We are in computer Era. The use of computers, software's and digital information is inevitable in today's day to day life. Present generation is accustomed to computers. The transactions and businesses now a days started to deal through cyber arena. It has wide scope and its space increases drastically day by day. At the same time needles to say that it has also brought in some negative effects and disadvantages too.

CYBER LAW

We are in computer Era. The use of computers, software's and digital information is inevitable in today's day to day life. Present generation is accustomed to computers. The transactions and businesses now a days started to deal through cyber arena. It has wide scope and its space increases drastically day by day. At the same time needles to say that it has also brought in some negative effects and disadvantages too.

The computer crime or an e-crime can be simply defined as a crime where a computer is the target of a crime or it is the means adopted to commit a crime. While some of the crimes may be new, the others are simply different ways to commit conventional crimes such as frauds, theft, blackmailing, forgery, and embezzlement using the online medium often involving the use of internet. What accelerates the growth of such crimes are typical characteristics of cyber space interalia anonymity, speed, access, dependency, borderless space.

Important cyber crimes are virus attacks, salami attacks, e-mail bombing, DOS attacks, internet hacking or information offences increase day by day.

LEGAL PROBLEMS: The Nature and Dimensions of the Information technology leads to peculiar legal problems. The problem deserve special treatment, because of the environment in which they creep up and the nature of the machinery used in the environment and the means employed for recording the information in question is typical. In all the other cases the documents are stored and transmitted through the use of visible and tangible letters, figures and marks however here the information which is stored and transmitted electronically has no visible shape or tangible form, this peculiarity of the technology gives rise to a deferent kind of legal problems. Therefore to overcome this legal problem the Information Technology Act, 2000 came into force in India on 17th of October 2000. The Act applies to all over India. Some times it applies to outside India also by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

MAJOR OFFENCES

Section 43 of the Act, which covers unauthorized access, downloading, introduction of virus, denial of access and internet time theft committed by any person. It prescribes punishment by way of damages not exceeding Rs. 1 crore to the affected party.

Chapter XI of the IT Act discusses the cyber crimes and offences interalia, tampering with computer source documents (Sec. 65), Hacking (Sec.66), Publishing of obscene information (Sec.67), Unauthorized access to protected system (Sec.70), Breach of confidentiality (Sec.72), Publishing false digital signature certificate (Sec.73).

THE MEANING OF COMPUTER

As per information technology Act "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network

TWO CATEGORIES OF CYBER CRIMES

1. The Computer as a Target :-using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.

2. Using the computer as a weapon :-using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Restricted videos etc.

MODES OF CYBER CRIMES

1. **Unauthorized access & Hacking:-**

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access means any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every acts committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to steal the credit card information, transfer money from various bank accounts to their own account etc.

Web hijacking is also a crime which means taking control of others webseite

1. **Virus and Worm attack:-**

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

4. E-mail & IRC related crimes:-

a) Email spoofing

an email shown to have sent from once source in fact has been sent frm a deferent source is called spoofing

b) Email Spamming

sending email to thousands and thousands of users - similar to a chain letter is called email spamming.

c) Sending malicious codes through email

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

d) Email bombing

abusive identical messages sent repeatedly to a particular address is called emails E-mail "bombing".

e) Sending threatening emails ,

f) Defamatory emails

g) Email frauds

h) IRC related

1. **Trojan Attack:-**

Trojan attack means by representing as a useful link or a helper it causes harm to your programme. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

1. **5. Denial of Service attacks:-**

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service and attempts to disrupt service to a specific system or person are examples of Deniel Service Attacks.

1. **6. Distributed DOS**

A distributed denial of service (DoS) attack is accomplished by using the Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into "zombies" and used to attack another system or website.

Types of DOS

There are three basic types of attack:

a. Consumption of scarce, limited, or non-renewable resources like NW bandwith, RAM, CPU time. Even power, cool air, or water can affect.

b. Destruction or Alteration of Configuration Information

c. Physical Destruction or Alteration of Network Components

e. Restricted videos:-

The literal meaning of the term 'Restricted videos' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

g. Forgery:-

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Also impersonate another person is considered forgery.

h. IPR Violations:-

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

Cyber Squatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

Cyber Squatters registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

i. Cyber Terrorism:-

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyberterrorism is an attractive option for modern terrorists for several reasons.

1.It is cheaper than traditional terrorist methods.

2.Cyberterrorism is more anonymous than traditional terrorist methods.

3.The variety and number of targets are enormous.

4.Cyberterrorism can be conducted remotely, a feature that especially appealing to terrorists.

5.Cyberterrorism has the potential to affect directly a larger number of people.

j. Banking/Credit card Related crimes:-

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information. Use of stolen card information or fake credit/debit cards are common. Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami.

k. E-commerce/ Investment Frauds:-

Sales and Investment frauds. False or fraudulent advertisements, claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online remains undelivered. In this the Investors are enticed to invest in this fraudulent scheme by the promises of seemingly high profits.

l. Sale of illegal articles:-

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. This kind of business is increasing day by day.

m. Online anti social game:-

Anti social game activities done through fake websites are called as online anti social game which is offence if it is game of chance.

n. Defamation: -

Defamation can be understood as tarnishing the image, respect or dignity of any person in front of right thinking members of the society.

A matter defaming a person is sent to the said person directly is not defamation however if the said mail is sent through CC or BCC to third parties and if the contents tarnish the image of the recipient it is defamation. Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. Publication of defamatory articles and matter on a website are defamation. Cyber defamation is also called as Cyber smearing.

Cyber Stacking:-

Cyber stalking involves following a persons 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.

In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications.

q. Identity Theft :-

Appropriation of others personal information without their knowledge in order to commit theft or fraud is called as identify theft. Identity theft is a vehicle for perpetrating other types of fraud schemes.

r. Data diddling:-

Changing data prior or during input into a computer is called as Data diddling. It also include automatic changing the financial information for some time before processing and then restoring original information.

s. Theft of Internet Hours:-

Unauthorized use of Internet hours paid for by another person.

By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

t. Theft of computer system (Hardware):-

u. Physically damaging a computer system:-

v. Breach of Privacy and Confidentiality

Confidentiality

It means disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected. Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties.

by M VINOD KUMAR

www.vinodadvocate.com