As per New CBCS Syllabus for Third Semester, B.Com. (Pass), Delhi University w.e.f. 2015-16

CYBER CRIMES AND LAWS

Dr. U.S. Pandey
Dr. Verinder Kumar
Dr. Harman Preet Singh

Himalaya Publishing House
ISO 9001:2008 CERTIFIED

CYBER CRIMES AND LAWS

[As per New Syllabus (CBCS) for Third Semester, B.Com. (Pass), Delhi University w.e.f. 2015-16]

Dr. U.S. PANDEY
M.Sc., Ph.D. (Computer Science)
Associate Professor,
School of Open Learning,
University of Delhi, Delhi.

Dr. VERINDER KUMAR
M.Com., MCA, M.Phil., Ph.D. (Computer Science)
Assistant Professor,
IGIPESS,
University of Delhi, Delhi.

Dr. HARMAN PREET SINGH
MBA, Ph.D.
Assistant Professor,
PGDAV College (M),
University of Delhi, Delhi.

Himalaya Publishing House

ISO 9001 : 2008 CERTIFIED

FIRST EDITION : 2017

Published by : Mrs. Meena Pandey for **Himalaya Publishing House Pvt. Ltd.,**
"Ramdoot", Dr. Bhalerao Marg, Girgaon, **Mumbai - 400 004.**
Phone: 022-23860170, 23863863; **Fax:** 022-23877178
E-mail: himpub@vsnl.com; **Website:** www.himpub.com

Branch Offices :

New Delhi : "Pooja Apartments", 4-B, Murari Lal Street, Ansari Road, Darya Ganj, New Delhi - 110 002. Phones: 011-23270392, 23278631; Fax: 011-23256286

Nagpur : Kundanlal Chandak Industrial Estate, Ghat Road, Nagpur - 440 018. Phones: 0712-2738731, 3296733; Telefax: 0712-2721215

Bengaluru : Plot No. 91-33, 2nd Main Road, Seshadripuram, Behind Nataraja Theatre, Bengaluru - 560020. Phones: 08041138821, 09379847017, 09379847005

Hyderabad : No. 3-4-184, Lingampally, Besides Raghavendra Swamy Matham, Kachiguda, Hyderabad - 500 027. Phones: 040-27560041, 27550139; Mobile: 09390905282

Chennai : New No. 48/2, Old No. 28/2, Ground Floor, Sarangapani Street, T. Nagar, Chennai - 600 012. Mobile: 09380460419

Pune : First Floor, "Laksha" Apartment, No. 527, Mehunpura, Shaniwarpeth, (Near Prabhat Theatre), Pune - 411 030. Phones: 020-24496323/24496333; Mobile: 09370579333

Lucknow : House No. 731, Shekhupura Colony, Near B.D. Convent School, Vikas Nagar, Aliganj, Lucknow - 226 022. Mobile: 09307501549

Ahmedabad : 114, "SHAIL", 1st Floor, Opp. Madhu Sudan House, C.G. Road, Navrang Pura, Ahmedabad - 380 009. Phone: 079-26560126; Mobile: 09377088847

Ernakulam : 39/176 (New No. 60/251), 1st Floor, Karikkamuri Road, Ernakulam, Kochi - 682011, Kerala. Phones: 0484-2378012, 2378016; Mobile: 09344199799

Bhubaneswar: 5, Station Square, Bhubaneswar - 751 001 (Odisha). Phone: 0674-2532129; Mobile: 09338746007

Kolkata : 108/4, Beliaghata Main Road, Near ID Hospital, Opp. SBI Bank, Kolkata - 700 010. Phone: 033-32449649; Mobile: 09883055590, 07439040301

DTP by : Sudhakar Shetty.

Printed at : Shri Krishna Offset Press, Delhi. On behalf of HPH.

This book is dedicated

to

My Mother

&

Father

Authors

(1) U.S. Pandey
(2) Verinder Kumar
(3) Harman Preet Singh

SYLLABUS

B.COM., SEMESTER III

PAPER BC3A (B): CYBER CRIMES AND LAWS

Duration: 2 Hours

Objective: This paper intends to create an understanding towards the cyber crimes and to familiarise the students with the application of cyber laws in general.

CONTENTS

Unit I: Cyber Crimes

Introduction — Computer Crime and Cyber Crimes: Distinction between Cyber Crime and Conventional Crimes; Cyber Forensic; Kinds of Cyber Crimes — Cyber Stalking, Cyber Terrorism, Forgery and Fraud, Crimes Related to IPRs, Computer Vandalism: Privacy of Online Data; Cyber Jurisdiction; Copyright Issues; Domain Name Dispute, etc.

Unit II: Definition and Terminology (Information Technology Act, 2000)

Concept of Internet, Internet Governance, E-contract, E-forms, Encryption, Data Security.

Access, Addressee, Adjudicating Officer, Affixing Digital Signatures, Appropriate Government, Certifying Authority, Certification Practice Statement, Computer, Computer Network, Computer Resource, Computer System, Cyber Appellate Tribunal, Data, Digital Signature, Electronic Form, Electronic Record, Information, Intermediary, Key Pair, Originator, Public Key, Secure System, Verify, Subscriber as defined in the Information Technology Act, 2000.

Unit III: Electronic Records

Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Use of Electronic Records and Digital Signatures in Government and its Agencies; Retention of Electronic Records; Attribution, Acknowledgement and Dispatch of Electronic Records; Secure Electronic Records and Digital Signatures.

Unit IV: Regulatory Framework

Regulation of Certifying Authorities; Appointment and Functions of Controller; License to Issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences.

CONTENTS

Chapter 1

Cyber Crimes

1.1 COMPUTER CRIME

Computer crime is a growing threat to society caused by the criminals and irresponsible actions of individuals who are taking advantage of the widespread use of computer networks in our society. It presents a major challenge to the ethical use of information technologies. Computer crime poses serious threats to the integrity, safety, and survival of most e-business systems, and thus makes the development of effective security methods a top priority.

According to Association of Information Technology Professionals (AITP), computer crime includes the following:

- The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources
- The unauthorized release of information
- The unauthorized copying of software
- Denying an end-user access to his or her own hardware, software, data, or network resources
- Using or conspiring to use computer or network resources to illegally obtain information or tangible property.

1.2 CYBER CRIME

Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Cyber crime includes traditional crimes conducted through the Internet. For example, hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through

the use of a computer and the Internet. Cyber crimes also includes offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails, noticeboards and groups) and mobile phones (SMS/MMS).

Cyber crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cyber crimes, including espionage, financial theft and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

1.3 COMPUTER CRIME AND CYBER CRIME

Computer crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are subject everywhere to criminal sanctions. The term computer misuse and abuse are also used frequently, but they have significantly different implications. Annoying behavior must be distinguished from criminal behavior in law. As per IT Act, 2000, no description has been categorically made for computer crime and cyber crime. So till today, it is very difficult to differentiate between these two words. In relation to the issue of intent, the principle of claim of right also informs the determinations of criminal behavior. For example, an employee who has received a password from an employer, without direction as to whether a particular database can be accessed, is unlikely to be considered guilty of a crime if he or she accesses those databases. So, a distinction must be made between what is unethical and what is illegal. The legal response to the problems must be proportional to the activity that is alleged. Common types of computer crimes are:

- Forgery;
- Fraud by system manipulation intentionally;
- Any modification to data or programs or databases; and
- Accessing computers without authorization;

However, cyber crimes are somehow different from computer crimes. Computer crime happens in physical space with or without the network. Cyber crime takes place in a virtual space through digital environment. Recent example of cyber crime was Bazzee.com case, which is a MMS scandal. Cyber crimes may happen globally as there is no geographical limit for cyberspace.

1.4 DISTINCTION BETWEEN CYBER CRIME AND CONVENTIONAL CRIMES

Although we talk about cyber crime as a separate entity to traditional crime, it is carried out by the same types of criminals for the same type of reasons. These hackers are professional

thieves, criminal gangs, disgruntled employees, professional competition, activists, disillusioned youth and state adversaries. They have the same motivations as traditional criminals such as boredom and vandalism, ideological or political support, malice or revenge, monetary gain through extortion or sale of illegally obtained data, terrorism or notoriety and sensationalism. However, there are certain differences between cyber crimes and conventional crimes, which are discussed below:

- **Evidence of the offences:** Traditional criminals usually leave traces of a crime, through either fingerprints or other physical evidences. On the other hand, cybercriminals rely on the Internet via which they commit their crimes, and it leaves very little evidence about the cyber crime. Forensic investigators usually experience great difficulty in gathering evidence that could lead to the conviction of cybercriminals since these criminals can freely change their identities. The Internet also allows the anonymity of its users, and this implies that cybercriminals can use any pseudonyms for their identification. On the other hand, it is difficult for traditional criminals to fake their gender, race, or age.
- **Length of investigations:** Since cyber crime involves perpetrators using falsified names and working from remote locations, it usually takes longer to identify the real cybercriminals and apprehend them. In most cases, cybercriminals (such as hackers) escape from arrest because the investigators cannot locate them. Traditional crimes take shorter time period to investigate because the criminals usually leave evidence that can be used to spot them. For instance, traditional criminals can leave evidence such as DNA, fingerprints, photographs and videos captured on surveillance cameras, or personal belongings such as identity cards, and this makes it easy for investigators to identify and capture the culprits. In addition, such evidence makes it easy for the judiciary to convict the offenders.
- **Constitutional law provisions:** Article 20(3) of the Indian constitution deals with the privilege against self-incrimination. According to this article, "No person accused of any offence shall be compelled to be a witness against himself". Consequently, cybercriminals can use this legal provision to deny the investigators any incriminating evidence that could lead to the prosecution of the cybercriminals. This implies that even in situations where cybercriminals are apprehended, the trial process may take long unless the investigators gathered irrefutable evidence about the crimes.
- **Use of force:** Most of the traditional crimes (such as rape, murder, arson, and burglary among others) involve the use of excessive force that results in physical injury and trauma of the victims. On the other hand, cyber crimes do not require the use of any force since the criminals merely use the identities of their victims to steal from them. For example, cybercriminals use spoofing and phishing to obtain personal information such as credit card numbers from their victims, or use encrypted emails to coordinate violence remotely.
- **Scale of attacks:** Cyber-attacks can be conducted on a scale not possible in the physical world. A traditional bank robber may only be able to hit one or two banks a week, a cyber-attack can target 100s if not 1000s of sites at once.

- **Reach of attacks:** Cyber-attacks can be performed from anywhere in the world; they can be performed anonymously and within jurisdictions where the consequences of those actions may not, or cannot, be addressed by the criminal justice system. Attackers are also able to extract far more data digitally than would ever be possible in the physical world. For example, 1 gigabyte of data is approximately 4,500 paperback books. Think of how many gigabytes of data is held on a system, hackers can extract this within a matter of minutes.
- **Speed of attacks:** Cyber-attacks are conducted at machine speed; a criminal can write a piece of code that can target multiple sites in minutes.
- **Perception and media effect:** The public and media perception of cyber crime is different from a conventional crime. When large financial institutions have been hacked, the media has often wholly apportioned blame to the organizations rather than the criminals; this would not be the case in a physical bank robbery.

1.5 CYBER FORENSICS

Cyber forensics (or computer forensics) is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures. After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

The need or the importance of the computer forensics is to ensure the integrity of the computer system. The system with some small measures can avoid the cost of operating and maintaining the security. The subject provides in-depth knowledge for the understanding of the legal as well as the technical aspects of computer crime. It is very much useful from a technical point of view.

The importance of computer forensics is evident in tracking the cases of child pornography and email spamming. Computer forensics has been efficiently used to track down the terrorists from the various parts of the world. The terrorists using the Internet as the medium of communication can be tracked down and their plans can be known.

There are various tools that can be used in combination with the computer forensics to find out the geographical information and the hideouts of the criminals. The IP address

plays an important role to find out the geographical position of the terrorists. The security personnel deploy the effective measures using the computer forensics. The Intrusion Detecting Systems are used for that purpose.

A number of techniques are used during computer forensics investigations such as:

- **Cross-drive analysis:** It is a forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.
- **Live analysis:** It involves examination of computers from within the operating system using custom forensics or existing system administration tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.
- **Deleted files:** It is a common technique used in computer forensics to recover the deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.
- **Stochastic forensics:** It is a method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.
- **Steganography:** It is one of the techniques used to hide data via steganography. It involves the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available). While the image appears exactly the same, the hash changes as the data changes.

1.6 TYPES OF CYBER CRIMES

There are many types of cyber crimes and the most common ones are explained below:

1.6.1 Cyber Defamation

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

Defamation comprises of both slander (defamation by speaking) and libel (defamation by means of writing). Slander involves the oral "publication" of a defamatory remark that is heard by another, which injures the subject's reputation or character. Slander can occur through the use of a hand gesture or verbal communication that is not recorded. Libel, on the other hand, is the written "publication" of a defamatory remark that has the tendency to injure another's reputation or character. Libel also includes a publication on radio, audio or video. Even though this would be considered oral, or verbal, communication to someone, it is actually considered to be libel because it is published in a transfixed form.

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

Quantitatively, a comment defaming a person can be sent to a large number of persons through email by a click of the mouse. Much easier would be to publish it on a discussion board known to be visited by thousands of persons every day. On the number game, it is still more convenient to make available the defamatory sentence to millions of people by merely publishing it on the website. The number of people a comment defaming a person might reach is gigantic and hence would affect the reputation of the defamed person much more than would an ordinary publication.

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

1.6.2 Corporate Cyber Smear

Harmful, defamatory, insulting or offending online message has been termed as corporate cyber smear. It is a false and disparaging rumor about a company, its management or its stock. This is commonly done through the internet via websites, blogs, forums, emails and instant messaging, chat rooms and now in the social networking sphere. This kind of criminal activity has been a concern especially in stock market and financial sectors where knowledge and information are the key factors for businessmen. Persons indulging in corporate cyber smear include disgruntled employees or insiders, ex-employees, envious ex-colleagues, impostors, competitors, creditors, and even those seeking a forum when they are denied employment or former shareholders.

False and defamatory statements made against Amazon Natural Treasures Inc. led to a stock price decline from an April 1997, 52-week high of $3.56 per share to approximately

12 cents per share. The low stock price led to a delisting from the OTCBB to the pink sheets. It transpired that the statements were made by the owner of Demonte & Associates, a New York public relations firm, who claimed that a collection agency was suing Amazon for about $7,000.

1.6.3 Forgery

Forgery is defined as the criminal act that includes the purposeful defrauding, misleading, deception, and misrepresentation of a product, service, or item with the intent to deceive. The scope forgery is a vast one; forgery can include the production of falsified documents, counterfeited items — products intended to resemble other products, and the misrepresentation of fraudulent identification.

The criminal act of forgery can take place in a variety of settings. However, with regard to identity theft, the act of unlawfully recreating the likeness of the signature belonging to another individual or entity with the intent of providing deceitful authorization for economic gain is one of the foremost methodologies undertaken. Desktop publishing systems, color laser and ink-jet printers, color copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

Forgery could be of various types:

- **Electronic forgery:** The misuse of computer networks, the internet, and various avenues within the online community in order to defraud potential victims of identity theft is classified as electronic or online forgery. Electronic forgery is quite common within the digital age, which can include the illegal and unlawful reproduction of endorsements in the form of electronic signatures in order to illicitly assume the identity of the victim of identity theft.
- **Financial forgery:** Criminal fraudulent activity applicable to the events involving the exchange and circulation of currency may be classified as financial forgery. Identity theft resulting from this type of forgery can occur in a variety of fashions, including fraudulent purchases through the use of finances — and financial information — belonging to the victims of this crime.
- **Commercial forgery:** Forgery involving business activities, commercial endeavors, or professional operation of the provision of products or services is classified as commercial forgery; items unlawfully purchased with illegal and illicit finances may result from identity theft.
- **Governmental and administrative forgery:** Administrative forgery includes the vast expanses of laws, acts, ordinances, and legislation; identity theft in an administrative realm may include the unlawful duplication of documentation or the illegal officiating of government-mandated forms and requirements.

In order to prevent these forgeries, electronic identity theft need to be stopped. Due to technological innovation, electronic identity theft is considered by many to be one of the most recently-developed crimes, credited — in part — to the ongoing advent of computer-based technology. This type of technology relies heavily on the Internet and online activity, and

as a result, regulations and oversight of this type of activity has been expressed in the spectrum of preventative measures involving the cessation of electronic identity theft.

Companies providing methods of identity theft prevention have employed protective measures ranging from securing online perimeters to communicative transmission inquiring about the validity of unsubstantiated activity. These types of companies have found their respective niche within the prevention of identity fraud upon providing protection in lieu of infringing on personal privacy.

1.6.4 Cyber Pornography

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

Two primary reasons why cyber pornography has, in recent years, gathered much attention of both the offender and user, are:

- Easy accessibility;
- Anonymity.

Individuals can easily view thousands of pornographic images day and night within the privacy of the four walls of their homes. The Internet has decreased the hurdle of shame that comes with purchasing pornographic materials in a shop or the embarrassment of being caught with physical hard copies of porno materials. The consumer of such publications is more comfortable in opening a website and viewing/watching. With availability of broadband connections and high downloading speeds, the demand, though privately, seems to have risen.

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

What has, however, been most disturbing is the increase in child pornography. Child pornography is different from other pornography, and consequently receives more stringent legal treatment. It is distinguished as an issue of child abuse — in its production and/or in

the way it is used by pedophiles to desensitize their victims. The growth of the Internet has provided child pornographers with a distribution vehicle which is perceived to be relatively anonymous.

1.6.5 Cyber Stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as email or instant messaging (IM), or messages posted to a website or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyber stalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

In a variation known as corporate cyber stalking, an organization stalks an individual. Corporate cyber stalking (which is not the same thing as corporate monitoring of email) is usually initiated by a high-ranking company official with a grudge, but may be conducted by any number of employees within the organization. Less frequently, corporate cyber stalking involves an individual stalking a corporation.

WHOA (Working to Halt Online Abuse), an online organization dedicated to the cyber stalking problem, reported that in 2001, cyber stalking began with email messages most often, followed by message boards and forums messages, and less frequently with chat. In some cases, cyber stalking develops from a real-world stalking incident and continues over the Internet. However, cyber stalking is also sometimes followed by stalking in the physical world, with all its attendant dangers.

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

(*a*) Ease of communication

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

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

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

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

There are a number of simple ways to guard against cyber stalking. One of the most useful precautions is to stay anonymous yourself, rather than having an identifiable online presence. Use your primary email account only for communicating with people you trust and set up an anonymous email account, such as Gmail or Yahoo, to use for all your other communications. Set your email program's filtering options to prevent delivery of unwanted

messages. When choosing an online name, make it different from your name and gender-neutral. Don't put any identifying details in online profiles.

Should you become the victim of a cyber stalker, the most effective course of action is to report the offender to their Internet service provider (ISP). Should that option be impossible, or ineffective, the best thing to do is to change your own ISP and all your online names.

1.6.6 Online Gambling

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

1.6.7 Online Sale of Illegal Articles

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

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

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

1.6.8 Cyber Fraud

Cyber fraud (or Internet fraud) refers to any type of deliberate deception for unfair or unlawful gain that occurs online. It involves the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form

of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Research suggests that online scams can happen through social engineering and social influence. It can occur in chat rooms, social media, email, message boards, or on websites.

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

Online auction and retail schemes are other kinds of cyber fraud. These schemes typically purport to offer high-value items — ranging from Cartier watches to computers to collectibles such as Beanie Babies — that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (*e.g.*, counterfeit or altered goods).

Business opportunity or work-at-home schemes are another type of fraud. Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn a substantial amount of money in "work-at-home" ventures. These schemes typically require the individuals to pay money upfront, but do not deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

1.6.9 Online Investment Fraud

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

Market manipulation scheme is another online investment fraud. Enforcement actions by the US Securities and Exchange Commission and criminal prosecutions indicate that the basic method for criminals to manipulate securities markets for their personal profit is the

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

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

Fraudulent financial solicitation is another online investment fraud. Due to its ease and anonymity, there have been instances of people soliciting money online for charitable purposes. One might seek financial contribution via credit card online to certain public purpose funds or schemes for the benefit of certain classes or downtrodden people of society. Many a time, fiscal statutes provide for income tax exemption for such contributions and online promises are made to provide a tax exemption certificate in case such contributions are made. The website may even provide for a printout of a fake certificate. On January 30, 2006, Gary S. Kraser pleaded guilty in the United States District Court for the Southern District of Florida to online fraud in connection with his fraudulent solicitation of charitable donations supposedly intended for Hurricane Katrina relief. According to the indictment, the defendant falsely claimed in conversations on the Internet, and ultimately via the website www.AirKatrina.com, that he was piloting flights to Louisiana to provide medical supplies to the areas affected by Hurricane Katrina and to evacuate children and others in critical medical condition. He further claimed that he had organized a group of Florida pilots to assist him in his supposed relief efforts. In just two days, the defendant received almost $40,000 in donations from 48 different victims from around the world.

1.6.10 Spam and Phishing

Spamming and phishing are two very common forms of cyber crimes. There are not much people can do to control them. Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cybercriminals offer a bait so that people take it and give out the information that cybercriminals want. The bait can be in form of a business proposal, announcement of a lottery to which people never subscribed, and anything that promises them money for nothing or a small favor. There are online loan companies too, making claims that people can get insecure loans irrespective of their location. Doing business with such claims, people sure suffer both financially and mentally in the end.

Such spamming and phishing attempts are mostly emails sent by random people whom others never hear of. People should stay away from any such offers especially when they feel that the offer is too good. The US Cyber Crime Center says — do not get into any kind of agreement that promise something too good to be true. In most cases, they are fake offers aiming to get people's information and to get their money directly or indirectly.

1.6.11 Spear Phishing

As with the email messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or website with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the email is likely to be an individual within the recipient's own company and generally someone in a position of authority.

Visiting West Point teacher and National Security Agency expert Aaron Ferguson calls it the "colonel effect." To illustrate his point, Ferguson sent out a message to 500 cadets asking them to click a link to verify grades. Ferguson's message appeared to come from a Colonel Robert Melville of West Point. Over 80% of recipients clicked the link in the message.

Most people have learned to be suspicious of unexpected requests for confidential information and will not divulge personal data in response to email messages or click on links in messages unless they are positive about the source. The success of spear phishing depends upon three things:

- The apparent source must appear to be a known and trusted individual
- There is information within the message that supports its validity, and
- The request the individual makes seems to have a logical basis.

Here's one version of a spear phishing attack. The perpetrator finds a web page for their target organization that supplies contact information for the company. Using available details to make the message seem authentic, the perpetrator drafts an email to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming. If a single employee falls for the spear phisher's ploy, the attacker can masquerade as that individual and use social engineering techniques to gain further access to sensitive data.

1.6.12 Cyber Terrorism

According to the US Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". It is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Cyber terrorism is sometimes referred to as electronic terrorism or information war.

Unlike a nuisance virus or computer attack that results in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the US Commission of Critical Infrastructure Protection, possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

Cyber terrorism can occur over the public internet, over private computer servers, or even through secured government networks. There are many ways in which a criminal could use electronic means to incite fear and violence. It is far less expensive to purchase a computer than to access guns or bombs, making this approach appealing for many potential criminals worldwide. It can be anonymous and conducted at a great distance away from the target. For just a few examples, consider these situations:

- Foreign governments may use hackers to spy on other countries' intelligence communications in order to learn about where their troops are located or otherwise gain a tactical advantage at war.
- Domestic terrorists may break into the private servers of a corporation in order to learn trade secrets, steal banking information, or perhaps the private data of their employees.
- Global terror networks may disrupt a major website, in order to create a public nuisance or inconvenience, or even more seriously, try to stop traffic to a website publishing content with which they disagree.
- International terrorists could try to access and disable the signal which flies drones or otherwise controls military technology.
- A cyber terrorist could try to attack the next generation of air traffic control systems, or collide two large civilian aircraft or try to derail the trains on the rail lines.

1.6.13 Social Engineering Identity Theft

Social engineering identity theft is a method where the cybercriminals make a direct contact with people using emails or phones with the intention to deceive. They try to gain their confidence and once they succeed at it, they get the information they need. This information can be personal, about money, about the company where someone works or anything that can be of interest to the cybercriminals.

It is easy to find out basic information about people from the Internet. Using this information as the base, the cybercriminals try to befriend them and once they succeed, they will disappear, leaving people prone to different financial injuries directly and indirectly. They can sell the information obtained from people or use it to secure things like loans in their name. They use social engineering for identity theft. So, the people should be very careful when dealing with strangers – both on phone and on the Internet.

1.6.14 Cyber Extortion

Cyber extortion is a crime involving an attack or threat of attack coupled with a demand for money to avert or stop the attack. In such attacks, while cybercriminals threaten to cripple websites or disclose sensitive data, the data itself (stolen or accessed without authorization) is not tampered with and is usually safely returned on demands of the cyber extortionists being met. Simply put, hackers are forcing companies to pay them to desist from impeding commercial operations — a fee to be left alone.

Cyber extortion can take many forms. Originally, denial of service (DoS) attacks against corporate websites were the most common method of cyber extortion; the attacker might initiate a ping storm and telephone the president of the company, demanding that money be wired to a bank account in a foreign country in exchange for stopping the attack.

In a shocking revelation, two Indian companies conceded to having paid hackers money to the tune of $10 million, to protect sensitive information stolen from their compromised computer networks, from imminent exposure. As the stolen information was incriminatory in nature, the attacks which seems to have originated in the Middle East, went unreported by the companies' even months after payments had been made and no case has been filed by either company. Nevertheless, the discovery has prompted an unprecedented interest in understanding cyber extortion, its operation and treatment in India.

In recent years, however, cybercriminals have developed ransomware which encrypts the victim's data. The extortionist's victim typically receives an email that offers the private decryption key in exchange for a monetary payment in Bitcoins, a digital currency. In another instance of cyber extortion, a businessman from Hyderabad recently found himself unable to access his company's database as it had been encrypted by a hacker demanding payment for decryption.

Cyber extortion can be lucrative, netting attackers millions of dollars annually. Unfortunately, as with other types of extortion, payment does not guarantee that further cyber-attacks will not be launched. Most cyber extortion efforts are initiated through malware in email attachments or on compromised websites. To mitigate the risks associated with cyber extortion, experts recommend that end-users should be educated about phishing exploits and back up their computing devices on a regular basis.

1.6.15 Intellectual Property Theft

Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions — known as "intellectual property". It includes theft of material that is copyrighted or patented, the theft of trade secrets, and trademark violations.

A copyright is the legal right of an author, publisher, composer, or other person who creates a work to exclusively print, publish, distribute, or perform the work in public. Examples of copyrighted material commonly stolen online are computer software, recorded music, movies and electronic games.

A patent is an exclusive right granted by a country to the owner of an invention to make, use, manufacture and market the invention, provided the invention satisfies certain conditions stipulated in the law. Exclusive right implies that no one else can make, use, manufacture or market the invention without the consent of the patent holder. This right is available for a limited period of time.

Theft of trade secrets means the theft of ideas, plans, methods, technologies, or any sensitive information from all types of industries including manufacturers, financial service institutions, and the computer industry. Trade secrets are plans for a higher speed computer, designs for a highly fuel-efficient car, a company's manufacturing procedures, or the recipe

for a popular salad dressing, cookie mix, or barbeque sauce. These secrets are owned by the company and give it a competitive edge. Theft of trade secrets damages the competitive edge and therefore the economic base of a business.

A trademark is the registered name or identifying symbol of a product that can be used only by the product's owner. Trademarks may be one or a combination of words, letters and numerals. They may also consist of drawings, symbols, three-dimensional signs such as shape and packaging of goods, or colors used as a distinguishing feature. Collective marks are owned by an association whose members use them to identify themselves with a level of quality. Certification marks are given for compliance with defined standards, for example ISO 9000. A trademark provides to the owner of the mark by ensuring the exclusive right to use it to identify goods or services or to authorize others to use it in return for some consideration (payment). A trademark violation involves counterfeiting or copying brand name products such as well-known types of shoes, clothing, and electronics equipment and selling them as the genuine or original product.

The two forms of intellectual property most frequently involved in cyber crime are copyrighted material and trade secrets. Piracy is a term used to describe intellectual property theft — piracy of software, piracy of music, etc. Historically, when there were no computers, intellectual property crimes involved a lot of time and labor. In the twenty-first century, software, music, and trade secret pirates operate through the Internet. Anything that can be digitized — reduced to a series of zeroes and ones — can be transmitted rapidly from one computer to another. There is no reduction of quality in second, third, or fourth generation copies. Pirated digital copies of copyrighted work transmitted over the Internet are known as "warez". Warez groups are responsible for illegally copying and distributing hundreds of millions of dollars of copyrighted material.

Pirated trade secrets are sold to other companies or illegal groups. Trade secrets no longer have to be physically stolen from a company. Instead, corporate plans and secrets are downloaded by pirates onto a computer disc. The stolen information can be transmitted worldwide in minutes. Trade secret pirates find pathways into a company's computer systems and download the items to be copied. Companies keep almost everything in their computer files. Pirated copies are sold over the Internet to customers who provide their credit card numbers and then download the copy.

1.6.16 Computer Vandalism

Computer vandalism is a type of mischievous behavior that damages computers and data in various ways and disrupts businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks such as extracting login credentials or erasing hard drive data. Cyber vandals are individuals who damage information infrastructures purely for their own enjoyment and pleasure. Their primary motivation is not financial; it is the desire to prove that the feat could be accomplished. Once inside, they leave their mark so there is no denying their presence. At first brush, this may seem more of a prank than an attack aimed at destruction. The effect on business, however,

is undeniable. These types of attacks fall into the category of denial-of-service attack. The affected site must be shut down and repaired before it can be returned to normal operation.

1.6.17 Computer Viruses and Worms

A virus is a program that searches out other programs and 'infects' them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the 'infection'. This normally happens invisibly to the user. However, unlike a worm, a virus cannot infect other computers without assistance. The virus may do nothing but propagate itself and then allow the program to run normally. Virus spreads to other computers through network file system, through the network, Internet or by the means of removable devices like USB drives and CDs. Usually, however, after propagating silently for a while, it starts doing things like writing messages on the terminal or playing strange tricks with the display. Certain viruses, written by particularly perversely minded crackers, do irreversible damage, like deleting all the user's files. Computer virus is a form of malicious code written with an aim to harm a computer system and destroy information. Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

On the other hand, a worm is a program that propagates itself over a network, reproducing itself as it goes. Therefore, worm, unlike a virus, does not require a medium to propagate itself and infect other computers.

1.6.18 Trojan Horses

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

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

1.6.19 Logic Bombs

In a computer program, a logic bomb, also called slag code, is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.

Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up-to-date anti-virus program.

For best results, the auto-protect and email screening functions of the anti-virus program should be activated by the computer user whenever the machine is online. In a network, each computer should be individually protected, in addition to whatever protection is provided by the network administrator. Unfortunately, even this precaution does not guarantee 100% system immunity.

In an instance of logic bomb, a computer systems administrator for UBS PaineWebber was charged with using a 'logic bomb' to cause more than $3 million in damage to the company's computer network. It was alleged that from November 2001 to February 2002, the accused constructed the logic bomb computer program. On March 4, as planned, his program activated and began deleting files on over 1,000 of PaineWebber's computers [US v. Smith].

1.6.20 Back Door

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

1.6.21 Malvertising

Malvertising is a method whereby users download malicious code by simply clicking at some advertisement on any website that is infected. In most cases, the websites are innocent. It is the cybercriminals who insert malicious advertisements on the websites without the knowledge of the latter. It is the work of advert companies to check out if an advertisement is malicious but given the number of advertisements they have to deal with, the malverts easily pass off as genuine ads.

In other cases, the cybercriminals show clean ads for a period of time and then replace it with malverts so that the websites and advertisements do not suspect. They display the malverts for a while and remove it from the site after meeting their targets. All this is so fast that the website does not even know they were used as a tool for cyber crime. Malvertising is one of the fastest, increasing types of cybercrime.

1.6.22 Hacking

The activity of breaking into a computer system to gain an unauthorized access is known as hacking. It is the act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

1.6.23 Theft of Internet Hours

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

1.6.24 Salami Attacks

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

1.6.25 Data Diddling

This computer crime relates to operation security and is minimized through strengthening of internal security controls. This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. This is a simple and common computer related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data.

1.6.26 Steganography

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

Following steps are generally followed to achieve the desired result:

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

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

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

(*d*) Emailing the carrier file to the receiver.

(*e*) Decryption of the message by the receiver.

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

1.6.27 Cyberwarfare

Cyberwarfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems — among many other possibilities.

Any country can wage cyberwar on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure. For the same reason, non-governmental groups and individuals could also launch cyberwarfare attacks.

Examples of cyberwarfare include:

- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
- Also in 2007, an unknown foreign party hacked into high-tech and military agencies in the United States and downloaded terabytes of information.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

The most effective protection against cyberwarfare attacks is securing information and networks. Security updates should be applied to all systems — including those that are not considered critical — because any vulnerable system can be co-opted and used to carry out

attacks. Measures to mitigate the potential damage of an attack include comprehensive disaster recovery planning that includes provisions for extended outages.

1.7 INDIAN LAWS ON CYBER CRIMES

The Information Technology Act, 2000 (ITA 2000) is a comprehensive legislation dealing with cyber crimes in India. ITA 2000 was amended by the Information Technology (Amendment) Act, 2008 (ITAA 2008). The IT Act amended important legislations such as Indian Penal Code, 1860 (section 91), The Indian Evidence Act 1872 (section 92), The Bankers' Books Evidence Act, 1891 (section 93) and the Reserve Bank of India Act, 1934 (section 94) in the manner specified in first, second, third and fourth schedule respectively annexed to the ITA 2000. Further amendments were made by the ITAA 2008.

The laws in India related to different types of cyber crimes are discussed below:

1.7.1 Legal Provisions Regarding Cyber Defamation and Corporate Cyber Smear

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

In the case of Tata Sons v. Turtle International, the Delhi High Court has held that publication is a comprehensive term, embracing all forms and mediums – including the Internet.

Cyber defamation is covered under sections 469, 499 and 503 of Indian Penal Code (IPC), 1860 read with section 4 of the IT Act. Section 469 of IPC says that whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine. Section 499 of the IPC says that whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person. Section 503 of IPC says that whoever, threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threats, commits criminal intimidation.

A bare perusal of the sections of IPC above makes it clear that no specific mention has been made with regard to any electronic publication. However, section 4 of the ITA 2000 gives legal recognition of electronic records. It provides that if any information has to be in written form by law, then such information is acceptable in electronic form and can be made available for subsequent reference. Following was the effect of ITA 2000 on defamation:

- The law of defamation under Section 499 got extended to "speech" and "documents" in electronic form.
- The phrase "intending that the document forged" under Section 469 was replaced by the phrase "intending that the document or electronic record forged".
- Section 503 of IPC extended the definition of the offense of criminal intimidation by use of emails and other electronic means of communication for threatening or intimidating any person or his property or reputation.

Keeping in mind the legal provision created by section 4 of the ITA 2000, if any defamatory information is posted on the Internet either through emails, chat rooms, chat boards, online discussion groups, intranets, electronic bulletin boards, etc., such posting would be covered under the sections 469, 499 and 503 of IPC and would amount to cyber defamation.

The offence of defamation is punishable under Section 500 of IPC with a simple imprisonment up to 2 years or fine or both. This is the legal position of cyber defamation in India. The same provisions of the law would be applicable to corporate cyber smear as well.

A person aggrieved of the offence of cyber defamation can make a complaint to the Cyber Crime Investigation Cell. The Cyber Crime Investigation Cell is a branch of the Criminal Investigation Department (CID). Cyber Crime Investigation Cells have opened up in many cities like Delhi, Mumbai, Chandigarh, Hyderabad, Bangalore, Tamil Nadu, Gurgaon, Pune, Madhya Pradesh, Lucknow, etc. The Cyber Crime Investigation Cells deal with offences related to the computer, computer network, computer resource, computer systems, computer devices and Internet. It also has power to look into other high-tech crimes.

1.7.2 Legal Provisions Regarding Forgery

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

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

1. Who dishonestly or fraudulently makes any electronic record, or, affixes any digital signature on any electronic record, or, makes any mark denoting the authenticity of the digital signature, with the intention of causing it to be believed that such electronic record or part of electronic record or digital signature was made, executed,

transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, executed or affixed; or

2. Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or
3. Who dishonestly or fraudulently causes any person to sign, execute or alter an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, does not know the contents of the electronic record or the nature of the alteration.

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

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

1.7.3 Legal Provisions Regarding Cyber Pornography

The issue of cyber pornography has been dealt with in section 67 of the IT Act where publishing of information which is obscene in electronic form has been made an offence. The section provides that any material which is published, or transmitted or caused to be published in the electronic form shall be an offence in the following situations:

(*a*) The material so published or transmitted is lascivious;

(*b*) The material appeals to the prurient interest;

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

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

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

1.7.4 Legal Provisions Regarding Cyber stalking

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

1.7.5 Legal Provisions Regarding Online Gambling

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

Relevant provisions of the IPC along with IT Act dealing with cheating, criminal misappropriation or criminal breach of trust with electronic means could be applied in cases of online gambling. However, there is no direct law in this regard.

1.7.6 Legal Provisions Regarding Online Sale of Illegal Articles

Under the Indian law, many articles are prohibited for sale. For instance, with regard to sale of arms and ammunition, section 7 of the Arms Act, 1959 specifically prohibits sale

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

Therefore, as far as the issue of legality of sale of any article on the Internet is concerned, it would be governed by a specific statute. Merely because it is being sold through the Internet would not change the character of sale and would still be within the ambit of the prohibitory provision of the enactment. So, the above mentioned laws could be read along with the provisions of the IT Act.

1.7.7 Legal Provisions Regarding Cyber Fraud, Online Investment Fraud and Phishing

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

As per section 43(d) (amended vide ITAA 2008), if any person without permission of the owner or in-charge of the computer, computer system or computer network damages it, he shall be liable to pay a fine not exceeding one crore rupees to the affected person. Section 43(d) penalizes a person who damages or causes damage to data. 'Damage', under clause (IV) of the Explanation, means to destroy, alter, add, modify or rearrange any computer resource by any means. Therefore, unauthorized alteration of data would come within the ambit of section 43(d) which is sufficient to cover computer crimes like issuance of false stocks or market manipulation schemes since they essentially involve alteration and/or addition of data.

Section 65 deals with tampering with computer source documents. It provides punishment for a period of up to 3 years or fine up to 2 lakh rupees for a person, who conceals, destroys or alters any computer source code, when the computer source code is required to be kept or maintained by law. 'Computer source code' has been defined as the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

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

Under the Indian Penal Code (IPC), Internet fraud would be covered by sections 415 to 420 which relates to 'cheating'. One is said to 'cheat' when he, fraudulently or dishonestly, induces another person to deliver any property to him by deceiving such person and which act causes damages or harm to the person deceived in body, mind, reputation or property.

If on the Internet, one is, by any of the numerous fraud schemes enumerated above, able to deceive a person so as to induce him to deliver any sum of money, it would be a case of 'cheating'. Section 416 of IPC deals with 'cheating by personation' that is *inter alia* cheating by pretending to be some other person. This covers 'phishing' as well.

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

1.7.8 Legal Provisions Regarding Cyber Terrorism

Section 66F of the IT Act (inserted vide ITAA 2008) deals with punishment for cyber terrorism. It provides a punishment of life imprisonment for a person who threatens unity, integrity, security or sovereignty of India or to strike terror in the people via cyber terrorism. That person may deny access of a computer resource to an authorized person or access a computer resource without or beyond authorization. He may introduce computer contaminant that may cause death or injuries to persons, damage property or disrupt supplies or services. He may gain access to restricted data that may threaten the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality; or cause contempt of court, defamation or incitement to an offence.

1.7.9 Legal Provisions Regarding Identity Theft

Section 66C of the IT Act (inserted vide ITAA 2008) contains provisions regarding punishment for identity theft. As per this section, if someone fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, then it is punishable by imprisonment up to 3 years and fine up to ₹ 1 lakh.

1.7.10 Legal Provisions on Cyber Extortion

In the case of the two Indian companies who paid $10 million, extortionist hackers avoided being reported as the information they accessed (and threatened to expose) could implicate their victims in wrongdoing, naturally prompting a silent payoff. Hence, even criminals engaging in digital extortion from within India, are likely to escape prosecution under existing laws due to the complexity of ascertaining identity of the perpetrators. However, if they are identified, they may be prosecuted for the offences of extortion and criminal intimidation under sections 383 and 503 of the Indian Penal Code read along with the provisions under the IT Act.

Section 383 of the IPC deals with extortion. It says:

Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits "extortion".

Section 503 of the IPC deals with criminal intimidation. It says:

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

1.7.11 Legal Provisions Regarding Intellectual Property Theft

The following legal provisions regarding intellectual property are available:

1.7.11.1 Copyright Protection

The Copyright Act, 1957, as amended in 1983, 1984, 1992, 1994 and 1999, governs the copyright protection in India. Computer programs and software are covered under literary works and are protected in India under copyrights. The total term of protection for literary work is the author's life plus 60 years. For cinematographic films, records, photographs, post-humous publications, anonymous publication, works of government and international agencies, the term is 60 years from the beginning of the calendar year following the year in which the work was published. For broadcasting, the term is 25 years from the beginning of the calendar year following the year in which the broadcast was made.

Copyright gives the creator of the work the right to reproduce the work, make copies, translate, adapt, sell or give on hire and communicate the work to the public. Any of these activities done without the consent of the author or his assignee is considered infringement of the copyright. There is a provision of "fair use" in the law, which allows copyrighted work to be used for teaching and research and development. In other words, making one photocopy of a book for teaching students may not be considered an infringement, but making many photocopies for commercial purposes would be considered an infringement. There is one associated right with copyright, which is known as the "moral right," which cannot be

transferred and is not limited by the term. This right is enjoyed by the creator for avoiding obscene representation of his/her works.

The owner of the copyright in an existing work or prospective owner of the copyright in a future work may assign to any person the copyright, either wholly or partially.

1.7.11.2 Patent Protection

The first Indian patent laws were promulgated in 1856. These were modified from time to time. New patent laws were made after the independence in the form of the Indian Patent Act, 1970. The Act has now been radically amended to become fully compliant with the provisions of the agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS. The most recent amendments were made in 2000, 2003 and 2005.

As per the amended Act of 2005, an invention will be considered novel if it does not form a part of the global state-of-the-art. A patent application involves an inventive step if the proposed invention is not obvious to a person skilled in the art, *i.e.*, skilled in the subject matter of the patent application. An invention must possess utility for the grant of patent. No valid patent can be granted for an invention devoid of utility.

Computer programs *per se* have not been defined in the Copyright Act but would generally tend to mean that a computer program without any utility would not be patentable. Topography of integrated circuits is protected through The Semiconductor Integrated Circuits Layout Design Act, 2000. Protection of seeds and new plant varieties is covered under the Protection of Plant Variety and Farmers Right Act, 2001 (PPVFR Act).

The term of the patent is 20 years from the date of filing for all types of inventions.

1.7.11.3 Trade Secrets Protection

In India, there are certain laws regarding every forms of Intellectual Property expect trade secrets. There is no specific legislation in India to protect trade secrets and confidential information. All member countries of TRIPS except India have already laws for the protection of trade secrets. So, the situation becomes even more challenging in the Internet era. This is because, the access to the secret information becomes easy with the new technology. The file which is stored in computer network may be encrypted, password protected and it is restricted to employees on a need-to-know basis. If an employee wants to access those information from computer network, then he could easily download it, email it, post it on internet or simply save it on a flash drive and walk out the front door undetected with thousands of information in his hand. The digital world is no friend to trade secrets. Nowadays, hackers break into networks and get confidential information of a company including trade secrets in such a manner which is not expected by anyone.

Trade secrets are protected in India under section 27 of the Indian Contract Act, 1872, which provides for remedies and also restrict any person from disclosing any information which he acquires at the time of employment or through contract. But in this provision, there is only civil remedy and no criminal remedies. According to this section, any information must be highly confidential to be constituted as trade secret. There are few criteria for deciding that whether any information amounts to trade secret or not, *i.e.*,

- The status of the employee and nature of his work.
- The nature of information itself.
- Whether the information could easily be isolated from other information which the employee was free to use.

Despite legislative limitations, Indian courts have upheld trade secret protection on the basis of principles of equity, and at times, upon a common law action of breach of confidence, which in effect amounts a breach of contractual obligation. The remedies available to the owner of trade secrets is to obtain an injunction preventing the licensee from disclosing the trade secret, return of all confidential and proprietary information and compensation for any losses suffered due to disclosure of trade secrets.

In India, a person can be contractually bound not to disclose any information that is revealed to him/her in confidence. The Indian courts have upheld a restrictive clause in a technology transfer agreement, which imposes negative covenants on licensee not to disclose or use the information received under the agreement for any purpose other than that agreed in the said agreement. The Delhi High Court in John Richard Brady and Others v. Chemical Process Equipments P. Ltd. and Anr [AIR 1987 Delhi 372] invoked a wider equitable jurisdiction and awarded injunction even in the absence of a contract.

1.7.11.4 Trademark Protection

Enactment of the Trademarks Act, 1999 is a big step forward from the Trade and Merchandise Marks Act 1958 and the Trademark Act, 1940. As per section 18(1) of the Trademark Act, 1999, any person claiming to be the proprietor of a trademark used or proposed to be used by him may apply in writing in prescribed manner for registration. The application must contain the name of the mark, goods and services, class in which goods and services fall, name and address of the applicant, period of use of the mark, etc.

Under section 29 of the Trademark Act, 1999, the use of a trademark by a person who not being registered proprietor of the trademark or a registered user thereof which is identical with, or deceptively similar to a registered trademark amounts to the infringement of trademark and the registered proprietor can take action or obtain relief in respect of infringement of trademark. "In a matter Supreme Court has held that in an action for infringement if the two marks are identical, then the infringement made out, otherwise the Court has to compare the two marks, the degree of resemblance by phonetic, visual or in the basic ides represented by the registered proprietor, whether the essential features of the mark of the registered proprietor is to be found used by other person than only the Court may conclude the matter."

Passing off is a common law tort used to enforce unregistered trademark rights.

Registration of a trademark is not a pre-requisite in order to sustain a civil or criminal action against violation of trademarks in India. In India, a combined civil action for infringement of trademark and passing off can be initiated. Significantly, infringement of a trademark is a cognizable offence and criminal proceedings can be initiated against the infringers. Such enforcement mechanisms are expected to boost the protection of marks in India and reduce infringement and contravention of trademarks.