laptop. Mr X deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

Illustration: Ms X is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Mr X tears up the paper on which she had drawn the flowchart. Mr X has destroyed the source code.

Alters, in relation to source code, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc.

Illustration: Ms X has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Mr X changes the file from HTML to text format. He has altered the source code.

Case Law

Syed Asifuddin and Ors. vs. The State of Andhra Pradesh & Anr. [2005CriLJ4314]

Summary of the case

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm. The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Background of the case

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with

an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically "unlocked" so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this "unlocking" by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Teleservices Limited officials for re-programming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defence

1) Subscribers always had an option to change from one service provider to another.

2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4) A telephone handset is neither a computer nor a computer system containing a computer programme.

5) There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Findings of the Court

1) As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2) The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4) When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Conclusions of the Court

1) A cell phone is a computer as envisaged under the Information Technology Act.

2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases

- "when the computer source code is required to be kept"
- "maintained by law for the time being in force".

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is Data theft?

.....

.....

.....

.....

.....

.....

.....

3.9 LET US SUM UP

This unit covers various types of Identity theft and Data theft and various techniques for obtaining and exploiting personal information for identity theft. Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras.

3.10 CHECK YOUR PROGRESS: THE KEY

1) Techniques for obtaining and exploiting personal information for identity theft are as under

- Retrieving personal data from redundant IT equipment and storage media including PCs, servers, PDAs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold on without having been properly sanitized.
- Using public records about individual citizens, published in official registers such as electoral rolls.
- Stealing bank or credit cards, identification cards, passports, authentication tokens ... typically by pickpocketing, housebreaking or mail theft.

- Skimming information from bank or credit cards using compromised or hand-held card readers and creating clone cards.
- Using 'contactless' credit card readers to acquire data wirelessly from RFID-enabled passports.
- Observing users typing their login credentials, credit/calling card numbers etc. into IT equipment located in public places (shoulder surfing).
- Stealing personal information from computers using malware, particularly Trojan horse keylogging programs or other forms of spyware.
- Hacking computer networks, systems and databases to obtain personal data, often in large quantities.

2) Data theft

Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras. Since employees often spend a considerable amount of time developing contacts and confidential and copyrighted information for the company they work for they often feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company or misuse it while they are still in employment.

While most organizations have implemented firewalls and intrusion-detection systems very few take into account the threat from the average employee that copies proprietary data for personal gain or use by another company. A common scenario is where a sales person makes a copy of the contact database for use in their next job. Typically this is a clear violation of their terms of employment.

UNIT 4 SPAM AND BOTNETS

Structure

4.0 INTRODUCTION

Spam

Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television http://en.wikipedia.org/wiki/Advertising and file sharing network spam.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions.

Botnets

In malware or malicious software, a **botnet** is a collection of infected computers or bots that have been taken over by hackers (also known as bot herders) and are used to perform malicious tasks or functions. A computer becomes a bot when it downloads a file (e.g. an e-mail attachment) that has bot software embedded in it. A botnet is considered a botnet if it is taking action on the client itself via IRC channels (Internet Relay Channel) without the hackers having to log in to the

client's computer. A botnet consists of many threats contained in one. A typical botnet consists of a bot server (usually an IRC server) and one or more botclients.

An **Internet Relay Channel** is a form of internet text messaging or synchronous conferencing.It is mainly designed for group communication in discussion forums called channels. It also allows one to one communication via private messaging as well as chat and data transfer including file transfer.

Malware, short for **malicious software**, consists of programming (code, scripts, active content and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code.

4.1 OBJECTIVES

After going through this Unit, you should be able to:

- define spam and botnets;
- list and explain various types of spam and botnets;
- describe various suggestions for curbing *Nigerian letter fraud* cases; and
- describe various steps of investigating *Nigerian letter fraud* cases.

4.2 TYPES OF SPAM

E-mail Spam

E-mail spam also known as unsolicited bulk E-mail (UBE), junk mail or unsolicited commercial e-mail (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Spam in e-mail started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years and today composes some 80 to 85% of all the e-mail in the world, by a "conservative estimate". Pressure to make e-mail spam illegal has been successful in some jurisdictions, but less so in others. Spammers take advantage of this fact and frequently outsource parts of their operations to countries where spamming will not get them into legal trouble.

Increasingly, e-mail spam today is sent via "zombie networks", networks of virus- or worm-infected personal computers in homes and offices around the globe; many modern worms install a backdoor which allows the spammer access to the computer and use it for malicious purposes. This complicates attemptsto control the spread of spam, as in many cases the spam doesn't even originate from the spammer. In November 2008 an ISP, McColo, which was providing service to botnet operators, was depeered and spam dropped 50%-75% Internet-wide. At the same time, it is becoming clear that malware authors, spammers and phishers are learning from each other and possibly forming various kinds of partnerships.

An industry of e-mail address harvesting is dedicated to collecting e-mail addresses and selling compiled databases. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site Quechup.

Instant Messaging Spam

Instant Messaging Spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002. As instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging system such as Skype.

Newsgroup Spam

Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet onvention defines spamming as excessive multiple posting,that is, the repeated posting of a message (or substantially similar messages). The prevalence of Usenet spam led to the development of the Breidbart Index as an objective measure of a message's "spamminess".

Forum Spam

Forum spam is the creating of messages that are advertisements or otherwise unwanted on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity if a sale goes through, when the spammer behind the spambot works on commission.

Mobile Phone Spam

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS.

Many online games allow players to contact each other via player-to-player messaging, chat rooms or public discussion areas. What qualifies as spam varies from game to game, but usually this term applies to all forms of message flooding, violating the terms of service contract for the website. This is particularly common in MMORPGs where the spammers are trying to sell game-related "items" for real-world money, chiefly among these items is in-game currency. This kind of spamming is also called Real World Trading (RWT). In the popular MMORPG Runescape, it is common for spammers to advertise sites that sell gold in multiple methods of spam. They send spam via the in-game private messaging system, via using emotes to gain attention and by yelling publicly to everyone in the area.

Video sharing sites, such as YouTube, are now being frequently targeted by spammers. The most common technique involves people (or spambots) posting links to sites, most likely pornographic or dealing with online dating, on the comments section of random videos or people's profiles. Another frequently used technique is using bots to post messages on random users' profiles to a spam account's channel page, along with enticing text and images, usually of a sexually suggestive nature. These pages may include their own or other users' videos, again often suggestive. The main purpose of these accounts is to draw people to their link in the home page section of their profile. YouTube has blocked the posting of such links. In addition, YouTube has implemented a CAPTCHA system that makes rapid posting of repeated comments much more difficult than before, because of abuse in the past by mass-spammers who would flood people's profiles with thousands of repetitive comments.

Yet another kind is actual video spam, giving the uploaded movie a name and description with a popular figure or event which is likely to draw attention or within the video has a certain image timed to come up as the video's thumbnail image to mislead the viewer. The actual content of the video ends up being totally unrelated, a Rickroll, sometimes offensive or just features on-screen text of a link to the site being promoted. Others may upload videos presented in an infomercial-like format selling their product which feature actors and paid testimonials, though the promoted product or service is of dubious quality and would likely not pass the scrutiny of a standards and practices department at a television station or cable network.

E-mail and other forms of spamming have been used for purposes other than advertisements. Many early Usenet spams were religious or political. Serdar Argic, for instance, spammed Usenet with historical revisionist screeds. A number of evangelists have spammed Usenet and e-mail media with preaching messages. A growing number of criminals are also using spam to perpetrate various sorts of fraud and in some cases have used it to lure people to locations where they have been kidnapped, held for ransom and even murdered.

4.3 COST BENEFIT ANALYSIS

The European Union's Internal Market Commission estimated in 2001 that "junk e-mail" cost Internet users •10 billion per year worldwide. The California legislature found that spam cost United States organizations alone more than $13 billion in 2007, including lost productivity and the additional equipment, software and manpower needed to combat the problem. Spam's direct effects include the consumption of computer and network resources and the cost in human time and attention of dismissing unwanted messages.

In addition, spam has costs stemming from the kinds of spam messages sent, from the ways spammers send them and from the arms race between spammers and those who try to stop or control spam. In addition, there are the opportunity cost of those who forgo the use of spam-afflicted systems. There are the direct costs, as well as the indirect costs borne by the victims-both those related to the spamming itself and to other crimes that usually accompany it, such as financial theft, identity theft, data and intellectual property theft, virus and other malware infection, child pornography, fraud and deceptive marketing.

The cost to providers of search engines is not insignificant: "The secondary consequence of spamming is that search engine indexes are inundated with useless pages, increasing the cost of each processed query". The methods of spammers are likewise costly. Because spamming contravenes the vast majority of ISPs' acceptable-use policies, most spammers have for many years gone to some trouble to conceal the origins of their spam. E-mail, Usenet and instant-message spam are often sent through insecure proxy servers belonging to unwilling third parties. Spammers frequently use false names, addresses, phone numbers and other contact information to set up "disposable" accounts at various Internet service providers. In some cases, they have used falsified or stolen credit card numbers to pay for these accounts. This allows them to quickly move from one account to the next as each one is discovered and shut down by the host ISPs.

The costs of spam also include the collateral costs of the struggle between spammers and the administrators and users of the media threatened by spamming. Many users are bothered by spam because it impinges upon the amount of time they spend reading their e-mail. Many also find the content of spam frequently offensive, in that pornography is one of the most frequently advertised products. Spammers send their spam largely indiscriminately, so pornographic ads may show up in a work place e-mail inbox-or a child's, the latter of which is illegal in many

jurisdictions. Recently, there has been a noticeable increase in spam advertising websites that contain child pornography.

Some spammers argue that most of these costs could potentially be alleviated by having spammers reimburse ISPs and persons for their material. There are three problems with this logic: first, the rate of reimbursement they could credibly budget is not nearly high enough to pay the direct costs, second, the human cost (lost mail, lost time and lost opportunities) is basically unrecoverable and third, spammers often use stolen bank accounts and credit cards to finance their operations and would conceivably do so to pay off any fines imposed.

Some spammers argue that most of these costs could potentially be alleviated by having spammers reimburse ISPs and persons for their material. There are three problems with this logic: first, the rate of reimbursement they could credibly budget is not nearly high enough to pay the direct costs, second, the human cost (lost mail, lost time and lost opportunities) is basically unrecoverable and third, spammers often use stolen bank accounts and credit cards to finance their operations and would conceivably do so to pay off any fines imposed.

Some companies and groups "rank" spammers; spammers who make the news are sometimes referred to by these rankings. The secretive nature of spamming operations makes it difficult to determine how proliferated an individual spammer is, thus making the spammer hard to track, block or avoid. Also, spammers may target different networks to different extents, depending on how successful they are at attacking the target. Thus considerable resources are employed to actually measure the amount of spam generated by a single person or group. For example, victims that use common anti-spam hardware, software or services provide opportunities for such tracking. Nevertheless, such rankings should be taken with a grain of salt.

In all cases listed above, including both commercial and non-commercial, "spam happens" because of a positive Cost-benefit analysis result if the cost to recipients is excluded as an externality the spammer can avoid paying.

Cost is the combination of

- **Overhead:** The costs and overhead of electronic spamming include bandwidth, developing or acquiring an e-mail/wiki/blog spam tool, taking over or acquiring a host/zombie etc.
- **Transaction cost:** The incremental cost of contacting each additional recipient once a method of spamming is constructed, multiplied by the number of recipients. (see CAPTCHA as a method of increasing transaction costs)
- **Risks:** Chance and severity of legal and/or public reactions, including damages and punitive damages
- **Damage:** Impact on the community and/or communication channels being spammed
- **Benefit** is the total expected profit from spam, which may include any combination of the commercial and non-commercial reasons listed above. It is normally linear, based on the incremental benefit of reaching each additional spam recipient, combined with the conversion rate. The conversion rate for botnet-generated spam has recently been measured to be around one in 12,000,000 for pharmaceutical spam and one in 200,000 for infection sites as used by the Storm botnet.http://en.wikipedia.org/wiki/Spam_(electronic) - cite_note-33 They specifically say in the paper "After 26 days and almost 350 million e-mail messages, only 28 sales resulted".

- Spam is prevalent on the Internet because the transaction cost of electronic communications is radically less than any alternate form of communication, far outweighing the current potential losses, as seen by the amount of spam currently in existence. Spam continues to spread to new forms of electronic communication as the gain (number of potential recipients) increases to levels where the cost/benefit becomes positive. Spam has most recently evolved to include wikispam and blogspam as the levels of readership increase to levels where the overhead is no longer the dominating factor. According to the above analysis, spam levels will continue to increase until the cost/benefit analysis is balanced.

4.4 USES OF SPAM

Spam can be used to spread computer viruses, trojan horses or other malicious software. The objective may be identity theft or worse (e.g. advance fee fraud). Some spam attempts to capitalize on human greed whilst other attempts to use the victims' inexperience with computer technology to trick them (e.g. phishing). On May 31, 2007, one of the world's most prolific spammers, Robert Alan Soloway, was arrested by U.S. authorities. Described as one of the top ten spammers in the world, Soloway was charged with 35 criminal counts, including mail fraud, wire fraud, e-mail fraud, aggravated identity theft and money laundering. Prosecutors allege that Soloway used millions of "zombie" computers to distribute spam during 2003. This is the first case in which U.S. prosecutors used identity theft laws to prosecute a spammer for taking over someone else's Internet domain name. A zombie computer/system is a virus infected computer./system

Check Your Progress 1

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Explain some types of Spam.

.....

.....

.....

.....

.....

.....

.....

4.5 BACKGROUND OF BOTNETS

Like many things on the Internet today, bots began as a useful tool without malicious overtones. Bots were originally developed as a virtual individual that could sit on an **IRC channel** and do things for its owner while the owner was busy elsewhere. Soon after the release of the first IRC bot, a few worms had exploited vulnerabilities in **IRC clients** and used the bots to steal passwords, log keystrokes and hide their identity. The main drivers for botnets are for recognition and financial gain. The larger the botnet, the more 'kudos' the herder can claim to have among the underground community. The bot herder/hacker will also 'rent out' the services of the botnet to third parties, usually for sending out spam messages or for performing

a denial of service attack against a remote target. Due to the large numbers of compromised machines within the botnet, huge volumes of traffic (either e-mail or denial of service) can be generated. However, in recent times, the volume of spam originating from a single compromised host has dropped in order to thwart anti-spam detection algorithms – a larger number of compromised hosts send a smaller number of messages in order to evade detection by anti-spam techniques.

Botnets have become a significant part of the Internet, albeit increasingly hidden. Due to most conventional IRC networks taking measures and blocking access to previously-hosted botnets, controllers must now find their own servers. Often, a botnet will include a variety of connections and network types. Sometimes a controller will hide an IRC server installation on an educational or corporate site where high-speed connections can support a large number of other bots. Exploitation of this method of using a bot to host other bots has proliferated only recently.

4.6 TYPES OF BOTNETS

Several botnets have been found and removed from the Internet. The Dutch police found a 1.5 million node botnet and the Norwegian ISP Telenor disbanded a 10,000-node botnet. In July 2010, the FBI arrested a 23-year old Slovenian held responsible for the malicious software that integrated an estimated 12 million computers into a botnet. Large coordinated international efforts to shut down botnets have also been initiated. It has been estimated that up to one quarter of all personal computers connected to the internet may be part of a botnet. Conficker is one of the largest botnets out there that has infected an estimated 1 million to 10 million machines which attempts to sell fake antivirus to its victims.

While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities.

While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (called zombie computers) running software, usually installed via drive-by downloads exploiting web browser vulnerabilities, worms, Trojan horses or backdoors, under a common command-and-control infrastructure.

A botnet's originator (aka "bot herder" or "bot master") can control the group remotely, usually through a means such as IRC and usually for nefarious purposes. Individual programs manifest as IRC "bots". Often the command-and-control takes place via an IRC server or a specific channel on a public IRC network. This server is known as the command-and-control server ("C&C"). Though rare, more experienced botnet operators program their own commanding protocols from scratch. The constituents of these protocols include a server program, client program for operation and the program that embeds itself on the victim's machine (bot). All three of these usually communicate with each other over a network using a unique encryption scheme for stealth and protection against detection or intrusion into the botnet network.

A bot typically runs hidden and uses a covert channel to communicate with its C&C server. Generally, the perpetrator of the botnet has compromised a series of systems using various tools. Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community. The process of stealing computing resources as a result of a system being joined to a "botnet" is sometimes referred to as "scrumping."

Botnet servers will often liaise with other botnet servers, such that a group may contain 20 or more individual cracked high-speed connected machines as servers, linked together for purposes of greater redundancy. Actual botnet communities usually consist of one or several controllers that rarely have highly-developed command hierarchies between themselves; they rely on individual friend-to-friend relationships.

The architecture of botnets has evolved over time and not all botnets exhibit the same topology for command and control. Depending upon the topology implemented by the botnet, it may make it more resilient to shutdown, enumeration or command and control location discovery. However, some of these topologies limit the saleability and rental potential of the botnet to other third-party operators. Typical botnet topologies are:

- Star
- Multi-server
- Hierarchical
- Random

4.7 FORMATION AND EXPLOITATION OF BOTNETS

- To thwart detection, some botnets were scaling back in size. As of 2006, the average size of a network was estimated at 20,000 computers, although larger networks continued to operate.
- This example illustrates how a botnet is created and used to send ***e-mail spam.***
- A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application-the bot.
- The bot on the infected PC logs into a particular C&C server (often an IRC server, but in some cases a web server).
- A spammer purchases the services of the botnet from the operator.
- The spammer provides the spam messages to the operator, who instructs the compromised machines via the IRC server, causing them to send out spam messages.
- Botnets are exploited for various purposes, including ***denial-of-service attacks,*** creation or misuse of ***SMTP mail relays*** for spam, ***click fraud,*** spamdexing and the theft of application serial numbers, login IDs and financial information such as credit card numbers.
- The botnet controller community features a constant and continuous struggle over who has the most bots, the highest overall bandwidth and the most "high-quality" infected machines, like university, corporate and even government machines.

4.8 TYPES OF ATTACKS

- Denial-of-service attacks where multiple systems autonomously access a single Internet system or service in a way that appears legitimate, but much more frequently than normal use and cause the system to become busy.
- Adware exists to advertise some commercial entity actively and without the user's permission or awareness, for example by replacing banner ads on web pages with those of another content provider.

- Spyware is software which sends information to its creators about a user's activities – typically passwords, credit card numbers and other information that can be sold on the black market. Compromised machines that are located within a corporate network can be worth more to the bot herder, as they can often gain access to confidential information held within that company. There have been several targeted attacks on large corporations with the aim of stealing sensitive information, one such example is the Aurora botnet.
- E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying or malicious in nature.
- Click fraud is the user's computer visiting websites without the user's awareness to create false web traffic for the purpose of personal or commercial gain.
- Access number replacements are where the botnet operator replaces the access numbers of a group of dial-up bots to that of a victim's phone number. Given enough bots partake in this attack, the victim is consistently bombarded with phone calls attempting to connect to the internet. Having very little to defend against this attack, most are forced into changing their phone numbers (land line, cell phone etc.).
- Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

4.9 PREVENTIVE MEASURES FOR BOTNETS

- If a machine receives a denial-of-service attack from a botnet, few choices exist. Given the general geographic dispersal of botnets, it becomes difficult to identify a pattern of offending machines and the sheer volume of IP addresses does not lend itself to the filtering of individual cases. Passive OS fingerprinting can identify attacks originating from a botnet: network administrators can configure newer firewall equipment to take action on a botnet attack by using information obtained from passive OS fingerprinting. The most serious preventive measures utilize rate-based intrusion prevention systems implemented with specialized hardware. A network based intrusion detection system (NIDS) will be an effective approach when detecting any activities approaching botnet attacks. NIDS monitors a network, it sees protected hosts in terms of the external interfaces to the rest of the network, rather than as a single system and get most of its results by network packet analysis.
- Some botnets use free DNS hosting services such as DynDns.org, No-IP.com and Afraid.org to point a subdomain towards an IRC server that will harbor the bots. While these free DNS services do not themselves host attacks, they provide reference points (often hard-coded into the botnet executable). Removing such services can cripple an entire botnet. Recently, these companies have undertaken efforts to purge their domains of these subdomains. The botnet community refers to such efforts as "nullrouting", because the DNS hosting services usually re-direct the offending subdomains to an inaccessible IP address. Similarly, some botnets implement custom versions of well-known protocols. The implementation differences can be used for fingerprint-based detection of botnets.
- For example, Mega-D features a slightly modified SMTP protocol implementation for testing the spam capability. Bringing down the Mega-D's SMTP server disables the entire pool of bots that rely upon the same SMTP server.
- The botnet server structure mentioned above has inherent vulnerabilities and

problems. For example, if one was to find one server with one botnet channel, often all other servers, as well as other bots themselves, will be revealed. If a botnet server structure lacks redundancy, the disconnection of one server will cause the entire botnet to collapse, at least until the controller(s) decides on a new hosting space. However, more recent IRC server software includes features to mask other connected servers and bots, so that a discovery of one channel will not lead to disruption of the botnet.

- Several security companies such as Afferent Security Labs, Symantec, Trend Micro, FireEye, Umbra Data and Damballa have announced offerings to stop botnets. While some, like Norton AntiBot (discontinued), are aimed at consumers, most are aimed to protect enterprises and/or ISPs. The host-based techniques use heuristics to try to identify bot behavior that has bypassed conventional anti-virus software. Network-based approaches tend to use the techniques described above; shutting down C&C servers, nullrouting DNS entries or completely shutting down IRC servers.

- Newer botnets are almost entirely P2P, with command-and-control embedded into the botnet itself. By being dynamically updateable and variable they can evade having any single point of failure. Commanders can be identified solely through secure keys and all data except the binary itself can be encrypted. For example a spyware program may encrypt all suspected passwords with a public key hard coded or distributed into the bot software. Only with the private key, which only the commander has, can the data that the bot has captured be read.

- Newer botnets have even been capable of detecting and reacting to attempts to figure out how they work. A large botnet that can detect that it is being studied can even DDoS those studying it off the internet.

- There is an effort by researchers at Sandia National Laboratories to analyze the behavior of these botnets by simultaneously running one million Linux kernels as virtual machines on a 4,480-node Dell high-performance computer cluster.

Check Your Progress 2

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Give some types of attack.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.10 NIGERIAN LETTER FRAUD CASES : A CASE STUDY

The *Nigerian Letter Frauds* are basically done by playing on the greed of the people. The following type of Nigerian frauds cases are usually prevalent.

1) Lottery Fraud

2) Black Dollar Scam

3) Online Job Fraud

4) Phishing and other similar offences

4.10.1 The Modus Operandi Adopted in Such Frauds

The Modus operandi adopted by the accused persons in such cases is that the accused persons sent alluring mails to various people regarding winning of huge amount of money in lottery or offering a lucrative job overseas or to transfer huge amount received in inheritance or to supply U.S. dollars in huge quantity. These mails are sent from abroad i.e. Nigeria, U.K, U.S.A etc. It is directed to the recipient of the mail to sent their personal particulars to claim the winning amount. The people who respond to the mail expecting the winning amount are asked to pay some amount in the name of courier charges. As soon as the victim become ready to pay an amount, he is contacted by a foreigner who pretends himself as a diplomat of the lottery agency and who is responsible for delivery of the winning amount. The amount of courier charges is asked to be deposited in some Indian account. Once this amount is deposited by the victim he is asked to deposit some more amount on various fake pretexts such as Anti Terrorist Certificate charges, Custom Charges, Non Resident Certificate Charges, Conversion of currency charges, etc. Once the victim coughs up these amounts, he is further enticed and allured to deposit the amount further demanded and he pays in the fear of losing the earlier amount deposited by him. This demand of the accused persons goes on, till either the victim himself realizes or comes to know from other sources, that he has been cheated. The fraudsters sometimes even use name of Government authorities like RBI, CBI and Customs etc. to show credibility. The amounts in these matters vary from few thousands to tens of lakhs. All of these amounts are asked to be deposited in various Indian accounts. During the period of communication with the victim, a number of 'diplomats' contacts the victim for various works, the numbers of which keep increasing and changing. These persons are responsible for providing the victim, the account details and for alluring/ pressurizing the victim to deposit the asked amount in these accounts. These persons use Indian mobile numbers for contacting the victim. All these numbers are managed using fake name or IDs or sometimes procured on someone else's (Indian) IDs.

There are some more foreigners involved, who are responsible for managing the account details. Some accounts are procured by these foreigners through their Indian friends and some are provided by the Indian groups who are working for them on commission basis. This group of Indian persons manages the accounts from their various contacts on fake pretexts. This group is also responsible for withdrawing the money from accounts so provided and the money is handed over to the fraudsters. Normally, an account is used for 10 to 15 days and after that all the documents of the account are destroyed. People of these groups too use the phone connections on fake IDs/Names.

Normally, the group of foreigners which contacts the victim does not contact the people of Indian group responsible for managing the account and the group of foreigners which collects the account/money from their Indian supporters doesn't

contact the victim. The foreigners of both the groups, however, keep in touch with each other and that too using phone connections managed on fake IDs.

As both the groups of these foreigners use different names and use phone numbers managed on fake IDs, it is difficult to prove their identity and to trace them during investigation.

The other safe-guard used by the fraudsters in such crimes is that they normally do not use bank account located in the state of residence of the victim because of which the state police is hesitant to act on the complaint.

In one of typical investigation scenario of such a fraud, the CBI came across 90 to 100 mobile phone numbers of accused persons, middlemen, accountholders etc. almost all of which were found to be procured using fake IDs. There were 20 to 30 middlemen who were providing/procuring accounts from the account holders. A total of as many as 20-30 accounts were used having transactions amounting to lakhs of rupees.

4.10.2 Suggestions for Curbing this Menace

1) Conducting educational programs by the banks and local police.

2) KYC (Know Your Customer) norms are not being fully looked into by the banks. For verification of the customer either the banks are outsourcing the persons or this work is being given to low paid employees who either for a meager favour or because of their less knowledge become instrumental for opening the accounts which are later used by thefraudsters.

3) In some cases it has seen that Nigerians are getting Indian visa using forged documents. The concerned embassies should be more conscious/thorough and take more checks while permitting VISA.

4) These fraudsters communicate with the victim through mobile phones procured using fake ID documents. Mobile service provider can be asked to be more cautious before issuing new connections.

4.10.3 Investigation of Nigerian Fraud Cases

Investigation of Nigerian Fraud Cases involves three steps:

1) Obtaining the details of IP addresses from which the e-mails are originated

As per experience the initial mails are normally generated from abroad. However, after few mails from abroad the fraudsters send mails from India also. Through IP (Internet Protocol) addresses of such mails, we can reach to the source of the mail which generally turns out to be a Cyber Café in India. Sometimes, these mails are found to be initiated from proxy/spoofed IP addresses because of which actual originator of mails is not identified.

CERT IN (Computer Emergency Response Team) can be contacted for assistance on this subjects.

2) Following the money trails from victim to suspect through account holder and the middleman of the chain

These cheaters use Indian bank accounts to siphon off the cheated amount. Hence, they can also be traced through the account holders. Mostly gullible/ unsuspecting persons let their accounts be used for petty gains. However, it is seen that normally these cheaters themselves do not come in the direct contact of the account holders and collect the account through some middlemen/friends. Middlemen are petty criminals who arrange these bank accounts for master minds.

3) Mobile numbers of the suspect and call detail analysis.

The cheaters also use mobile phones to communicate with the victim. Sometimes these numbers pertain to overseas service providers. However, most of the time these are local numbers. We can also trace these cheaters through such phone connections which they have used. Minute call detail analysis of the phone numbers of suspects or middlemen may give substantial leads in the investigation. It has been seen in some cases that the fraudsters use phone connections procured/managed on fake IDs making it difficult to trace these fraudsters.

In the *Nigerian Letter Fraud* Cases, it is seen that the victim receives number of alluring mails because of which victim come in the trap of these cheaters. First step in the investigation of such cases is to find out the origin of these mails. The initial mails are normally, generated from abroad, however, after few mails from abroad the fraudsters sent mails from India also. Through IP addresses of such mails, we can reach to the source of the mail. Secondly, the cheaters used mobile phones to communicate with the victim. Sometimes theses numbers pertains to overseas service providers however, in most of the time these are Indian Phone. We can also trace these cheaters through the phone connection they have used. It has seen in last few cases that the fraudsters use phone connection procure/manage on the fake ID because of which it is difficult to trace these fraudsters through phone connection. However, few mistake done by these fraudsters such as using mobile handsets used for fraud, in their genuine phone numbers leads the investigation to the cheaters.

These cheaters used Indian account to siphon off the cheated amount. Hence, they can also be traced through the account holders. However, it is seen that normally these cheaters themselves not come in the direct contact of the account holders and collects the account through some middlemen/friends.

It is also experienced that Nigerians use their nick names while introducing themselves to the victim as well as, to the middlemen. Identifying and tracing them with the nickname is just impossible. However, it is seen that these persons keep some fake identity card of colleges or of embassy in the nickname they are using. Recovery of such identity cards from them is becomes good evidence. Some times these identity cards of having nickname of the accused is also found used to procure some relevant mobile connection.

In almost all the cases dealt by Cyber Crime Cell of CBI, it is seen that the Nigerian Nationals arrested found over staying in India without valid travel document like Passport/Visa. Foreigners Act. can be invoked in such cases.

It is also seen that these persons procure Visa from Indian Embassies, using forged business invitations, shown issued by any Indian institute/firm. If there is reason to believe that a Nigerian has managed Visa on fake grounds, Indian Embassy issuing the Visa, can be contacted through Ministry of External Affairs to find out the truth and if the grounds/documents found fake a complaint can be made to concerned embassy for action against the person.

Immediate reporting/registration/action in such cases is the key of success.

Check Your Progress 3

Notes: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

Explain three steps of investigating Nigerian fraud cases.

.....

.....

.....

.....

.....

.....

4.11 LET US SUM UP

This unit covers various types of spam and botnets. Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs wiki spam, online classified ads spam, mobile phone messaging spam Internet forum spam, junk fax transmissions, social networking spam, television http://en.wikipedia.org/wiki/Advertising and file sharing network spam. Botnet is a collection of infected computers or bots that have been taken over by hackers (also known as bot herders) and are used to perform malicious tasks or functions. A computer becomes a bot when it downloads a file (e.g. an e-mail attachment) that has bot software embedded in it. This unit also covers a case study on *Nigerian Letter Fraud*.

4.12 CHECK YOUR PROGRESS: THE KEY

1) **Types of Spam**

Instant Messaging spam

Instant Messaging Spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002. As instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging system such as Skype.

Newsgroup spam

Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet onvention defines spamming as excessive multiple posting,that is, the repeated posting of a message (or substantially similar messages). The prevalence of Usenet spam led to the development of the Breidbart Index as an objective measure of a message's "spamminess".

Forum spam

Forum spam is the creating of messages that are advertisements or otherwise unwanted on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity if a sale goes through, when the spammer behind the spambot works on commission.

Mobile phone spam

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS.

Many online games allow players to contact each other via player-to-player messaging, chat rooms or public discussion areas. What qualifies as spam varies from game to game, but usually this term applies to all forms of message flooding, violating the terms of service contract for the website. This is particularly common in MMORPGs where the spammers are trying to sell game-related "items" for real-world money, chiefly among these items is in-game currency. This kind of spamming is also called Real World Trading (RWT). In the popular MMORPG Runescape, it is common for spammers to advertise sites that sell gold in multiple methods of spam. They send spam via the in-game private messaging system, via using emotes to gain attention and by yelling publicly to everyone in the area.

2) **Types of attack**

- Denial-of-service attacks where multiple systems autonomously access a single Internet system or service in a way that appears legitimate, but much more frequently than normal use and cause the system to become busy
- Adware exists to advertise some commercial entity actively and without the user's permission or awareness, for example by replacing banner ads on web pages with those of another content provider.
- Spyware is software which sends information to its creators about a user's activities - typically passwords, credit card numbers and other information that can be sold on the black market. Compromised machines that are located within a corporate network can be worth more to the bot herder, as they can often gain access to confidential information held within that company. There have been several targeted attacks on large corporations with the aim of stealing sensitive information, one such example is the Aurora botnet.
- E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying or malicious in nature.

3) **Investigation of Nigerian Fraud Cases involves three steps**

- **Obtaining the details of IP addresses from which the e-mails are originated**

  As per experience the initial mails are normally generated from abroad. However, after few mails from abroad the fraudsters send mails from India also. Through IP (Internet Protocol) addresses of such mails, we can reach to the source of the mail which generally turns out to be a Cyber Café in India. Sometimes, these mails are found to be initiated from proxy/spoofed IP addresses because of which actual originator of mails is not identified.

  CERT IN (Computer Emergency Response Team) can be contacted for assistance on this subjects.

- **Following the money trails from victim to suspect through account holder and the middleman of the chain**

  These cheaters use Indian bank accounts to siphon off the cheated amount. Hence, they can also be traced through the account holders. Mostly gullible/unsuspecting persons let their accounts be used for petty gains. However, it is seen that normally these cheaters themselves do not come in the direct contact of the account holders and collect the account through some middlemen/friends. Middlemen are petty criminals who arrange these bank accounts for master minds.

- **Mobile numbers of the suspect and call detail analysis**

  The cheaters also use mobile phones to communicate with the victim. Sometimes these numbers pertain to overseas service providers. However, most of the time these are local numbers. We can also trace these cheaters through such phone connections which they have used. Minute call detail analysis of the phone numbers of suspects or middlemen may give substantial leads in the investigation. It has been seen in some cases that the fraudsters use phone connections procured/managed on fake IDs making it difficult to trace these fraudsters.

Student Satisfaction Survey

ignou THE PEOPLE'S UNIVERSITY

Student Satisfaction Survey of IGNOU Students

Enrollment No.	
Mobile No.	
Name	
Programme of Study	
Year of Enrolment	
Age Group	☐ Below 30 ☐ 31-40 ☐ 41-50 ☐ 51 and above
Gender	☐ Male ☐ Female
Regional Centre	
States	
Study Center Code	

Please indicate how much you are satisfied or dissatisfied with the following statements

Sl. No.	Questions	Very Satisfied	Satisfied	Average	Dissatisfied	Very Dissatisfied
1.	Concepts are clearly explained in the printed learning material	☐	☐	☐	☐	☐
2.	The learning materials were received in time	☐	☐	☐	☐	☐
3.	Supplementary study materials (like video/audio) available	☐	☐	☐	☐	☐
4.	Academic counselors explain the concepts clearly	☐	☐	☐	☐	☐
5.	The counseling sessions were interactive	☐	☐	☐	☐	☐
6.	Changes in the counseling schedule were communicated to you on time	☐	☐	☐	☐	☐
7.	Examination procedures were clearly given to you	☐	☐	☐	☐	☐
8.	Personnel in the study centers are helpful	☐	☐	☐	☐	☐
9.	Academic counseling sessions are well organized	☐	☐	☐	☐	☐
10.	Studying the programme/course provide the knowledge of the subject	☐	☐	☐	☐	☐
11.	Assignments are returned in time	☐	☐	☐	☐	☐
12.	Feedbacks on the assignments helped in clarifying the concepts	☐	☐	☐	☐	☐
13.	Project proposals are clearly marked and discussed	☐	☐	☐	☐	☐
14.	Results and grade card of the examination were provided on time	☐	☐	☐	☐	☐
15.	Overall, I am satisfied with the programme	☐	☐	☐	☐	☐
16.	Guidance from the programme coordinator and teachers from the school	☐	☐	☐	☐	☐

After filling this questionnaire send it to:
Programme Coordinator, School of Vocational Education and Training,
Room no. 19, Block no. 1, IGNOU, Maidangarhi, New Delhi- 110068

MPDD-IGNOU/P.O.1T/Feb,2012

ISBN-978-81-266-5922-7