: Intruduction to Cybercrime :

Cyber Security : Cyber security is the protection of internet Connected System, including hardware Software and data from Cyber attack.

- Cyber crime :- A crime conducted in which a Computer was directly and Significantly instrumental is called as cyber crime.
  - cyber crime is an illegal behaviour directed by means of electronic operations that targets the security of Computer system and the data processed by them.
  - Internet crime, Hightech, Computer crime, E-crime.

- Two types of crimes / attacks :

Techocrime : Primedidated act against a system with intent to copy, steal, prevent access to the Computer System.

Techno Vandalism : The act of brainless defacement of website and other activities such as files and publicing their content publically are usually Opportunities in nature.

- Cyber terrirism : cyber terrirism is defined as any person or group of person are organisation who with terrirst intent utilize the computer device and there by knowlingly attempts to engage in a terriorist act commits the affence of cyber terrirism.

- Phishing : Phishing is a cyber attack that uses E-mails as weapon. the goal is to trick email recipient into beliving that the message is something they want to need a request from their bank or note from their Company to check the links as attacks.

- Cyber Space : TCP.-IP
  Cyber Space is a world wide network of Computer network that uses the transmission Control Protocal (TC and Internet Protocal (IP) for communication to facilitate transmission and Exchange of data.

- Cyber Squatting :
  Cyber Squatting reffers to the act of regestering or using a domain name with the aim of profiting for a trademark, Carprelt name and personal name of Indivisual.

- Cyber punk : The term cyber Punk means something like anarchy via machines or computer rebel moment.

- Cyber warfare : Cyber Warfare means the information attac against an unexpecting opponents a computer network destroying and paralising nations machines. This type of cyber attack are often presented as thread to militaly forces and the Internet has majar implifications for Espoenage.

* : Cybercrime and Information Security :

Types of crimes	2004%.	2005	2006	2007	2008
DoS	39	362	25	25	21
laptop theft.	49	48	47	50	42
Unauthorized access	35	29	29	22	22
virus	78	74	65	52	50
Insider abuse	59	48	42	59	44
Sobotage	10	9	9	8	9

Botnet Menace :

Bot = Automatically

A group of Computers that are controlled by software containing harmfull programmes without their user's knowledge is called BOTNET

The term Botnet is used to refer to a group of Compramised computers. running ~~always~~ malways under a Common Comand & Controlled infrastrture

- DoS
- Adwares
- Spyware
- Email Spam.
- Finacial / creditcard.

Types of Cybercriminals :

Type I. : Hungry for Recognition

Type II : Not interested in Recognition

Type III : Insiders.

Classification of Cybercrimes :

Cybercrime against Individual

Cybercrime against Property.

Cybercrime against Organization

cybercrime against Society.

crimes Emanating from usenet and newsgroups.

* Cybercrime against Individual:

- Email Spoofing:

A Spoofed E-mail is one that appears to originate from one source but actually has been sent from another source.

- Online frauds:
- Phishing: → Spear phishing : with group of persons.
  - → vishing : through phone calls
  - → Smishing. through sms they grab our information
- Spamming: • Simply they are sending the msg's. rapidly
  - • through spam boats
- Cyber defamation: Reputation). to destroy the Reputation of an Person. through online
- Cyber stalking and harassment:

  they are collecting the person's indivisual document and they start harace that documents.
- Computer Sobatage:

  their intenstion to destroy the computer.
- Password Sniffing: they are using sniffer to grab the information.

* Cybercrime against Property:

- Credit card Frauds:

  through inserting the cards, they are
- Intellectual Property (IP) crimes:
- Internet time theft:

  Unauthorised using of intarnet.

* Cybercrime against Organization:

- Unauthorised access of Computer: [Hacking]
- Password Sniffing:
- DoS attack: to stop that Service.

  Dos →

- Virus attack :
  By inserting any one type of viruse then whole Organisation computers are attacked by that viruse.

- Email bombing :
  they are repitedly sending the msg for targeted system

- Salami attack / Salami technique : this is used for Committing finacial crimes. through ~~transi~~ tranaction.

- logic bomb :

- Trojan Horse : difficult viruse.

- Data diddling :

- Industrial spying :

* Cybercrime against Property & Society :

* Logic bomb a piece of often malicious code that is intentionally inserted into software.