

Introduction 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 : Primordially 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 publicizing their content publicly are usually Opportunities in nature.

* Cyber terrorism : Cyber terrorism is defined as any person or group of person or organisation who with terrorist intent, utilize the computer device and thereby knowingly attempts to engage in a terrorist act commits the offence of cyber terrorism.

* Phishing : Phishing is a cyber attack that uses e-mails as weapon. The goal is to trick email recipient into believing 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 Protocol (TCP) and Internet Protocol (IP) for communication to facilitate transmission and exchange of data.

* **Cyber Squatting**:
 Cyber Squatting refers to the act of registering or using a domain name with the aim of profiting for a trademark, corporate name and personal name of individual.

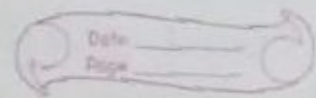
* **Cyber punk**: The term cyber Punk means something like anarchy via machines or computer rebel movement.

* **Cyber warfare**: Cyber warfare means the information attack against an unexpected opponents a computer network destroying and paralysing nations machines. This type of cyber attack are often presented as threat to military forces and the Internet has major implications for espionage.

* **Cybercrime and Information Security**:

Types of crimes	2004%	2005	2006	2007	2008
DoS	39	36	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
Sabotage	10	9	9	8	9

Botnet Menace :



Bot = Automatically

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

The term Botnet is used to refer to a group of compromised computers, running always malwares under a Common Command & Controlled Infrastructure

- DoS
- Adwares
- Spyware
- Email Spam.
- Financial / credit card.

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 email 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 bots.
 - Cyber defamation: Reputation to destroy the reputation of an person through online.
 - Cyber stalking and harassment:
they are collecting the person's individual document and they start harass that documents.
 - Computer sabotage:
their intention 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:
Unauthorized using of internet.

* Cybercrime against Organization:

- Unauthorized access of Computer: [Hacking]
- Password Sniffing:
- DoS attack: to stop that service.
DoS →

- Virus attack :

By inserting any one type of virus ^{then} ~~whole~~ ^{Page} organisation computers are attacked by that virus.

- Email bombing :

they are repeatedly sending the msg for targeted system

- Salami attack / salami technique : this is used for committing financial crimes.
through transi transaction.

- Logic Bomb :

- Trojan Horse : difficult virus.

- Data diddling :

- Industrial spying :

* Cybercrime against Property & Society :

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