Vidyalankar Institute of Technology

# INFORMATION TECHNOLOGY ACT RATHER THAN GIVING INFORMATION AND TECHNOLOGY GIVES RISE TO MORE CYBER CRIME

**Submitted by**

**Jagadesh 02, Snehal 04, Sairam 06, Saurabh 08, Arun 10, Mayuresh C 12, Ritesh 14, Amey 16, Yogesh 18, Pritam 20**

**MMS Batch II | Group 1**

**2012**

# INTRODUCTION

"Information technology", in a broad sense, connotes that technology which is connected with information. More particularly, it connotes that technology which has taken shape during the last five decades or so, involving electronics. The use of such technology for the storage, retrieval and dissemination of information has given rise to several legal, social and ethical problem. In this context , the word "information "is not to be taken as limited to news or information material. Rather, it is to be understood as encompassing all matter that is intended to be recorded electronically, whether it to be correspondence, government documents, legal instrument, private exchanges of news and views or any other matter which emanates from man and is transformed into machine – recorded data.

## LEGAL PROBLEMS – THEIR NATURE AND DIMENSIONS

Information technology gives rise to a variety of legal problems. The problems themselves are not novel, in their essentials character. But they deserve special treatment, because of the environment in which they take their birth and the nature of the machinery used in the environment and the means employed for recording the information in question. Traditional documents are stored and transmitted through the use of visible and tangible latters, figures and marks, while information which is stored and transmitted electronically, has no visible shape or tangible form. It is this peculiarity of the technology, that gives rise to a variety of legal problems. These problems can be generally resolved on principles already known to the legal systems. But in view of their subject matter, they may necessitate some adjustments in, and additions to, the content of the law.

### The machine, the medium and message

The majority of the legal problems that arise in this sphere are relatable to the following components of information technology, namely –

(a)The machine (i.e. The instrument used in the technology)

(b)The medium used for the purpose (i.e. Symbols and, other means, used for recording and transmitting the information) and

(c)The message i.e. The information which is stored or transmitted, through the above medium.

A few illustrations will make the matter clear.

First, so far as the computers are concerned, they can be tampered with, and made to give out results that were never intended. The law has therefor to concern itself with question whether any, and if so, what additional provisions, are needed, to deal with aspects.

Secondly, there is the question of the medium. Communications with the assistance of information technology – particularly through the internet – cross the borders of various countries. They are transnational in character and raise, inter alia, problems of jurisdiction. Besides this, the medium by which information is recorded – i.e. The operational symbols – are radically different, from the means employed in traditional writing or printing. Traditional means, such as letters, numerals or punctuation marks, are not put into the computer in their original form (through they do come out in the final print out, in traditional form).

Finally, as regards the message transmitted through information technology, there are certain special issues that fail to be considered. No doubt, the print – out the issues from computer is not substantially different from typed matter. But matter put on the internet may, by reason of its content, come into conflict with the law of the country where it emanates or the law of the country where it is received. How far, is each of these countries legally eqipped, to eal with such infringement? The answer to this question will depend on the substance of the laws of the country concerned. If the contravention is to be examined from the point of view of the criminal law, the exact text of the penal statute becomes material.

## The Legal Responses

For dealing with issues of the nature mentioned above (as arising out of the use ok information technology), some countries have enacted specific legislation. In India, the information technology Act 2000, is an example of such legislation. However, in the absence of specific legislation, or in regard to matters not covered by such specific legislation, the legal problems that arise will be governed by general principles of law – which are often referred to as principles of "common law".

## The Uncondified Law

These principles belong to the uncondified law of India. For example, if X sends out, on the internet, message that are dafamatory of Y, then (apart from instituting a criminal prosecution) Y has the right to sue for damages for defamation, which is a tort (a species of a civil wrong, independent of contract).Such a remedy is available to Y, under the law of torts, which is mostly

based upon judicial decisions dealings with various kinds of civil wrongs. In such matter, the information Technology Act 2000, would not supply a complete answer.

# THE INFORMATION TECHNOLOGY ACT – ITS ROLE

With regards to matters which are dealt with in the information Technology Act 2000, its specific provisions will apply. But a few observations have to be made in this context. The first is, that besides the information Technology Act, there are other statutory provisions ( as contained in certain other Acts), which are also relevant to information technology. In fact, regarding some of these Acts, the Information Technology Act itself has effected specific amendments. These include, the Indian Panel Code, the Indian Evidence Act , 1872, the bankers' Book Evidence Act , 1891 and the Reserve Bank of India Act 1934.

Secondly, even before the information Technology Act,2000, came into force, Parliament had provided for the maintenance of computerized records, by amending the legislation in force relating to customs, excise and companies.

Thirdly, as pointed out above, many legal issues arising out of the use of information technology will continue to be dealt with, by common law rules. Torts are an outstanding example. Thus, it can be said that a study of information technology Law has to begin with a study of the Information Technology Act, 2000, but cannot end with it.

# MAIN OBJECT AND GENERAL SCHEME OF THE ACT

The information Technology Act, 2000 (Central Act 21 of 2000), was enacted to make, in the main, three kinds of provisions, as under :

(a) It provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronis communications, usually referred to, as "electronic Commerce".
(b) It facilitates the electronic filling of documents with the Governement agencies,(and also with the publication of rules etc in the electronic form, see Section 8)
(c) It amends the, Indian Penal Code, the indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1981, and reserve Bank of India Act, 1934, so as to bring in electronic documentation within the purview of the repective enactment.

The Act comprises of 94 Sections, spread out amongst 13 Chapters followed by four Schedules. The topics dealt with in the main Act are as under :

1. Preliminary matters
2. Digital signatures
3. Electronis governance
4. Electronic records
5. Secure electronic records and secure digital signatures
6. Certifying authorities
7. Digital signature certificates
8. Duties of subscriber
9. Penalties and adjudication
10. The cyber regulations appellate Tribunal
11. Offences
12. Immunity of net work services providers in certain cases
13. Miscellaneous

The four Schedules annexed to the Act set out the amendments made in Four Central Acts, so as to weave, into their fabric, the concepts of electronics records. The four Acts are –

(a) The Indian Panel code
(b) The Indian evidence Act, 1872
(c) The bankers' Book Evidence Act, 1891
(d) The Reserve Bank of India Act, 1934

# WHAT IS CYBERCRIME?

The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cybercrime – illegal activitiy committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spams, software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

– National Research Council, "Computers at Risk", 1991

What is Cyber crime? We read about it in newspapers very often. Let's look at the dictionary definition of Cybercrime: "It is a criminal activity committed on the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money".

Cybercrimes can be basically divided into 3 major categories:

1. Cybercrimes against persons.
2. Cybercrimes against property.
3. Cybercrimes against government.

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

A minor girl in Ahmedabad was lured to a private place through cyberchat by a man, who, along

with his friends, attempted to gangrape her. As some passersby heard her cry, she was rescued.

Another example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide.

In the United States alone, the virus made its way through 1.2 million computers in one-fifth of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug".

Cyber harassment is a distinct Cybercrime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes.

Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyberspy.

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

In a report of expressIndia.com, it was said that internet was becoming a boon for the terrorist organizations. According to Mr. A.K. Gupta, Deputy Director (Co-ordination), CBI, terrorist outfits are increasingly using internet to communicate and move funds. "Lashker-e-Toiba is collecting contributions online from its sympathisers all over the world. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathisers and also using the medium for intra-bank transfer of funds".

Cracking is amongst the gravest Cyber-crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

Coupled with this the actuality is that no computer system in the world is cracking proof. It is unanimously agreed that any and every system in the world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of Cyber-crimes which are slowly emerging as being extremely dangerous.

**Unauthorized access**

Using one's own programming abilities as also various programmes with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programmes which do irreparable damage to computer systems is another kind of Cybercrime. Software piracy is also another distinct kind of Cybercrime which is perpetuated by many people online who distribute illegal and unauthorized pirated copies of software.

Professionals who involve in these cybercrimes are called crackers and it is found that many of such professionals are still in their teens. A report written near the start of the Information Age warned that America's computers were at risk from crackers. It said that computers that "control (our) power delivery, communications, aviation and financial services (and) store vital information, from medical re-cords to business plans, to criminal records", were vulnerable from many sources, including deliberate attack.

**"Script-kiddies"**

Crackers do more than just spoiling websites. Novices, who are called "script-kiddies" in their circles, gain "root" access to a computer system, giving them the same power over a system as an administrator – such as the power to modify features. They cause damage by planting viruses.

The Parliament of India passed its first Cyber Law, the Information Technology Act in 2000. It not only provides the legal infrastructure for E-commerce in India but also at the same time, gives draconian powers to the Police to enter and search, without any warrant, any public place for the purpose of nabbing cybercriminals and preventing cybercrime. Also, the Indian Cyber Law talks of the arrest of any person who is about to commit a cybercrime.

The Act defines five cyber-crimes – damage to computer source code, hacking, publishing electronic information which is lascivious or prurient, breach of confidentiality and publishing false digital signatures. The Act also specifies that cybercrimes can only be investigated by an official holding no less a rank than that of Dy. Superintendent of Police.

The Act simply says "Notwithstanding anything contained in any other law for the time being in force, any Police Officer not below the rank of Dy.SP may enter, search and arrest any person without search warrant in any public place who he thinks is committing or about to commit a cybercrime".

It is common that many systems operators do not share information when they are victimized by crackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep crackers from gaining access again with as little public attention as possible.

According to Sundari Nanda, SP, CBI, "most of the times the victims do not complain, may be because they are aware of the extent of the crime committed against them, or as in the case of business houses, they don't want to confess their system is not secure".

As the research shows, computer crime poses a real threat. Those who believe otherwise simply have not been awakened by the massive losses and setbacks experienced by companies worldwide. Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime.

Similarly, information systems in government and business alike have been compromised. The economic impact of computer crime is staggering.

**Cyberspace**

As the cases of cybercrime grows, there is a growing need to prevent them. Cyberspace belongs to everyone. There should be electronic surveillance which means investigators tracking down hackers often want to monitor a cracker as he breaks into a victim's computer system. The two basic laws governing real-time electronic surveillance in other criminal investigations also apply in this context, search warrants which means that search warrants may be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime.

There should also be analyzing evidence from a cracker's computer by the officials investigating the crime. A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer.

Researchers must explore the problems in greater detail to learn the origins, methods, and motivations of this growing criminal group. Decision-makers in business, government, and law enforcement must react to this emerging body of knowledge. They must develop policies, methods, and regulations to detect incursions, investigate and prosecute the perpetrators, and prevent future crimes. In addition, Police Departments should immediately take steps to protect their own information systems from intrusions.

Internet provides anonymity: This is one of the reasons why criminals try to get away easily when caught and also give them a chance to commit the crime again. Therefore, we users should be careful. We should not disclose any personal information on the internet or use credit cards and if we find anything suspicious in e-mails or if the system is hacked, it should be immediately reported to the Police officials who investigate cyber-crimes rather than trying to fix the problem by ourselves.

Computer crime is a multi-billion dollar problem. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cybercrime is a menace that has to be tackled effectively not only by the official but also by the users by co-operating with the

law. The founding fathers of internet wanted it to be a boon to the whole world and it is upon us to keep this tool of modernization as a boon and not make it a bane to the society.

# PREVENTIVE MEASURES

**a. Criminals Can Operate Anonymously Over the Computer Networks.**

1. Be careful about talking to "strangers" on a computer network. Who are these people anyway? Remember that people online may not be who they seem at first. Never respond to messages or bulletin board items that are: Suggestive of something improper or indecent; Obscene, filthy, or offensive to accepted standards of decency; Belligerent, hostile, combative, very aggressive; and Threaten to do harm or danger towards you or another

2. Tell a grown-up right away if you come across any information that makes you feel uncomfortable.

3. Do not give out any sensitive or personal information about you or your family in an Internet "chat room." Be sure that you are dealing with someone you and your parents know and trust before giving out any personal information about yourself via e-mail.

4. Never arrange a face-to-face meeting without telling your parents or guardians. If your parent or guardian agrees to the meeting, you should meet in a public place and have a parent or guardian go with you.

**b. Hackers Invade Privacy**

1. Define a hacker –
A hacker is someone who breaks into computers sometimes to read private e-mails and other files.

2. What is your privacy worth? What information about you or your parents do you think should be considered private?

For example, medical information, a diary, your grades, how much money your parents owe, how much money your family has in a savings account or in a home safe, and your letters to a friend. Would this kind of invasion of your privacy be any different than someone breaking into your school locker or your house to get this information about you and your family?

**c. Hackers Destroy "Property" in the Form of Computer Files or Records**

1. Hackers delete or alter files.

2. When you write something, like a term paper or report, how important is it to be able to find it again? Would this be different if someone broke into your locker and stole your term paper?

3. How important is it that data in computers like your term paper, a letter, your bank records, and medical records, not be altered? How important is it for a drug company or a pharmacy to not have its computer files altered or deleted by hackers? What would happen if a hacker altered the chemical formulas for prescription drugs, or the flight patterns and other data in air traffic control computers? What does the term "tamper" mean? To interfere in a harmful way or to alter improperly. Is tampering with computer files different from tampering that occurs on paper files or records?

**d. Hackers Injure Other Computer Users by Destroying Information Systems**

1. Hackers cause victims to spend time and money checking and rescuing systems after break-in. They also cause them to interrupt service. They think its fine to break-in and snoop in other people's files as long as they don't alter anything. They think that no harm has been done.

2. Hackers steal telephone and computer time and share unauthorized access codes and passwords. Much of the stealing is very low-tech. "Social engineering" is a term used among crackers for cracking techniques that rely on weaknesses in human beings rather than on software. "Dumpster diving" is the practice of sifting refuse from an office or technical installation to extract confidential data, especially security compromising information. Who do you think pays for this? How much stealing of computer time do you thinks there is? For
example, there is $2 billion annually in telephone toll fraud alone. Would you want someone going through your garbage? Have you ever thrown away private papers or personal notes?

3. Hackers crash systems that cause them to malfunction and not work. How do we use computer information systems in our daily lives? What could happen if computers suddenly stopped working? For example, would public health and safety be disrupted and lives are endangered if computers went down?

**e. Computer "Pirates" Steal Intellectual Property**

1. Intellectual property is the physical expression of ideas contained in books, music, plays, movies, and computer software. Computer pirates steal valuable property when they copy software, music, graphics/pictures, movies, books (all available on the Internet).

2. How is the person who produced or developed these forms of entertainment harmed? Is this different from stealing a product (computer hardware) which someone has invented and manufactured? Who pays for this theft?

3. It may seem simple and safe to copy recordings, movies and computer programs by installing a peer-to-peer (P2P) file sharing software program. However, most material that you may want to copy is protected by copyright which means that you are restricted from making copies unless you have permission to do so. Making copies of intellectual property including music, movies and software--without the right to do so is illegal. P2P software and the files traded on the P2P networks may also harm your computer by installing viruses or spy ware, or allow others to access the files contained on your hard drive beyond those you intend to share.

4. Copyright violations have civil and criminal remedies.

a. **Civil remedy:** copyright holder can sue infringer for money to cover loss of sales or other loss caused by infringement.

b. **Criminal remedy:** jail or fine paid to the government (not copyright holder) where person infringes a copyright for commercial advantage or private gain. For example, a person who makes multiple copies of a video, and sell the copies.

# TYPES OF CYBER CRIME

Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

**Financial crimes**

This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

**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). Recent Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken. In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple for pornography.

**Sale of illegal articles**

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication.

E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

**Phishing**

In computing, phishing (also known as carding and spoofing) is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords.

**Online gambling**

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

**Intellectual Property crimes**

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

**Email spoofing**

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Pooja has an e-mail address pooja@asianlaws.org. Her enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

**Forgery**

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and

high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

**Cyber Defamation**

This occurs when defamation takes place with the help of computers and or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

**Cyber stalking**

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Frequently Used Cyber Crimes Unauthorized access to computer systems or networks

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". Theft of information contained in electronic form

This includes information stored in computer hard disks, removable storage media etc

**Email bombing**

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Some of the major email related crimes are:

1. Email spoofing
2. Sending malicious codes through email
3. Email bombing
4. Sending threatening emails
5. Defamatory emails
6. Email frauds

**Data diddling**

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

**Salami attacks**

These attacks are 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.

**Denial of Service attack**

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash.

**Virus / worm attacks**

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory

**Logic bombs**

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date

**Trojan attacks**

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

**Internet time thefts**

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In a case reported before the enactment of the Information Technology Act, 2000 Colonel Bajwa, a resident of New Delhi, asked a nearby net caf owner to come and set up his Internet connection. For this purpose, the net caf owner needed to know his username and password.

After having set up the connection he went away with knowing the present username and password. He then sold this information to another net cafe. One week later Colonel Bajwa found that his Internet hours were almost over. Out of the 100 hours that he had bought, 94 hours had been used up within the span of that week. Surprised, he reported the incident to the Delhi police. The police could not believe that time could be stolen. They were not aware
of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested the net café owner under the charge of theft as defined by the Indian Penal Code. The net cafe owner spent several weeks locked up in Tihar jail before being granted bail.

**Web jacking**

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website in a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained
control over her website.

**Theft of computer system**

This type of offence involves the theft of a computer, some parts of a computer or a peripheral attached to the computer. Physically damaging a computer system. This crime is committed by physically damaging a computer or its peripherals.

# CYBER CRIMINALS

**Kids (age group 9-16 etc.)**

It seems really difficult to believe but it is true. Most amateur hackers and cyber criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride to have hacked into a computer system or a website. There is also that little issue of appearing really smart among friends. These young rebels may also commit cybercrimes without really knowing that they are doing anything wrong.

**Organized hacktivists**

Hacktivists are hackers with a particular (mostly political) motive. In other cases this reason can be social activism, religious activism, etc. The attacks on approximately 200 prominent Indian websites by a group of hackers known as Pakistani Cyber Warriors are a good example of political hacktivists at work.

**Disgruntled employees**

One can hardly believe how spiteful displeased employees can become. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire
systems down.

**Professional hackers (corporate espionage)**

Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needless if hacking can retrieve those.

**Denial of Service Tools**

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. Usually these attacks do not necessitate the need to get access into anyone's system.

These attacks have been getting decidedly more popular as more and more people realize the amount and magnitude of loss, which can be caused through them.

What are the reasons that a hacker may want to resort to a DoS attack? He may have installed a Trojan in the victim's computer but needed to have the computer restarted to activate the Trojan. The other good reason also may be that a business may want to harm a competitor by crashing his systems.

Denial-of-service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo and eBay. The attack is initiated by sending excessive demands to the victim's computer's, exceeding the limit that the victim's servers can support and making the server's crash. Sometimes, many computers are entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer. On the other side, the victim of such an attack may see many such demands (sometimes even numbering tens of thousands) coming from computers from around the world. Unfortunately, to be able to gain control over a malicious denial-of service attack would require tracing all the computers involved in the attack and then informing the owners of those systems about the attack. The compromised system would need to be shut down or then cleaned. This process, which sounds fairly simple, may prove very difficult to achieve across national and later organizational borders.

Even when the source(s) of the attack are traced there are many problems, which the victim may be faced with. He will need to inform all the involved organizations in control of the attacking computers and ask them to either clean the systems or shut them down. Across international boundaries this may prove to be a titanic task. The staff of the organization may not understand the language. They may not be present if the attack were to be launched during the night or during weekends.

The computers that may have to be shut down may be vital for their processes and the staff may not have the authority to shut them down. The staff may not understand the attack, system administration, network topology, or any number of things that may delay or halt shutting down the attacking computers. Or, more simply, the organization may not have the
desire to help.

If there are hundreds or even thousands of computers on the attack, with problems like the ones mentioned above, the victim may not be able to stop the attack for days by which time the damage would have been done. His servers would be completely incapacitated to administer to so many demands and consequently would crash. It is very simple for anyone to launch an attack because denial-of service tools can easily be procured from the Net. The major versions of distributed denial of service attack tools are Trinoo (or trin00), TFN, TFN2K and Stacheldraht. Denial-of-Service tools allow the attackers to automate and preset the times and frequencies of such attacks so that the attack is launched and then stopped to be launched once again later. This makes it very difficult, in fact almost impossible, to trace the source of the attack.

These tools also provide another service by which the attacking computer can change its source address randomly thereby making it seem as if the attack is originating from many thousands of computers while in reality there may be only a few. Distributed denial-of-service attacks are a very perturbing problem for law enforcement agencies mainly because they are very difficult to trace. In addition, usually these attacks are directed towards very sensitive systems or networks sometimes even those that are vital to national security. Sometimes, even when the perpetrators can be traced, international extradition laws may prove to be a hitch in bringing them under the authority of the law.

As seen above that how the cybercrime have been escalating in the India and the damage it can do to a company, hence to protect the importance of privacy of a company the government of India realized the significance to create a governance to regulate and keep a tab on the activity of cybercrime. The main aim to create the **Information Technology Act 2000** was to safeguard a business organization from cybercrime.

# INFORMATION TECHNOLOGY ACT 2000

Connectivity via the Internet has greatly abridged geographical distances and made communication even more rapid. While activities in this limitless new universe are increasing incessantly, laws must be formulated to monitor these activities. Some countries have been rather vigilant and formed some laws governing the net. In order to keep pace with the changing generation, the Indian Parliament passed the much-awaited Information Technology Act, 2000 .As they say, **"Its better late than never".**

However, even after it has been passed, a debate over certain controversial issues continues. A large portion of the industrial community seems to be dissatisfied with certain aspects of the Act. But on the whole, it is a step in the right direction for India.

**The Information Technology Act 2000,** regulates the transactions relating to the computer and the Internet.

The objectives of the Act as reflected in the Preamble to the Act are:

1. The Preamble to the Act states that it aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and aims at
facilitating electronic filing of documents with the Government
agencies.

2. To facilitate electronic filing of the document with the government of India. The General Assembly of the United Nations had adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its General Assembly Resolution A/RES/51/162 dated January 30, 1997. The Indian Act is in keeping with this resolution that recommended that member nations of the UN enact and
modify their laws according to the Model Law. Thus with the enactment of this Act, Internet transactions will now be recognized, on-line contracts will be enforceable and e-mails will be legally acknowledged. It will tremendously augment domestic as well as international trade and commerce. The Infromation Technology Act extends to the **whole of India** and, save as **otherwise**

**provided in this Act**, it applies also to any offence or contravention thereunder committed outside India by any person.

However The Act does not apply to:

1. A negotiable instrument as defined in section 13 of the Negotiable Instruments Act,1881;
2. A power-of-attorney as defined in section 1A of the Powers-of- Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trusts Act, 1882;
4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925including any other testamentary disposition by whatever name called;
5. Any contract for the sale or conveyance of immovable property or any interest insuch property;
6. Any such class of documents or transactions as may be notified by the CentralGovernment in the Official Gazette.

**Some of the Important Definition:**

1. "**Adjudicating officer**" means an adjudicating officer appointed under subsection of section 46;

2. "**Affixing digital signature**" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

3. "**Appropriate Government**" means as respects any matter,—
(i) Enumerated in List II of the Seventh Schedule to the Constitution;
(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

4. "**Asymmetric crypto system**" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

5. "**Certifying Authority**" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

6. "**Certification practice statement**" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

7. "**Cyber Appellate Tribunal**" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

8. "**Digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

9. "**Digital Signature Certificate**" means a Digital Signature Certificate issued under subsection of section 35;

10. "**Electronic form**" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

11. "**Electronic Gazette**" means the Official Gazette published in the electronic form;

12. "**Secure system**" means computer hardware, software, and procedure that—
(a) are reasonably secure from unauthorised access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures;

**Legitimacy and Use of Digital Signatures**

The Act has adopted the Public Key Infrastructure for securing electronic transactions. As per Section 3 of the Act, a digital signature means an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act. Thus a subscriber can authenticate an electronic record by affixing his digital signature. A private key is used to create a digital signature whereas a public key is used to verify the digital signature and electronic record. They both are unique for each subscriber and together form a functioning key pair. Section 5 provides that when any information or other matter needs to be authenticated by the signature of a person, the same can be authenticated by means of the digital signature affixed in a manner prescribed by the Central Government.

Under Section 10, the Central Government has powers to make rules prescribing the type of digital signature, the manner in which it shall be affixed, the procedure to identify the person affixing the signature, the maintenance of integrity, security and confidentiality of electronic records or

payments and rules regarding any other appropriate matters. Furthermore, these digital signatures are to be authenticated by Certifying Authorities (CA's) appointed under the Act. These authorities would inter alias; have the license to issue Digital Signature Certificates (DSC's). The applicant must have a private key that can create a digital signature. This private key and the public key listed on the DSC must form the functioning key pair.

Once the subscriber has accepted the DSC, he shall generate the key pair by applying the security procedure. Every subscriber is under an obligation to exercise reasonable care and caution to retain control of the private key corresponding to the public key listed in his DSC. The subscriber must take all precautions not to disclose the private key to any third party. If
however, the private key is compromised, he must communicate the same to the Certifying Authority (CA) without any delay.

**Writing requirements**

Section 4 of the Act states that when under any particular law, if any information is to be provided in writing or typewritten or printed form, then notwithstanding that law, the same information can be provided in electronic form, which can also be accessed for any future reference. This nonobstinate provision will make it possible to enter into legally binding
contracts on-line!

**Attribution, Acknowledgement and Dispatch of Electronic Records**

Explicates the manner in which electronic records are to be attributed, acknowledged and dispatched. These provisions play a vital role while entering into agreements electronically.
Section 11 states that an electronic record shall be attributed to the originator as if it was sent by him or by a person authorized on his behalf or by an information system programmed to operate on behalf of the originator.

As per Section 12, the addressee may acknowledge the receipt of the electronic record either in a particular manner or form as desired by the originator and in the absence of such requirement, by communication of the acknowledgement to the addresses or by any conduct that would sufficiently constitute acknowledgement. Normally if the originator has stated that the electronic record will be binding only on receipt of the acknowledgement, then unless such acknowledgement is received, the record is not binding. However, if the acknowledgement is not received within the stipulated time period or in the absence of the time period, within a reasonable time, the originator may notify

the addressee to send the acknowledgement, failing which the electronic record will be treated as never been sent.

Section 13 specifies that an electronic record is said to have been dispatched the moment it leaves the computer resource of the originator and said to be received the moment it enters the computer resource of the addressee.

**Utility of electronic records and digital signatures in Government Audits Agencies**

According to the provisions of the Act, any forms or applications that have to be filed with the appropriated Government office or authorities can be filed or any license, permit or sanction can be issued by the Government in an electronic form. Similarly, the receipt or payment of money can also take place electronically.

Moreover, any documents or records that need to be retained for a specific period may be retained in an electronic form provided the document or record is easily accessible in the same format as it was generated, sent or received or in another format that accurately represents the same information that was originally generated, sent or received. The details of the origin, destination, date and time of the dispatch or receipt of the record must also be available in the electronic record. Furthermore, when any law, rule, regulation or byelaw has to be published in the Official Gazette of the Government, the same can be published in electronic form. If the same are published in printed and electronic form, the date of such publication will be the date on which it is first published.

However, the above-mentioned provisions do not give a right to anybody to compel any Ministry or Department of the Government to use electronic means to accept issue, create, retain and preserve any document or execute any monetary transaction. Nevertheless, if these electronic methods are utilized, the Government will definitely save a lot of money on paper!

**Regulation of Certifying Authorities (CAs)**

A CA is a person who has been granted a license to issue digital signature certificates. These CAs are to be supervised by the Controller of CAs appointed by the Central Government. Deputy or Assistant Controllers may also assist the Controller. The Controller will normally regulate and monitor the activities of the CAs and lay down the procedure of their conduct.

The Controller has the power to grant and renew licenses to applicants to issue DSCs and at the same time has the power to even suspend such a license if the terms of the license or the provisions

of the Act are breached. The CAs has to follow certain prescribed rules and procedures and must comply with the provisions of the Act.

**Issuance, Suspension and Revocation of Digital Signature Certificates (DSCs)**

As per Section 35, any interested person shall make an application to the CA for a DSC. The application shall be accompanied by filing fees not exceeding Rs. 25,000 and a certification practice statement or in the absence of such statement; any other statement containing such particulars as may be prescribed by the regulations. After scrutinising the application, the CA may either grant the DSC or reject the application furnishing reasons in writing for the same.

While issuing the DSC, the CA must inter alias, ensure that the applicant holds a private key which is capable of creating a digital signature and corresponds to the public key to be listed on the DSC. Both of them together should form a functioning key pair.

The CA also has the power to suspend the DSC in public interest on the request of the subscriber listed in the DSC or any person authorised on behalf of the subscriber. However, the subscriber must be given an opportunity to be heard if the DSC is to be suspended for a period exceeding fifteen days. The CA shall communicate the suspension to the subscriber. There are two cases in which the DSC can be revoked. Firstly, as per Section 38 (1), it may be revoked either on the request or death of the subscriber or when the subscriber is a firm or company, on the dissolution of the firm or winding up of the company. Secondly, according to Section 38(2), the CA may sue moto revoke it if some material fact in the DSC is false or has been concealed by the subscriber or the requirements for issue of the DSC are not fulfilled or the subscriber has been declared insolvent or dead. A notice of suspension or revocation of the DSC must be published by the CA in a repository specified in the DSC.

**Penalties for Computer Crimes**

As per the Act, civil liability and stringent criminal penalties may be imposed on any person who causes damage to a computer or computer system. The offender would be liable to pay compensation not exceeding Rs. 1 Crore (10 million) for gaining unauthorized access to a computer or computer system, damaging it, introducing a virus in the system, denying access to an authorized person or assisting any person in any of the above activities. Furthermore, the Act also defines specific penalties for violation of its provisions or of any rules or regulations made there under. However, if any person contravenes any rules or regulations framed under the Act for which no specific penalty is prescribed, he will be liable to pay compensation not exceeding Rs. 25,000.

Moreover, any person who intentionally or knowingly tampers with computer source documents would be penalized with imprisonment up to three years or a fine of up to Rs. 2 lakhs or both. In simpler terminology, hacking is made punishable.

The Act also disallows the publishing and dissemination of obscene information and material. The introduction of this provision should curtail pornography over the net. Any person who disobeys this provision will be punishable with imprisonment of two years and a fine of Rs. 25,000 for the first conviction. In the event of a subsequent conviction, the imprisonment is five years and the fine doubles to Rs. 50,000. The Controller has the power to issue directions for complying with the provisions of the Act. Failure to comply with his directions is punishable. Moreover, the interference with protected systems or the reluctance to assist a Government Agency to intercept information in order to protect state sovereignty and security is also made punishable. The adjudicating court also has the powers to confiscate any computer, computer system, floppies, compact disks, tape drives or any accessories in relation to which any provisions of the Act are being violated. No penalty or confiscation made under this Act will affect the imposition of any other punishment under any other law in force. If penalties that are imposed under the Act are not paid, they will be recovered, as arrears of land revenue and the licence or DSC shall be suspended till the penalty is paid.

**Adjudicating Officers**

The Central Government shall appoint an officer not below the rank of Director to the Government of India or equivalent officer of the State Government as an adjudicating officer to adjudicate upon any inquiry in connection with the contravention of the Act. Such officer must have the legal and judicial experience as may be prescribed by the Central Government in that behalf.

The Adjudicating Officer must give the accused person an opportunity to be heard and after being satisfied that he has violated the law, penalize him according to the provisions of the Act. While adjudicating, he shall have certain powers of a Civil Court.

**Cyber Regulations Appellate Tribunal (CRAT)**

A Cyber Regulations Appellate Tribunal (CRAT) is to be set up for appeals from the order of any adjudicating officer. Every appeal must be filed within a period of forty-five days from the date on which the person aggrieved receives a copy of the order made by the adjudicating officer. The appeal must be the appropriate form and accompanied by the prescribed fee. An appeal may be

allowed after the expiry of forty-five days if sufficient cause is shown. The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal. The CRAT shall also have certain powers of a civil court.

As per Section 61, no court shall have the jurisdiction to entertain any matter that can be decided by the adjudicating officer or the CRAT. However, a provision has been made to appeal from the decision of the CRAT to the High Court within sixty days of the date of communication of the order or decision of the CRAT. The stipulated period may be extended if sufficient cause is shown. The appeal may be made on either any question of law or question of fact arising from the order.

**Police Powers**

A police officer not below the rank of deputy superintendent of police has the power to enter any public place and arrest any person without a warrant if he believes that a cybercrime has been or is about to be committed. This provision may not turn to be very effective for the simple reason that most of the cybercrimes are committed from private places such as one's own home or office. Cyber-cafés and public places are rarely used for cybercrimes. However, if the Act did give the police department powers to enter people's houses without search warrants, it would amount to an invasion of the right to privacy and create pandemonium. Keeping this in mind, the Legislature has tried to balance this provision so as to serve the ends of justice and at the same time, avoid any chaos.

On being arrested, the accused person must, without any unnecessary delay, be taken or sent to the magistrate having jurisdiction or to the officer in- charge of a police station. The provisions of the Code of Criminal Procedure, 1973 shall apply in relation to any entry, search or arrest made by the police officer.

**Network Service Providers not liable in certain cases**

To quote Section 78, it states: "For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation. For the purposes of this section,

(a) Network service provider means an intermediary;

(b) Third party information means any information dealt with by a network service provider in his capacity as an intermediary.

Thus a plain reading of the section indicates that if the network service provider is unable to prove its innocence or ignorance, it will be held liable for the crime.

**Possible Uses of E-Governance-**

The future of e-governance is very bright. With the help of information technology, the daily matters can be effectively taken care of irrespective of the field covered by it. For instance, the Delhi Police Headquarter has launched a website, which can be used for lodging a First Information Report. Similarly, the Patna High Court has taken a bold step of granting bail on the basis of an online bail application. The educational institutions, including universities, are issuing admission forms electronically, which can be downloaded from their respective websites. The results of examinations of various educational institutions, both school level and university level, are available online, which can be obtained without any trouble. These are but some of the instances of the use of technology for a better e-governance. The beneficial concept of e-governance can be utilized for the following purposes:

- To have access to public documents.
- For making online payments of various bills and dues.
- To file statutory documents online.
- To file the complaints, grievances and suggestions of citizens online.
- The online facility can be used to enter into a partnership the appropriate government in cases of government contracts.
- The citizens can use the online facility to file their income tax returns.
- The citizens will enjoy the facility of online services.

**Digital Signature**

Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure Rapid developments in e-business pose a growing need for online security and authentication. Many emerging technologies are being developed to provide online authentication. The major concern in e-business transactions is the need for the replacement of the hand-written signature with an online' signature. The traditional e-mail system, which has problems of message integrity and non-repudiation, does not fulfil the basic requirements for an online

signature. Further, since the Internet communication system is prone to various types of security breaches, the discussion of robust and authenticated e-business transactions is incomplete without consideration of 'security' as a prominent aspect of 'online signatures'.

One may consider an e-signature as a type of electronic authentication. Such authentication can be achieved by means of different types of technologies. A Digital Signature (DS) can be considered as a type of esignature, which uses a particular kind of technology that is DS technology. DS technology involves encrypting messages in such a way that only legitimate parties are able to decrypt the message. Two separate but interrelated 'keys' carry out this process of encryption and decryption. One party in the transactions holds the secret key, or the private key, and the other party holds the public key or the key with wide access. The selection and use of an encryption technique plays a crucial role in the design and development of keys. In short, a DS satisfies all the functions, such as authenticity, non-repudiation, and security, of a hand-written signature. Such a 'signature' can be viewed as a means of authentication and can be owned by an individual. While using this technology, there must be third party involvement order to handle the liability issues that may be raised by bilateral transactions. With this existing legal infrastructure and the rapid emergence of software security products, it is important to understand the role of emerging technologies like DS in e-business. One of the major indicators of technological improvements is the market development and commercialization of that technology.

# KEY TERMS

**Digital Signature**

A digital signature authenticates electronic documents in a similar manner a handwritten signature authenticates printed documents. This signature cannot be forged and it asserts that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient of a digitally signed message can verify that the message originated from the person whose signature is attached to the document and that the message has not been altered either intentionally or accidentally since it was signed. Also, the signer of a document cannot later disown it by claiming that the signature was forged. In other words, digital signatures enable the "authentication" and “non-repudiation” of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

A digital signature is issued by a Certification Authority (CA) and is signed with the CA's private key. A digital signature typically contains the: Owner's public key, the Owner's name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

If you file electronically using digital signature you do not have to submit a physical copy of the return. Even if you do not have a digital signature, you can still e-File the returns. However, you must also physically submit the printed copy of the filled up Form along with the copy of the Provisional Acknowledgement Number of your e-Return.]

India is one of the select band of nations that has the Digital Signature Legislation in place. This Act grants digital signatures that have been issued by a licensed Certifying Authority in India the same status as a physical signature. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

The Information Technology Act, 2000 provides for use of Digital Signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. Certification Agencies are appointed by the office of the Controller of Certification Agencies (CCA) under the provisions of IT Act, 2000. There are a total of seven Certification Agencies authorised by the CCA to issue the Digital Signature Certificates.

**Certifying authority**

**Cyber Laws: Need for Certifying Authority**

Hacking' and 'Cyber theft' are popular buzzwords on the Internet. Remember, most Internet security measures have to go beyond anti-virus, firewall, spy-ware and anti-malware programs and encompass many concepts that ordinary Internet users may not even think of. Most hackers are professionals. They know how to impersonate as legitimate online business entity. Then, they hack the visitors' information. Let's understand why this is done.

**Cyber Laws: How Unlawful Withdrawal or Misuse of Sums of Money Happens Online**

Numerous cyber law cases pertain to unlawful withdrawal of sums of money from online accounts without lawful consent and verification. This continues to happen on the Internet. Here is a simpler example to explain the concept.

Suppose, Mr X wants to transfer money online to his brother's account from his ABC bank account. He would encrypt his private key with the bank's public key. Now, the bank can decrypt the transaction with the secret key that it holds. However, Tom, a hacker, may act as an imposter and replace the bank's public key with his. So, when Mr X is decrypting his private key with a false key, Tom can extract Mr X's account information and re-encrypt Mr X's key with the bank's key. Such things happen so confidentially that neither Mr X nor the Bank are likely to detect that the transaction has been intercepted even if they are online.

For the same reason, it is not practical for companies to send their public key to their clients via courier, telephone or diskettes. This dilemma can be attributed to the tremendous increase in the number of clients that companies have to cater to on a daily basis.

Further, due to the incessant growth of the Internet, online communications are taking place multilaterally as well as bilaterally. As all the parties to the communication do not know each other, it becomes more difficult for companies and online consumers to communicate or conduct

transactions. This is where a certifying authority comes into the picture.

**Cyber Laws: What is a Certifying Authority and what does it do?**

In cyber laws, a Certifying Authority is an entity that is relied upon by both online businesses and their clients for securing communication. The Certifying Authority acts as a third party and issues digital signatures to businesses that are operating online. The authority vouches for the identity of these businesses and assures their clients on the issue of security. So, these clients, in turn, can share their personal information without worries. The information usually includes details such as the name, phone number, address, bank records, and credit/debit card number or medical records.

It is important to note that this information is traded between the parties in an encrypted form. Therefore, any disputes or legal issues pertaining to digital signatures are governed by the Information Technology Act, 2000, that was enacted by the Indian Parliament. In India, the IDRBT CA is an entity that issues certificates to the financial institutions and banks for RBI's PKI enabled applications including NEFT, PDO-NDS, RTGS and SFMS. This aspect fortifies an online buyer's confidence to go ahead with the online transactions using the secured keys.

**E commerce**

E-commerce has made an incredible journey from the financial industry to the dot.com 'bomb'. History tells us that our experiences with e-business are not new; other technological revolutions – such as E-Banking, E- Payments. Thus we require studying security aspects which are related to it and measure attached E-Risk, types of Cyber Crime. This paper reviews examines the origins of e-commerce, identifies e-risks, describes retail trade on the Internet, defines virtual business, identifies aspects of website design, and describes types of cyber crime that hamper e-commerce.

Electronic commerce, also called e-commerce, is increasing around the globe. E- commerce mostly consists of electronic business transactions related to the purchase and delivery of goods and services. . Some people define e-commerce as including only transactions that involve the electronic transfer of money; however, e-commerce is generally regarded as including any electronic transaction concerning a purchase by check, phone, or some other means. E-commerce includes retail trade between business and consumers (B2C) as well as business-to-business (B2B) trade. Businesses use the Internet, extranets, or electronic data interchange (EDI) in carrying out e-commerce. E-commerce is now being used in all types of business, including manufacturing companies, retail stores, and service firms. E-commerce has made business processes more

reliable and efficient. Consequently, e-commerce is now essential for businesses to be able to compete in the global marketplace. The purpose of this paper is to review identify e-risks, retail trade on the Internet, define virtual business, identify aspects of website design, and describe types of cyber crime that hamper e-commerce. The Internet is an excellent medium for advertising. E-commerce has been heavily promoted via Internet advertising. Research indicates that when people read an online ad they are more likely to buy online. Estimates from various sources indicate that advertisers spend hundreds of millions of dollars to put their messages on high-traffic websites. An advertising banner on the Internet potentially levels the playing field between large and small companies.

Cyberspace is a term that refers to the electronic medium of computer networks, principally the Internet, in which online communication, including e-commerce takes place. Cyber crime is a criminal act that involves computers and networks. This means that cyber crime includes criminal acts such as hacking, phishing, and denial of service attacks that cause e-commerce websites to lose money. A basic knowledge of cyber crime is essential to e-commerce companies. Each year, companies lose billions of dollars in stolen assets, lost business, and damaged reputations as a result of cyber crime. Money is stolen, literally with the push of a button. When a company website goes down, e-commerce stops. The company's customers often take their business to a different website. When a company becomes the victim of cyber crime, this hurts the company's reputation. Perceived vulnerability to cyber crime may cause customers to lose trust in a company's ability to effectively process sales transactions and safeguard customer information. As a result, companies must strive to defend against cyber crime. A list of some common cyber crimes are as mentioned below:

**Phishing** - Phishing occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator.

**Botnet** - A Botnet infection occurs when a hacker transmits instructions to other computers for the purpose of controlling them, and then using them for various purposes such as spam distribution or phishing.

**E-bank theft -** E-bank theft occurs when a perpetrator hacks into a banking system and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online.

**Netspionage -** Netspionage occurs when perpetrators hack into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties (criminals)

**Online credit card fraud -** Online credit card fraud is illegal online acquisition of a credit card number and use of it for unauthorized purposes such as fraudulent purchases.

**E-fraud -** E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include spoofing, phishing, and online credit card fraud.

***Cyber-crimes*** are new versions of age-old crime. An illustration of this is the con artist. Before the new information technologies existed, a con artist would go from house- to-house and use his communication skills to gain the confidence of his victims. In the current day, a con artist makes use of the Internet and online communications to perpetrate his crimes.

The cybercrime of phishing occurs when a perpetrator distributes fictitious emails to people, which include links to fraudulent websites that appear official and cause the victims to provide personal information to the perpetrator. The deceptively obtained information is later used for unauthorized purposes such as fraudulent purchases, acquiring fraudulent loans, or identity theft. Key steps in the cybercrime of phishing are as below:

1. The phishing perpetrator creates fraudulent email that appears to come from a legitimate source. The phishing emails are then sent to numerous potential victims.

2. The phishing email provides a link to the fraudulent website, which appears to be a genuine website.

3. The user/ victim connect to the fraudulent website and provide requested information, on the assumption that it's a genuine website.

4. The phishing perpetrator accumulates data obtained in the fake website to illegally obtain funds or sells the data to online clearinghouses.

The cyber crime of botnet infection takes place when a hacker transmits instructions to other computers in order to control them. The hacker who sends out the "bot" program is designated as the "herder." Numerous computers can be controlled in a botnet. Computers controlled in a botnet

can be used for nefarious activities such as spam distribution or phishing. Actual owners of computers in the botnet typically are unaware that their computer is part of a botnet. Key steps in the botnet cybercrime are as below:

1. The hacker who disseminates the “bot”program is referred to as a “herder.”

2. The Bot program is designed to infect and control infected PCs. The Bot may infect a PC directly or piggy-back on a virus or Trojan horse program.

3. The Botnet infection can include thousands of PCs. Botnets can be used for various purposes

e.g. spam distribution or phishing.

**Payment Gateway**

A payment gateway is a way to process electronic transactions. Payment gateways provide the tools to process payments between customers, businesses, and banks. This article will explain how a payment gateway works and features of payment gateways.

If you are looking to set up your business so that you can take advantage of ecommerce operations, you have probably heard the term "payment gateway." A payment gateway is a necessary part of the transaction between customer, business and the banking institutions that both are using. A payment gateway is used to facilitate electronic transactions. Some of the main features of a payment gateway include:

- Software application designed especially for ecommerce, although it can be used to authorize payments in traditional brick and mortar businesses.
- Encryption of payment and personal data.
- Communication between the financial institutions involved and the business and the customer.
- Authorization of payments.

Some payment gateways feature tools that can help your customers figure out shipping and handling costs, as well as sales tax. There are also fraud detection tools and other features that can be used with a payment gateway. Many ecommerce Web hosts offer payment gateways as part of their hosting packages.

**How does a payment gateway work?**

A payment gateway takes advantage of the Internet to send and receive information. It is a specially designed application that facilitates purchase transactions. Many traditional businesses use them as well, since it allows for more accurate and immediate authorization of payment. An Internet connection is required, since most of the time a payment gateway makes use of the communications channel available over the Internet. This is much faster than older credit card processing done by via the phone line.

**Here is an illustration of how a payment gateway works:**

1. The customer makes a purchase. This can be via a Web site, or physically in person. It may even be a phone order that the business enters in by hand while on the phone with the customer.
2. The Internet browser being used by the customer uses Secure Socket Layer (SSL) encryption to "scramble" the information being sent.
3. The business Web site takes the details and forwards them to the payment gateway. The payment gateway is separately hosted in some cases, and encryption is still necessary.
4. The payment gateway takes the information and sends the details to the bank used by the business.
5. The bank sends the request to the card association. In the case of American Express or Discover, the card association is the same as the bank, and a response can then be issued. If the card used has a MasterCard or Visa logo, additional steps occur.
6. With Visa or MasterCard, the card association forwards the information to the bank that issued the card. This is the customer's bank.
7. The customer's bank assesses whether or not there are sufficient funds to cover the transaction.
8. The issuing bank then sends an authorization code. This code will tell the payment processor card association whether or not to allow the transaction to go through. The authorization code corresponds to the reason for a decline if there is one, or simply includes the code that allows the transaction to take place.
9. The payment processor sends the authorization code to the payment gateway.
10. The payment gateway then sends the code on to the business. If the transaction is declined, the sale is terminated. If the transaction is approved, the sale goes through and the money is placed on "hold" from the customer's account.

While this process seems lengthy, in reality it only takes a few seconds to complete. In some cases, it happens in two seconds. In other cases, it can take as long as 10 seconds. It depends on the

connection speed of the site, as well as traffic on the local Internet service provider. Before the sale is properly "settled", however, the product must be shipped. Here are the additional steps that a transaction must go through to reach final authorization:

- The business gathers all of the authorization codes from that day into a "batch" at the end of business. These codes are submitted to the bank where the business has its merchant account.
- The business's bank takes the approved funds and puts them into the proper account. In some cases, this account may be with a different bank. It is whatever the merchant designates. This is known as settlement funding. It takes about three days from the time of purchase for a business to actually receive usable funds.

A payment gateway can be very useful. If you want to accept online transactions you will need one. Even if you don't operate a business Web site, a payment gateway can be a useful ecommerce too

# SOME IMPORTANT SECTIONS

**Sec 45. Residuary penalty.-**

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

**Sec 61. Civil court not to have jurisdiction. -**

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**Sec 69. Directions of Controller to a subscriber to extend facilities to decrypt information. –**

(1) If the Controller is satisfied that it is necessry or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years

# FACTS AND FIGURES

In 2006, this number more than doubled to 200 incidents. Not only were attacks being launched in India but 2006 saw the maximum phishing attacks being launched from India on other countries as well. Security expert, Surinder Singh says, 'As per Websense Security Lab, we find that at any given point in time in 2006, there were 2 to 300 websites being hosted. There was a spurt in October where we identified 790 websites which were hosted in India and being used to carry out attacks." The United States remains at the top with 28.78% of all phishing sites located out of the United States and 11.96% out of China. Korea, Germany, Australia, Canada, Japan, United Kingdom, Italy and India are the other countries where phishing attacks are prevalent. As of now, 2.11% of the phishing sites are located in India. Singh says, 'India on the threshold of having more and more people getting into online banking or taking online peronal loans. So, it won't be a surpirzse if someday someone tells me that out of the total size of frauds happening - India would be at 1% or 2% - but even that would be Rs 200 crore."

During the year 2003, 60 cases were registered under IT Act as compared to 70 cases during the previous year thereby reporting a decline of 14.3 percent in 2003 over 2002. Of the total 60 cases registered under IT Act 2000, around 33 percent (20 cases) relate to Obscene Publication Transmission in electronic form, normally known as cases of cyber pornography. 17 persons were arrested for committing such offences during 2003. There were 21 cases of Hacking of computer systems wherein 18 persons were arrested in 2003. Of the total (21) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were to the tune of 62 percent (13 cases) and that related to Hacking under Section 66(2) of IT Act were 38 percent (8cases). During 2003, a total of 411 cases were registered under IPC Sections as compared to 738 such cases during 2002 thereby reporting a significant decline of 44 percent in 2003 over 2002. Andhra Pradesh reported more than half of such cases (218 out of 411) (53 percent). 4 Of the 411 cases registered under IPC, majority of the crimes fall under 3 categories viz. Criminal Breach of Trust or Fraud (269), Forgery (89) and Counterfeiting (53). Though, these offences fall under the traditional IPC crimes, the cases had the cyber tones wherein computer, Internet or its related aspects were present in the crime and hence they were categorized as Cyber Crimes under IPC.

During 2003, number of cases under Cyber Crimes relating to Counterfeiting of currency/Stamps stood at 53 wherein 118 persons were arrested during 2003. Of the 47,478 cases reported under Cheating, the Cyber Forgery (89) accounted for 0.2 per cent. Of the total Criminal Breach of Trust cases (13,432), the Cyber frauds (269) accounted for 2 percent. Of the Counterfeiting offences (2,055), Cyber Counterfeiting (53) offences accounted for 2.6 percent. A total of 475 persons were arrested in the country for Cyber Crimes under IPC during 2003. Of these, 53.6 percent offenders (255) were taken into custody for offences under Criminal Breach of Trust/Fraud (Cyber) and 21.4 percent (102) for offences under 'Cyber Forgery'.

The age-wise profile of the arrested persons showed that 45 percent were in the age-group of 30-45 years, 28.5 percent of the offenders were in the age-group of 45-60 years and 11 offenders were aged 60 years and above. Gujarat reported 2 offenders who were below 18 years of age. Fraud/Illegal gain (120) accounted for 60 per cent of the total Cyber Crime motives reported in the country. Greed/Money (15 cases) accounted for 7.5 percent of the Cyber Crimes reported. Eve-teasing and Harassment (8 cases) accounted for around 4 per cent. Cyber Suspects include Neighbors / Friends / Relatives (91), Disgrunted employees (11), Business Competitors (9), Crackers Students / Professional learners (3).

Cybercrime is not on the decline. The latest statistics show that cybercrime is actually on the rise. However, it is true that in India, cybercrime is not reported too much about. consequently there is a false sense of complacency that cybercrime does not exist and that 5 society is safe from cybercrime. This is not the correct picture. The fact is that people in our country do not report cybercrime for many reasons. Many do not want to face harassment by the police. There is also the fear of bad publicity in the media, which could hurt their reputation and standing in society. Also, it becomes extremely difficult to convince the police to register any cybercrime, because of lack of orientation and awareness about cybercrimes and their registration and handling by the police. A recent survey indicates that for every 500 cybercrime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cybercrime. The number of viruses and worm variants rose sharply to 7,360 that is a 64% increase over the previous reporting period and a 332% increase over the previous year. There are 17,500 variants of Win.32 viruses. Threats to confidential information are on the rise with 54% of 6 the top 50 reporting malicious code with the potential to expose such

information. Phishing messages grew to 4.5 million from 1 million between July and December 2004.

# Conclusion

As we can see that there where so many cyber crimes happening in India before the amendment of information technology act the rate of crime have not stopped nor it have come down but it is reaching its high . We have try to find out various reasons that despite of such a tight act and high penalties and punishments what are the lope holes in the act which is blocking the proper implementation of such a force full act .

Cyber Law in India is in its infancy stage. A lot of efforts and initiatives are required to make it a mature legal instrument. Law has been instrumental in giving Cyber Law in India a shape that it deserves. To make the circle complete we are proudly introducing another effort in this direction.

Following are some of the lope holes which we have tried to figure out:

1. Reporting of important matters pertaining to Cyber Law in India:
2. Analysis of Cyber Law scenario in India,
3. Providing a comprehensive database for cases and incidents related to Cyber Law in India,
4. A ready reference for problems associated with Cyber Law in India, etc.

The discussion group cum database will analyse Cyber Law of India that suffers from the following drawbacks:

1. Non-inclusion of contemporary Cyber crimes and Contraventions like Phishing, Spamming, Cyber extortions, Compromised e-mails, Cyber Terrorism, etc.
2. An obscure position of Freedom of speech and expression under the IT Act, 2000.
3. Absence of Liability for illegal blocking of websites, blogs, etc.
4. Lack of Techno-Legal compliance under the IT Act, 2000.
5. Lack of Wireless security under the IT Act, 2000.
6. Absence of legal protection pertaining to IPRs in cyberspace.
7. A confusion regarding Locus-standi and due diligence.
8. Absence of Private defence in cyberspace.
9. Non-dealing of issues like Cyber terrorism and private defence,
10. E-waste in India must be taken seriously, etc.

Besides these grey areas India is also facing problems of lack of Cyber Security in India as well as ICT Security in India. A techno-legal base is the need of the hour. Unfortunately, we do not have a sound and secure ICT Security Base in India and Cyber security in India is still an ignored World. If opening of Cyber Cells and Cyber Units is Cyber Security than perhaps India is best in the World at managing Cyber Security issues. Unfortunately ICT Security in India is equated with face saving exercises of false claims and redundant exercises. The truth remains that ICT Security in India is a myth and not reality. The Cyber Law in India requires a dedicated and proactive approach towards ICT and Cyber Security in India. In the absence of a dedicated and sincere approach, the Cyber Law in India is going to collapse.

Now as we know what are the major lope holes in the act let us try to fine the possible suggestion to over come these and try to learn form what us/uk are following inorder to have a virus free cyber.

# Suggestion

**Recruitment**

There is a high need to increase the strength of staff for proper functioning of the ACT.

**Red coding System**

Set - up a red coding system, with the help of which the government can keep a tap on mails, chat, etc. this system will help the government to detect the possibility of further cyber crime.

**Training and Development**

One of the most important requirements for the proper function of the ACT is that, there should be good quality training programs on a regular base.

**Domain**

It is necessary, Domain should be treated as a separate entity rather then treating it as IP ACT .

**Cyber theft, cyber stalking, cyber harassment and cyber defamation are presently not covered under the act.**

These crimes need to have specific provisions in the act to enable the police to take quick action.

**Vague Definitions**

Definitions, prescriptions of punishment and certain provisions (such as that dealing with hacking) need specific amendment.

**Parameters for its implementation**

Law enforcement officials need to be trained for effective enforcement.