CS & DF

Unit 1 : Introduction To Cyber Security

contents

- Introduction to Cybercrime and cybersecurity
- Types of Cybercrimes:
  - Crime against Individual
  - Crime against Property
  - Cyber Extortion
  - Drug Trafficking
  - Cyber Terrorism
- Threat to Information Security
- Need of Information Security

Introduction to Cybercrime and cybersecurity

CYBERCRIME :-

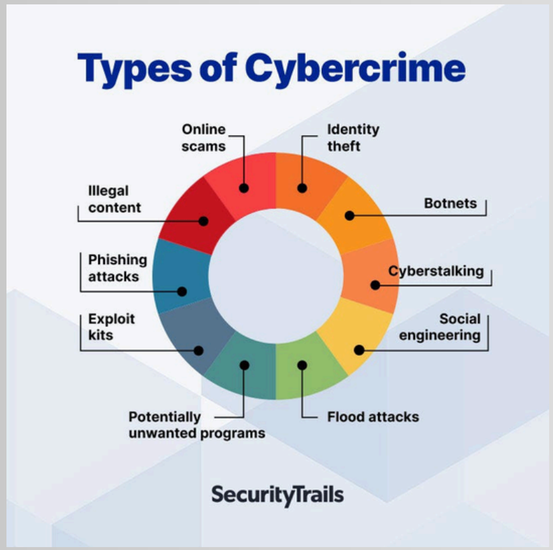
- Cyber Crime is a type of crime that is carried out using computers, the internet, or other digital devices, instead of traditional physical methods.
- It refers to various illegal activities that take place in cyberspace, such as stealing information, spreading malware, or committing fraud.
- The main targets of cyber crime can be data, computer systems, online networks, or even individual people who use the internet.
- Common examples of cyber crime include hacking into accounts, phishing through fake emails or messages, and online frauds where money is stolen digitally.

Introduction to Cybercrime and cybersecurity

CYBERSECURITY :-

- Cyber Security is the practice of protecting computers, networks, and digital data from unauthorized access, attacks, or damage caused by cyber criminals.
- It involves the use of technologies, processes, and security measures to keep information safe from threats like hacking, phishing, or malware.
- The main goal of cyber security is to ensure the confidentiality, integrity, and availability of data and systems, so that users can trust and safely use technology.
- In simple words, Cyber Security means creating a safe digital environment by preventing cyber crimes and protecting people, organizations, and nations from online threats.

TYPES OF CYBERCRIMES



A. Crime Against Individuals

- Crime against individuals refers to cyber crimes where a single person becomes the main target of attack.
- These crimes are usually aimed at stealing personal information, causing financial loss, or mentally harassing the victim.
- The attacker uses the internet or digital platforms to exploit, cheat, or threaten individuals for personal gain.
- Examples include identity theft, cyber bullying, phishing, and online frauds where the victim suffers directly.

Phishing

- Phishing is a type of cyber crime where attackers send fake emails, messages, or websites to trick people into sharing sensitive information.
- The goal of phishing is to steal personal details like usernames, passwords, bank account numbers, or credit card details.
- It looks very real and official, often pretending to be from a bank, government, or trusted company.

Example:-

- A person receives an email that looks like it is from their bank, asking them to "verify their account" by clicking a link.


Let's Go Phishing!

Spear Phishing

- Spear Phishing is a targeted form of phishing where attackers focus on a specific person, group, or organization.
- The attacker collects personal details about the victim (like name, job role, or company info) to make the fake message look more genuine.
- Because it looks very real and personalized, victims are more likely to trust and fall for it.

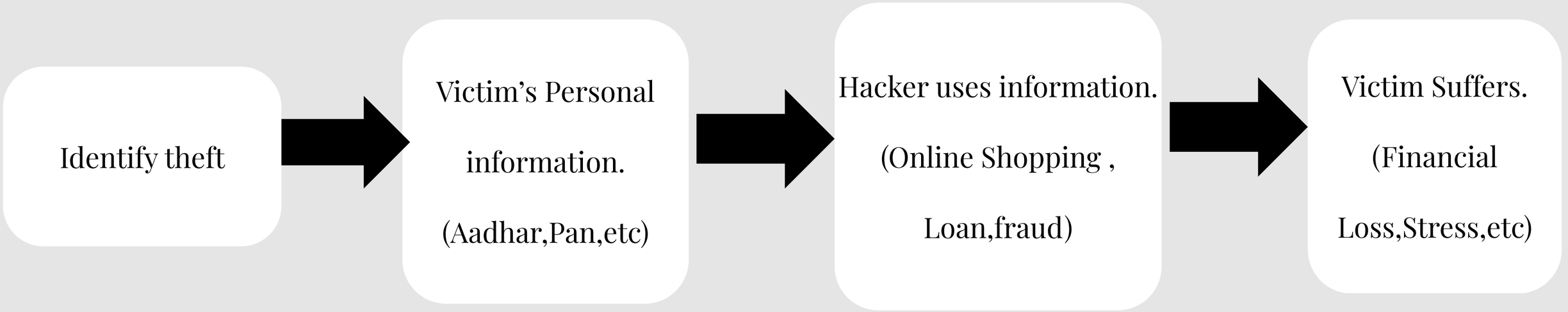
Example

- An employee receives an email that looks like it is from their CEO or manager, asking them to urgently share a confidential report or transfer money.

Identity Theft

- Identity Theft means stealing someone's personal information like Aadhaar, PAN, credit card, or login details.

- The attacker then uses this information to commit fraud, such as taking loans or shopping online in the victim's name.



Cyber Stalking

- Cyber Stalking means using the internet to continuously harass, threaten, or monitor someone.
  It often happens through emails, social media, or messaging apps.

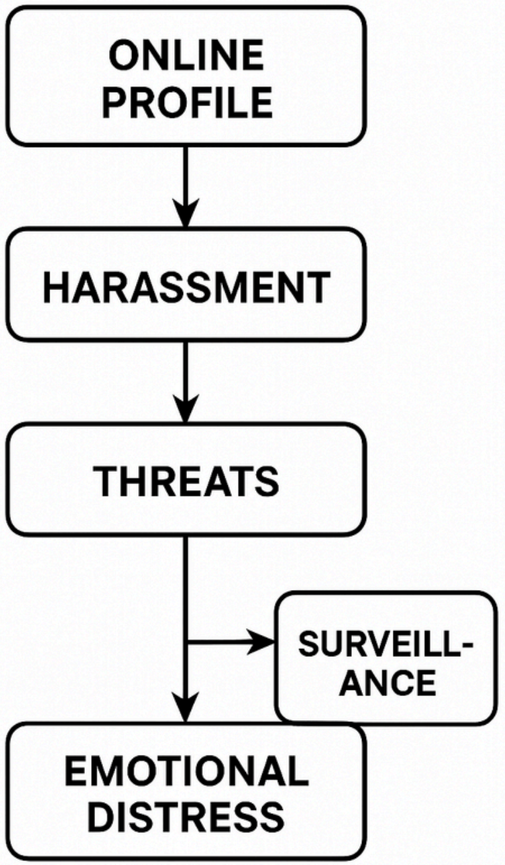
- Victims feel unsafe, scared, and mentally stressed because of constant digital harassment.

Example

- A person keeps sending unwanted messages and threats on social media to someone, even after
  being blocked, to scare and control them.

DIAGRAM

CYBER STALKING



B. Crime Against Property

- A crime against property is any illegal act where someone's property (money, goods, land, etc.) is stolen, damaged, or misused.
- **Key Points:**

1. Involves taking or damaging someone else's property without permission.
2. Victim suffers financial loss.
3. Includes theft, robbery, burglary, or vandalism.

- **Example:**

A person breaks into a house and steals a laptop and cash.

Cyber Fraud

- Cyber Fraud means scams or illegal activities online that trick people into giving money or personal information.

Key Points:

- Fraudsters use fake websites, emails, or apps to cheat people.
- Victims lose money or sensitive information like bank details.
- Common types include phishing, fake online shopping, and investment scams.
- Can happen to anyone using the internet.

Example:

- A fake e-commerce website asks for payment for a product but never delivers it.

Social Engineering

- Social Engineering is a technique where attackers manipulate people into revealing confidential information like passwords, bank details, or personal data.

Key Points:

- Attackers exploit human psychology instead of technical hacking.
- Common methods include phishing emails, fake calls, or messages.
- Victims may unknowingly give sensitive information.

Example:

- A fraudster calls pretending to be a bank employee and convinces a person to share their OTP, which is then used to steal money.

Hacking

- Hacking is the unauthorized access to someone's computer, network, or system to steal, alter, or damage information.

Key Points:

- Hackers break into computers, websites, or networks without permission.
- Can steal sensitive information like passwords, bank details, or personal files.
- Types include ethical hacking (for security) and malicious hacking (illegal).
- Leads to financial loss, data theft, or system damage.

Example:

- A hacker breaks into a company's database and steals customers' credit card information.

1. Recossanssing & information

2. Scanning & tools for find vullerallition

3. Explonning Enurmatiion

3. Gaining Access lennoiints

4. Install backdovrs or malware

5. Installing logs and hiding activities

5. Covering Tacks

C.Cyber Extortion

- Cyber Extortion is when a hacker or cybercriminal threatens to damage, block, or steal your data unless you pay them money or do what they want.

Key Points with Examples:

- **Threat to Data or System** – Hackers may threaten to delete, leak, or lock your important files.

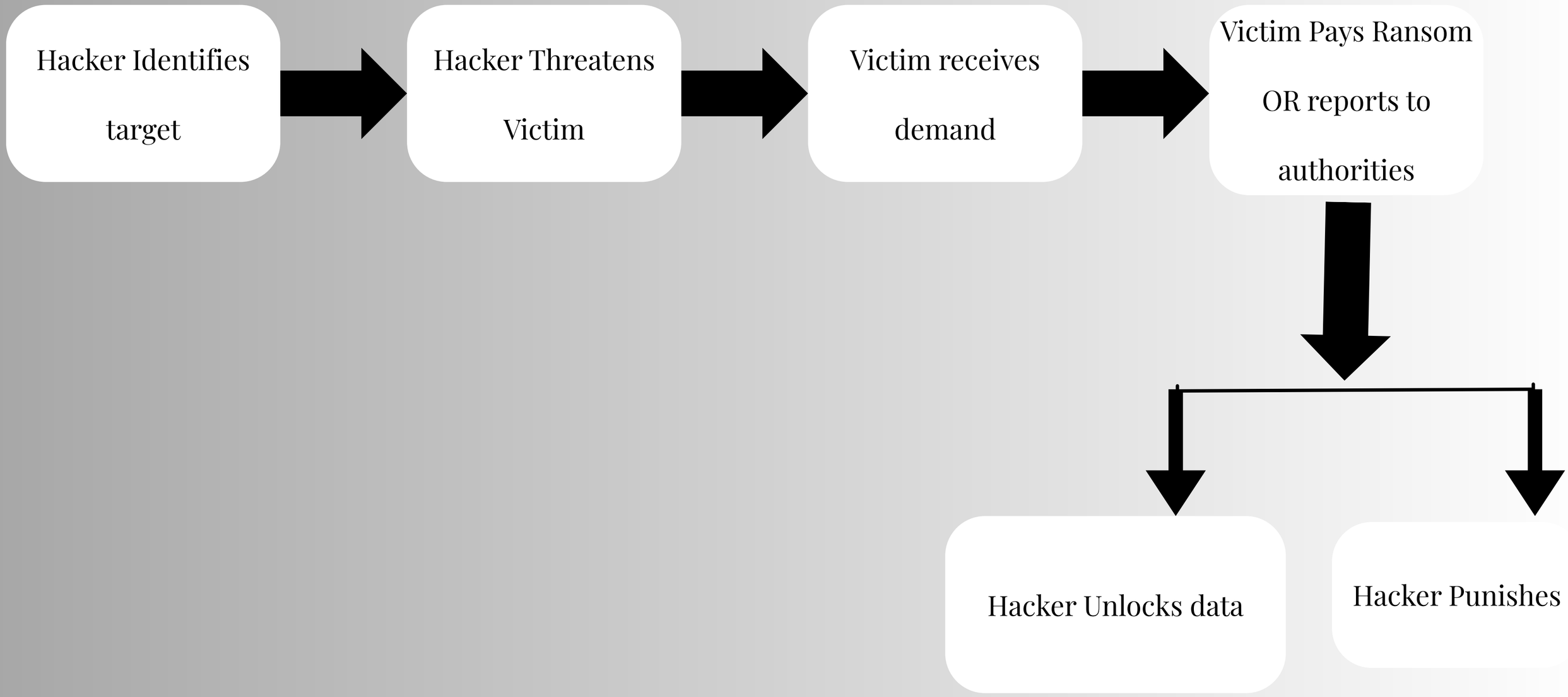
  Example: Ransomware locks all files on a company computer and demands money to unlock them.

- **Demand for Money** – Extortion usually involves asking for ransom, cryptocurrency, or bank transfers.

  Example: A hacker sends an email demanding $1000 to prevent releasing private photos.

- **Psychological Pressure** – Criminals create fear or urgency to force victims to pay.

  Example: “If you don’t pay in 24 hours, your website will be permanently deleted.”


Hacker Identifies target
Hacker Threatens Victim
Victim receives demand
Victim Pays Ransom OR reports to authorities
Hacker Unlocks data
Hacker Punishes

D. Drug Trafficking

- Drug Trafficking is the illegal production, transportation, and selling of drugs for profit.

Key Points with Examples:

- **Illegal Trade of Drugs** – Selling or moving drugs like heroin, cocaine, or marijuana is illegal.

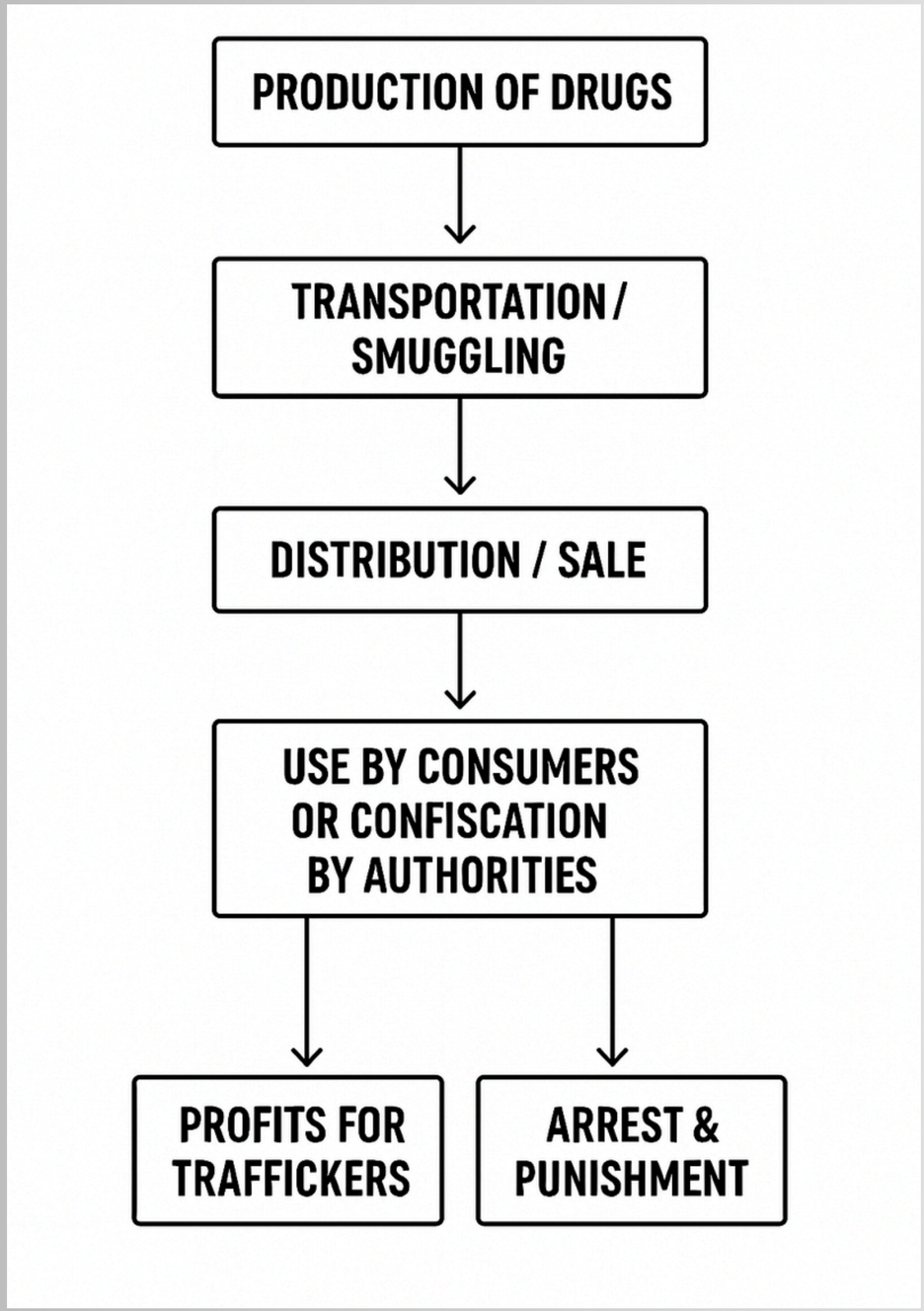
  Example: Smugglers transporting drugs across borders secretly.

- **Cross-Border or Local** – Trafficking can happen within a country or internationally.

  Example: Drugs sent from one country to another hidden in shipments.

- **Criminal Networks** – Organized groups often control production, distribution, and sales.

  Example: Mafia or gangs running a drug distribution chain in a city.


PRODUCTION OF DRUGS
TRANSPORTATION / SMUGGLING
DISTRIBUTION / SALE
USE BY CONSUMERS OR CONFISCATION BY AUTHORITIES
PROFITS FOR TRAFFICKERS
ARREST & PUNISHMENT

E. Cyber Terrorism

- Cyber Terrorism is when terrorists use the internet or computers to attack, threaten, or disrupt

  a country's systems, causing fear, damage, or harm.

Key Points with Examples:

- **Use of Technology for Terror** – Attacks are done using computers, networks, or online tools.

  Example: Hacking a government website to spread propaganda.

- **Disrupts Services or Systems** – Can cause damage to critical systems like power grids, banks, or transport.

  Example: Virus attack on a city's power supply causing blackout.

CYBER TERRORISM

COMPUTER INFECTION

↓

HIJACKING ESSENTIAL OPERATIONS

↓

DISRUPTION & DAMAGE

CYBER TERRORISM

PLANNING → IMPLEMENTATION TARGET → ATTACK

WORK FLOW

Information Security

Definition:

- Information Security is the practice of protecting data, information systems, and networks from unauthorized access, use, disclosure, disruption, modification, or destruction.

Key Points with Examples:

- **Protects Confidentiality** – Ensures only authorized people can access information.
- **Maintains Integrity** – Ensures information is accurate and not tampered with.
- **Ensures Availability** – Keeps information and systems accessible to authorized users when needed.
- **Prevents Cyber Threats** – Guards against hacking, malware, and data theft.

Threat to Information Security

1. Malware Attacks

- Harmful software like viruses, worms, trojans, ransomware that damage systems or steal data.
- Example: Ransomware that locks files and demands money.

2. Phishing & Social Engineering

- Tricking users with fake emails, websites, or calls to steal passwords or bank details.
- Example: A fake bank email asking for login details.

3. Insider Threats

- Employees or authorized users misuse their access and leak sensitive data.
- Example: A staff member selling customer information.

4. Denial of Service (DoS/DDoS) Attacks

- Attackers overload a system or website so it crashes or becomes unavailable.
- Example: An e-commerce site going down during heavy traffic attack.

Need of Information Security

1. Protect Confidential Data

- Safeguards sensitive info like ID numbers, bank details, and medical records.
- Example: Prevents identity theft and financial fraud.

2. Ensure Privacy

- Keeps personal data on apps and social media safe from misuse.
- Example: Protects chats, emails, and photos from leaks.

3. Prevent Financial Loss

- Stops phishing, ransomware, and scams that cause money loss.
- Example: Secure customer card details in online stores.

4. Maintain Trust & Reputation

- Protects customer data to avoid loss of trust and legal issues.
- Example: Banks use encryption to secure transactions

THANK YOU