Struxnet

mahak™ Date: 12/09/23 Page:

UNIT - I
Introduction to Cyber Crime

Cyber crime.

Cyber crime or a computer oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of crime or it may be target. cyber crime especially uses the internet as computing devices are majorly used in the field of e-commerce, government activity, important information sharing and entertainment.

The cyber crime may be a person and financial system. cyber crime is divided in two category.

① The crimes that aim at computer n/w or devices which includes threats like virus, bugs and DOS (denial of service), attacks

* A generalized definition of Cyber crime may be 'unlawful acts' wherein the computer is either a tool or target or both.

Cyber Security

Cyber
(Computer System, N/W, program or data)

Security
(Sys. Security N/W " Program or data Sqn.)

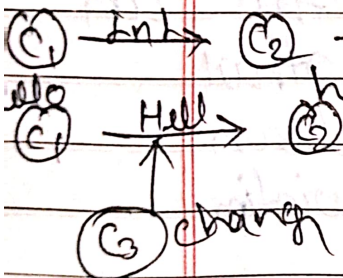
Need for Cyber Security.

* To Protect Private data.
* To Protect Banking or financial data
* National Security
* Global economy
* Protect sensitive data.

Cyber Security Goal -

CIA.

C - Confidentiality
I - Integrity
A - Availability, authentication



History of Cyber Sq. -

1969- Professor of UCLA sent msg to research institute.
"login" ⟶ "lo"

1970 - Robert thomas created first virus namely CREPER

1986 - Russians used cyber power as weapons to target National hq.

1988 - American scientist created program to check size of internet.

Challenges of cyber crime -

① People are unaware of their cyber crime. the cyber crims usually happ with illitrate people around the world who are unaware about their cyber rights implimented by the govt.

② **Anonymity** - Than who commit cyber crim are annonymus for us so we do not do know anything to that person.

③ **Mostly commited by well educated people** - The person who commit cyber c is a very technical person so he knowes that how do do the crim and not get caught by the authority.

* Less no. of case registered
* No harsh punishment
* Prevention of Cyber crime
* use strong password

~~Maintain different~~ Maintain different username & password combination for each account.

* Use trusted Antivirus in devices.
* Keep your device s/w updated.
* Educate and train users.

Provide c.s training to individuals, employee or family members

* Data encryption:- Encrypt sensitive data to ensure that even if it's accessed by unauthorized users, they can't read without the decryption key.
* Regular backups.
* Secure Social media use.
* Don't use public wifi. (unauthorised)

Information Security -

Origin of the word -

The term 'cybercrime' relates to a number of other terms such as -

* Computer related crime
* Computer crime.
* Internet crime.
* E - Crime
* High tech crime.

⇒ Akash Arora (1999) was one of the earliest examples of cybercrime in india (Yahoo can → Xaabo.)

⇒ * Information is a valuable asset. Security of information is a critical issue which must be addressed properly, nowdays everyone is dipendent on info. for personal as well as professional activities.

* The concept of info. security involve maintanance of confidentiality, integrity and availbility of info. security

[OR]

Classification of cyber crime -

① Against Individual
- (a) cyber stalking
- (b) Spoofing
- (c) Phishing
- (d) Hacking
- (e) defamation

② Against Property
- (a) cyber Squatting
- (b) Cyber vandalism
- (c) IPR crime
- (d) Transmitting virus

③ Against Society
- (a) online Gambling
- (b) Cyber trafficking

④ Against Govt.
- (a) Cyber warfare
- (b) Cyber terrorism.

(1) Against individual
(2) Against Property
(3) Against Govt
(4) Against Society

Classification of Cybercrime -

* Against individual -

① **Cyber stalking** -

* Stalking in general means behaviour of harassing or threatening other person.

* Cyber stalking refers to stalking other person over internet using Info. Technology.

Focus section 6 : Action

Date:
Page:

* In cyber stalking, internet, email, chat room etc are used to stalk or harass an individual person.

Stalking generally involves :-

→ Following a person
→ appearing at person's home or workplace.
→ Making harassing phone call, email etc.

There are three ways in which cyber stalking is conducted.

(i) Stalking by Email
(ii) Stalking by internet
(iii) stalking by Computer.

(2) Spoofing - Spoofing means to provide false info. about your identity to gain unauthorised accss to computer system.

For exp- If we have our online payment shop and anybody purchase thing from the shop and do online payment but actually he did not do the

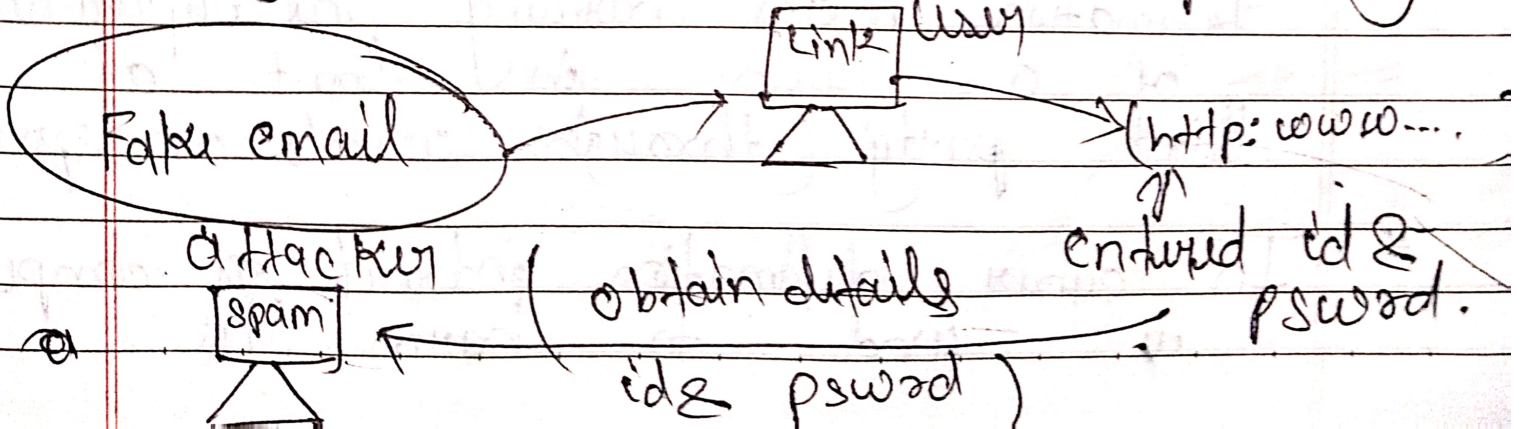
payment and show fake screenshot of the payment So this crime is called spoofing.

(8) Phishing :- * The term phishing refers to an attack using mail programs to trick web user into revealing sensitive info. that can be used for criminal purpose.

(OR)

* Phishing is fraudulent to obtain sensitive info. or data, such as username, pswrds and credit card details by suggesting oneself as a trustworthy entity in an electronic comm.

Ex- Gain user id and password of the victim ~~issue~~ by sharing an email with a fake link website which is created by attackers and its look like original website the types of techniques in phishing.



(4) **Hacking** :- Hacking is a technical process where finds and exploits the weakness in computer system and/or n/w to gain access. Hackers are usually skilled computer programmer with knowledge of computer security.

Types of hackers :-

(1) Ethical hacker (white hat) → legal way.
(2) Black hat hacker → illegal way.
(3) Gray hat hacker → only try to hack into
(4) Hacktivist hacker → Politician purpose hack site
(5) Script kiddies → Non skilled other hacker tool used
(6) Phreaker → Telephone hack.

(5) **Difamation** :-

* Cyber difamation is divided into two parts - cyber and difamation.

* Difamation means harming the reputation of a person in front of third party (through words or spoken)

* In cyber difamation internet or computer is used to harm the

reputation of other person.

In india, liability of defamation in two folds -

[1] **Primary writer:** The person who has written the defamatory content & publish it on the cyberspace.

[2] **Service providers:** The Service provider or owner of the site who authorized for publication of such defamatory content.

→ **Laws of defamation** - It is punishable offline under the IT act 2000 & indian panel code (IPC)

IPC - Section 499, Section 500, Section 469
Section 503
IT Act - Section 66A

* Against Property:-

① **Cyber squatting** - It is also known as domain squatting.
the term cybersquatting refers to the unauthorized registration and use of internet domain names that are similar to trademarks, company names or personal names.
Cyber squatting registrants use the domain name with bad faith intent to profit from the goodwill of the actual trademark owner

[OR]

Cyber squatting is used to create a fake domain website to make a good profit or threating the people by using other identity or company name but this is also a illegal way.

⇒ the ACPA (anticybersquatting protection act) is a federal law, banned domain name registration that are similar to trademark.

③ **Cyber vandalism** -- Dont use publicwifi for transfering intention to destroy property.

Cyber vandalism is like damaging property its when someone intentionally messes up website, online profiles or other internet thing causing trouble or chaos they might deface websites, delete imp. files or spread harmful msg, just like vandalizing physical things

[OR]

"Typical cyber vandalism involves the creation of malicious programs designed to perform harmful task such as extracting login credintials or erasing hard drive data."

④ **IPR (intellectual Property rights) Crime:-**

IPR Crime is when someone steals or uses things that someone else created like ideas, inventions or artistic works without permission, its like taking someone special drawing, stories or unique ideas and using them for your own benefit without asking or giving them credit. it's not fair and against the rule.

Against Society:-

① **Online gambling:-** Online gambling cybercrime is when bad people use the internet to do illegal things related to betting and gambling this could be cheating in games, stealing money or personal info from players or using gambling website for criminal activities like money laundering that's the cybercrime part of online gambling.

② **Cyber trafficking:-** Cyber trafficking, also known as cybercrime or online trafficking, is when people use the internet to engage in illegal activities involving the trade, sale or exploitation of goods, services or individuals. this can include things like selling illegal drugs, weapons, stolen goods or even engaging in human trafficking or exploitation through online platforms

Against Govt:-

① **Cyber warfare** - Cyber warfare is like a battle that happens in the digital world. In this kind of warfare, countries, groups or individuals use computers, the internet and technology to attack or gain access to information from other. It is like a fight using hacking, viruses to damage or control computer systems now. The goal is to win an advantage or cause damage without physically fighting.

② **Cyber terrorism**:-

* Cyber terrorism is use of computers and internet connectivity in order to launch a terrorism attak.

* Cyber terrorism try to cause damage and activities are as public as possible. the idea is to strike fear among people.

Cybercrime Era: Survival mantra for Netizens

Netizens:

Netizens are people who use the internet, like you and me, the word "netizens" is a combination of "internet" and "citizens". 😊

The 5p Netizen mantra for online Security is:

① Precaution ② Protection ③ Prevention
④ Preservation ⑤ Perseverance (दृढ़ता)

→ Protect personal info.
→ Use strong password
→ Beware of scams
→ Use virtual private n/w

Cyber offenses:-

Cyber offenses are like breaking the rules and laws on the internet. just like in the real world, there are laws and guidelines for what is allowed and what's not when you're online. when someone does something illegal or harmful on internet, it is consider a cyber offense.

Here some common example of cyber offens-

Cracker
criminal + hacker

mahak™
Date:
Page:

① Hacking
② identity theft.
③ cyber stalking
④ Online scam etc..

Social Enginuring -

* Social enginuring is the "Technique to influnce" and "persuassion to deciue" people to obtain the information or perform some action.

* Social enginuring involves gaining sensitive information or unauthorized acces by building inappropriate trust relationship with insiders.

* It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.

* The goal of social enginur is to fool somon into providing valuable informati or acess to that information.

Ex - Imagin you get a phon call from somon who claims to work for your bank, they say thur's problm with your account, and they nud to verify your personal info to fix. they speak very profesional and

urgent, making you feel worried, you give them your account number, password, & other sensitive details.

Zombie

Botnet: the fuel for CyberCrime -

Botnet is also known "Zombie n/w"
A botnet is a n/w of Computers infected with a malicious program that allows cybercriminals to control the infected machine remotely without knowing the user. Zombie n/w have become of income for entire groups of cybercriminals

"A botnet" is like a big group of Computers or devices that have been taken over by attacker then attacker can control them devices from far away without the owners knowledge.

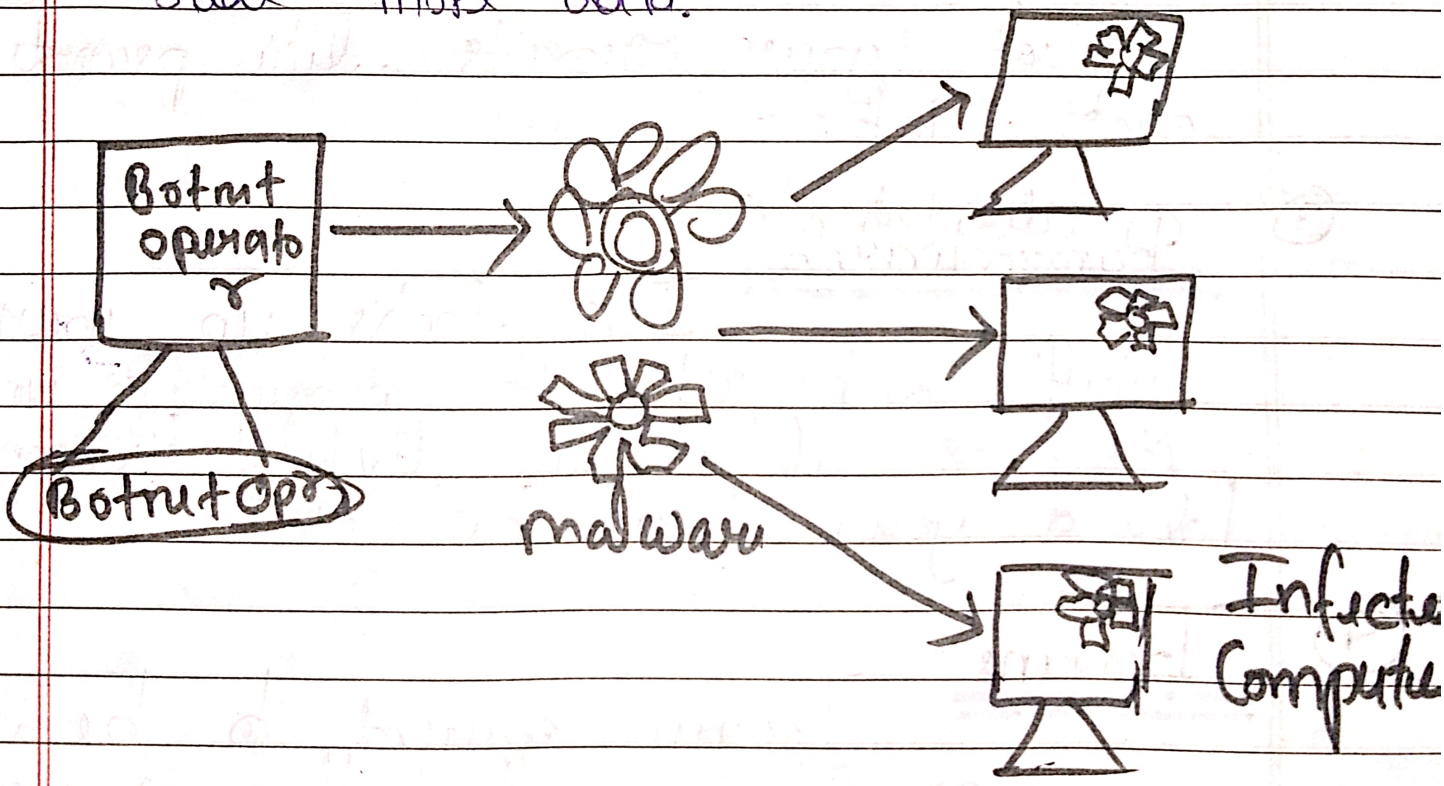
The fuel for cybercrime is what keep them attackers going. its a stuff that helps them to do bad things.

③ Money:- Cybercriminals wants to make money. they might steal your bank info., sell stolen data or even make a demand or for ransomware.

your files.

② **Information -** They gain information - your pursonal details, password, credit card details, they use or sell this info. for their own profit.

③ **Power and Control -** Controlling botnets gives them power. they can shut down websites, manipulate system or steal more data!



Malware - "Malware" is a word made from "malicious s/w" It's like having a intention to damage or slow the performance in your computer.

(OR)

"Malwares are developed by cybercriminals to steal data and damage or destroy computer system"

Type of malware -

① Viruses -

② Spyware - Think of this as a snoopy spy (जासूसी). It quietly watches what you do on your device and can steal your secrets, like pswds or bank info.

③ (like kidnapping)
Ransomware - Its locks up your stuff and ask for money to unlock it. its like a digital kidnapper holding your file hostage (बंधक)

④ Trojans - Trojans pretend to be nice apps or file, but they secretly can damage once you open them.

⑤ Worms - It's like spreading germs

Worms can copy themselves and travel through n/w, causing a lot of trouble for many devices.

⑥ **Adware -**

Adware is like a pushy salesperson. it bombards you with unwanted ads and pop-ups, trying to sell you things or take you other websites.

⑦ **Rootkit -**

A "Rootkit" is like a secret hideout for sneaky S/W on your computer. It's a type of malicious S/W that hides deep inside your system, making it hard to find and remove.

Attack vector -

It is a term used to describe the method a cybercriminal uses to gain initial (essential) access to a victim n/w or infrastructure.

Common attack vectors -

① Malware ② Viruses ③ Infected email attachments ④ Webpage malicious links and popups ⑤ Instant msgs ⑥ Social Engineering.

Access Control :-

Access control is like having a special key to enter a secret clubhouse. Let suppose if a treehouse had a magical lock that only lets certain friends inside.

In the computer world, its similar, Access Control is like having digital locks and keys, it decide who get to use or see certain things on computer or in a n/w. not everyone gets the same key. Some keys might open many doors, while others only open a few.

Access control helps keep things safe and private in digital world.

Access control policies are.

→ Identification
→ Authentication
→ Authorization
→ Non-Repudiation (जो वो नहीं करेंगे मना करना)

Thank You

RRSIMT
CLASSES
By - ARMAN ALI

Don't Forget to subscribe