In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

The Computer as a Target :- using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon :- using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

a. 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 would therefore mean 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 act 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 stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

By hacking web server taking control on another persons website called as web hijacking

b. Trojan Attack:-

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.

The name Trojan Horse is popular.

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.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

c. 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.

d. E-mail & IRC related crimes:-

1. Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3. 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.

4. Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails

6. Defamatory emails

7. Email frauds

8. IRC related

Three main ways to attack IRC are: "verbalâ‚?Ŧ#8220; attacks, clone attacks, and flood attacks.

e. 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.

Examples include

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

attempts to disrupt service to a specific system or person.

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. Pornography:-

The literal mining of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc."

This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Adult entertainment is largest industry on internet. There are more than 420 million individual pornographic webpages today.

Research shows that 50% of the web-sites containing potentially illegal contents relating to child abuse were 'Pay-Per-View'. This indicates that abusive images of children over Internet have been highly commercialized.

Pornography delivered over mobile phones is now a burgeoning business, "driven by the increase in sophisticated services that deliver video clips and streaming video, in addition to text and images."

Effects of Pornography

Research has shown that pornography and its messages are involved in shaping attitudes and encouraging behavior that can harm individual users and their families.

Pornography is often viewed in secret, which creates deception within marriages that can lead to divorce in some cases.

In addition, pornography promotes the allure of adultery, prostitution and unreal expectations that can result in dangerous promiscuous behavior.

Some of the common, but false messages sent by sexualized culture.

Sex with anyone, under any circumstances, any way it is desired, is beneficial and does not have negative consequences.

Women have one value - to meet the sexual demands of men.

Marriage and children are obstacles to sexual fulfillment.

Everyone is involved in promiscuous sexual activity, infidelity and premarital sex.

Pornography Addiction

Dr. Victor Cline, an expert on Sexual Addiction, found that there is a four-step progression among many who consume pornography.

1. Addiction: Pornography provides a powerful sexual stimulant or aphrodisiac effect, followed by sexual release, most often through masturbation.

2. Escalation: Over time addicts require more explicit and deviant material to meet their sexual "needs."

3. Desensitization: What was first perceived as gross, shocking and disturbing, in time becomes common and acceptable.

4. Acting out sexually: There is an increasing tendency to act out behaviors viewed in pornography.

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 isespecially 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. An offering that uses false or fraudulent 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 are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally 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.

Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.

m. Online gambling:-

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

n. Defamation: -

Defamation can be understood as the intentional infringement of another person's right to his good name.

Cyber Defamation 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. Information posted to a bulletin board can be accessed by anyone. This means that anyone can place

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.

p. Pedophiles:-

Also there are persons who intentionally prey upon children. Specially with a teen they will let the teen know that fully understand the feelings towards adult and in particular teen parents.

They earns teens trust and gradually seduce them into sexual or indecent acts.

Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.

q. Identity Theft :-

Identity theft is the fastest growing crime in countries like America.

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud.

Identity theft is a vehicle for perpetrating other types of fraud schemes.

r. Data diddling:-

Data diddling involves changing data prior or during input into a computer.

In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.

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):-

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

u. Physically damaging a computer system:-

Physically damaging a computer or its peripheralseither by shock, fire or excess electric supply etc.

v. Breach of Privacy and Confidentiality

Privacy

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others.

Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

Confidentiality

It means non 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.

Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

Special techniques such as Social Engineering are commonly used to obtain confidential information.