SUB: cybersecurity

Unit 2: Cyber Offenses and Cyberstalking

Prof. Morade D.S.

Cyber Offenses:

Definition:

"Cyber offenses refer to illegal activities that are carried out in a sophisticated manner using a computer as either a tool or a target, or both."

The following are the offences covered by the Information Technology Act of 2000:

1] Tampering with the source documents on the computer.

2] Using a computer system to hack.

3]Penalty for breach of privacy and confidentiality.

4]Publishing obscene information in an electronic format.

Criminals Plan:

Technology Use – Good & Bad

- Technology can be used for both **positive and negative** purposes.
- People with bad intentions may use it to:
  - Cause damage
  - Do **illegal activities**
  - Harm others for **personal gain**

Cybercrimes – Borderless Crimes

- In today's world, crimes using the internet can happen **across countries**.
- Common cybercrimes include:
  - **Hacking**
  - **Cyberterrorism**
  - **Password sniffing**
  - **Computer viruses**
  - **Network intrusions**

Purpose of Cybercriminals

- They use computers and internet to:
  - Steal **data**
  - Access **contacts, passwords, account info**
  - Commit **illegal acts**

Lack of Awareness

- Criminals take advantage of the fact that many people **don't know much** about:
  - **Cyber laws**
  - **Cybercrime threats**

Tools to Find Weakness

- Cybercriminals use different tools and methods to find **weak points** in:
  - Individuals
  - Groups
  - Organizations

Crackers vs Hackers

- **Cracker**: A person who breaks into computers with **bad intentions**.
- **Hacker**: A person who loves experimenting with computers. Not always bad — some are just curious and smart.

Categories of Cybercrime Cyber Attacks (Phases):[4M]

Types of Cybercrime (based on target):

a) Crimes Against Individuals

- Targets one person
- Examples: Cyberbullying, harassment, stalking, identity theft

b) Crimes Against Property

- Targets devices or digital property
- Example: Malware, ransomware, stealing files

c) Crimes Against Organizations

- Targets companies or governments
- Known as **Cyber Terrorism**
- Goal: To **steal data**, **damage files**, or **shut down systems**

- **Based on Attack Pattern:**

a) Single Event

- Crime happens **once**
- Example: Clicking a phishing link and losing data

b) Series of Events

- Attacker builds a relationship, then uses it to harm
- Example: Grooming victim online and later exploiting them

- **Categories of Vulnerabilities**

Cybercriminals look for weak points such as:

- Unprotected computers
- Default system settings
- Weak passwords
- Remote access servers with poor security

These weaknesses help them **break in easily**.

i. Purpose of Cyber Attacks

- Criminals use attacks to find and exploit the **vulnerabilities** of the victim.
- Victim can be a **person, group, or organization**.

ii. Types of Attacks

a) Passive Attack

- Goal: **Gather info** secretly
- No changes are made to the system
- Example: Listening to conversations, watching without permission

b) Active Attack

- Goal: **Change, damage, or stop** system
- May delete files, spread viruses, or alter data

iii. Attackers Can Be:

a) Inside Attacker

- Works **within the organization** (like an employee)
- Misuses access to do harm

b) Outside Attacker

- **Not a part of the organization**
- Tries to break into systems from outside (e.g., hacker)

iv. Phases in Cybercrime Planning

Phase 1: Reconnaissance

- Also called **information gathering**
- It is a **passive attack**
- Attacker collects details about the target (IP, system info, habits)

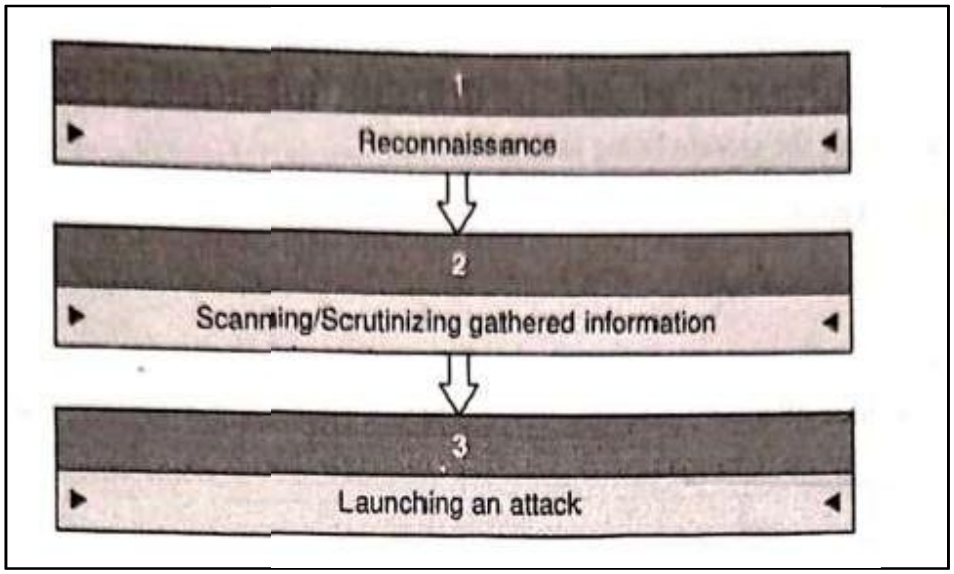
Phase 2: Scanning and Scrutinizing

- Attacker checks if collected data is **valid**
- Finds **loopholes** or weak spots to break into the system

Phase 3: Launching the Attack

- Final step
- Criminal uses weaknesses to **attack**, **steal info**, or **control** the system

The criminal's plan undergoes three prime phases:



1] Reconnaissance:

- Reconnaissance is the first phase of criminal plan. It is also called as information gathering phase, wherein as much as possible information is gathered regarding victims or targets.
- In hacking world, reconnaissance phase starts with "**Footprinting**"

"Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks." To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Footprinting can be categorized based on the manner of collecting necessary information.

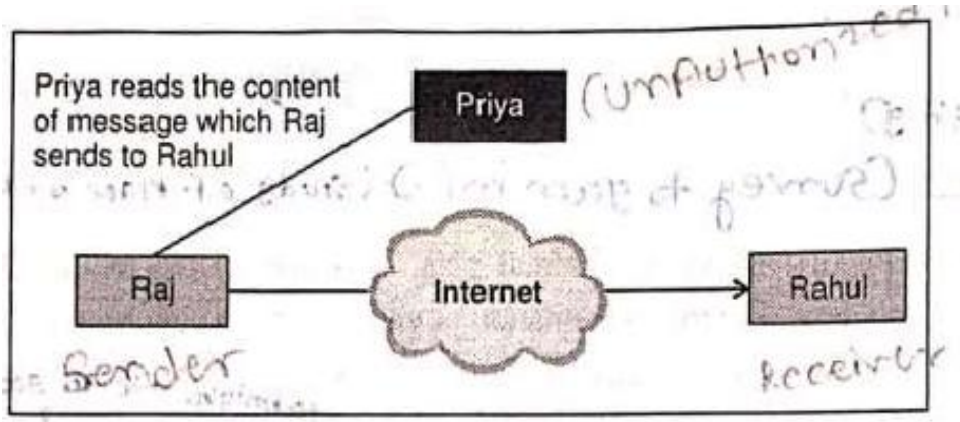
- **Passive Attack:**

Passive attack is also called as Passive footprinting. A passive attack tries to gain knowledge of the system but does not affect system resources.

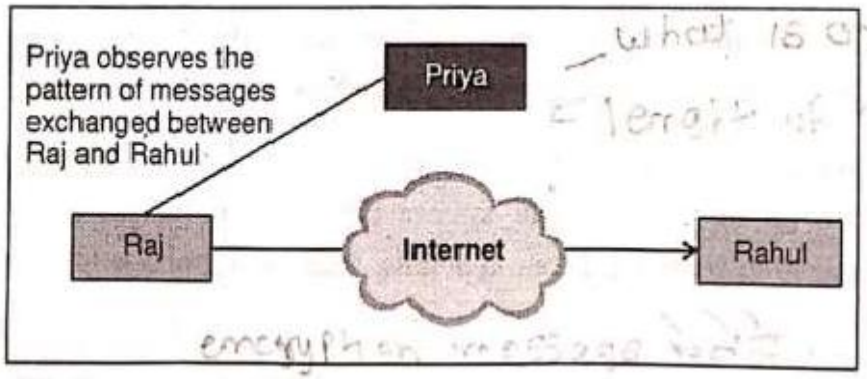
Types of Passive Attacks:

Passive attacks are of two types:

***1] The release of message content*:** In the release of message content, sensitive or confidential Information may leak through an electronic mail, conversation over telephone or through transferred files.



2] Traffic analysis: Traffic analysis attack is used to analyze the traffic, to find out the location, discover communicating hosts and scrutinize the occurrence and length of exchanged messages.

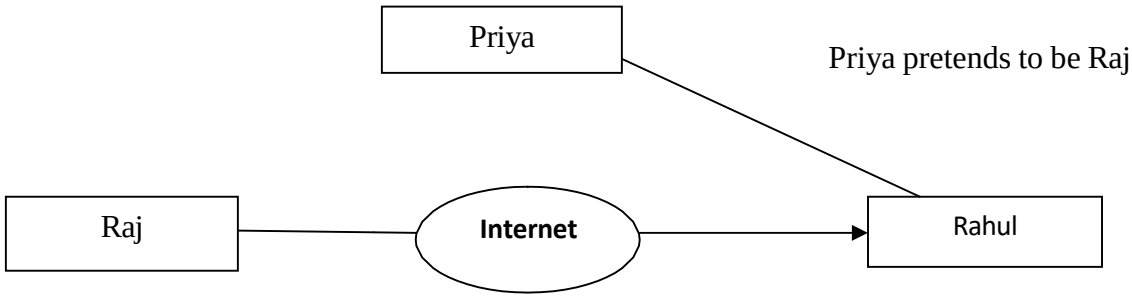


- **Active Attack:**

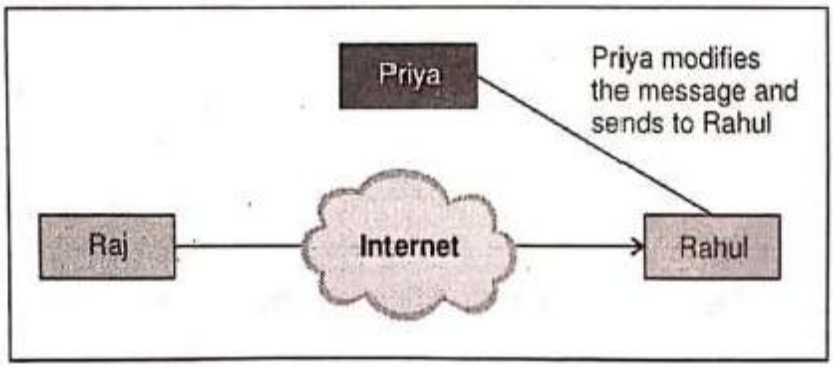
Active attack is also called as Active footprinting. Active attack tries to modify system resources.

Types of Active Attacks:

1] Masquerade: Masquerade attack occurs when one entity pretends to be different entity.

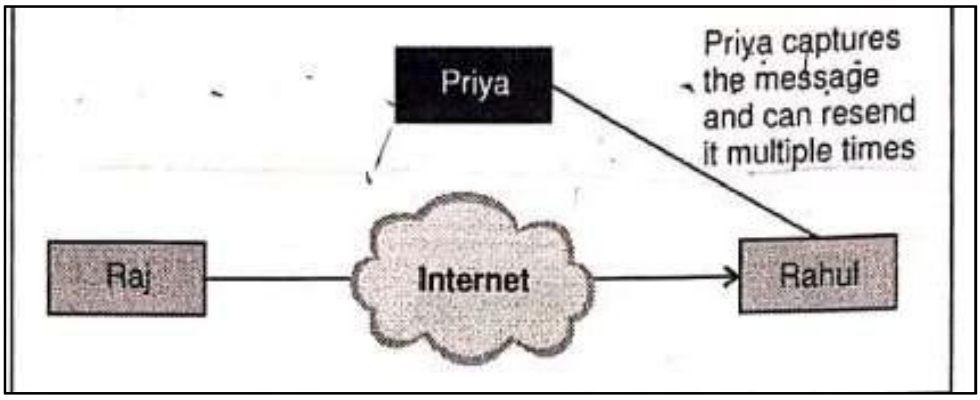


2] Modification of Messages: Modification of messages means that several parts of a message is modified.

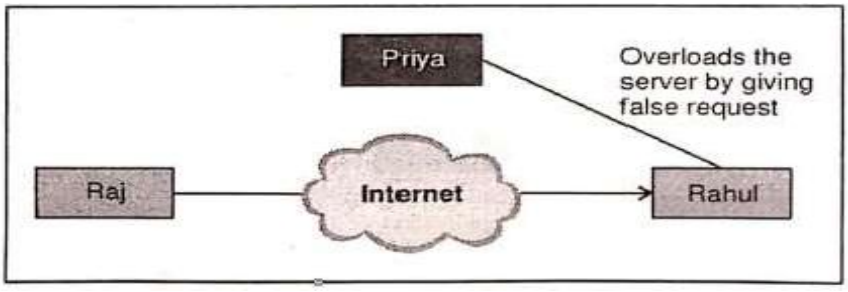


3] Repudiation: Repudiation is a type of attack made by either sender or receiver. The sender or receiver can refuse later that he/she has send or receive a message.

4] Replay: Replay attack entails passively capturing a message and then transmitting it in order to accomplish an authorized effect.



5] Denial of Service: Denial of service stops regular use of communication services. This type of attack might have a specific victim.



2] Scanning/Scrutinizing Gathered Information:

After collecting basic information during the reconnaissance **phase, the attacker now starts checking the details more deeply. This step is called** scanning or scrutinizing**.The goal is to** find weak points **(vulnerabilities) that can be used to launch an attack.**

i) **Port Scanning:** Port (doorways to a computer) scanning is used to identify open as well as closed ports and services.

Example:
An attacker scans a computer and sees that **Port 80 (HTTP)** is open. This tells them that a website is running and they might try to hack it.

ii) **Network Scanning:** Network scanning is used to be aware of IP addresses and other associated information regarding the computer network system.

Example:
The attacker finds out that several devices are connected to the same Wi-Fi and one of them has weak security.

iii) **Vulnerability Scanning:** Vulnerability scanning is used to recognize existing weaknesses of the system.

Example:
If an old version of Windows is installed without security updates, it becomes a vulnerability that can be attacked.

3] Launching an Attack (Gaining and Maintaining the System Access):

- This is the **final step** in a cyberattack.
- After collecting information (reconnaissance) and finding weaknesses (scanning), the attacker is now ready to **launch the actual attack**.

Goal:

To **gain access** to the victim's system and **maintain control** for a long time without being detected.

Steps to Launch the Attack:

1. Crack or Break the Password

- The attacker tries to **guess or hack** the user's password.
- Techniques used:
  - Brute force (trying many combinations)
  - Social engineering (tricking the person to share password)
  - Keyloggers (software that records keystrokes)

Example: Trying hundreds of combinations to unlock an admin account.

2. Use the Password

- Once the password is cracked, the attacker **logs into the system** like a normal user.
- This helps avoid detection, as it looks like a **genuine login**.

Example: Hacker logs into a company server using the stolen credentials.

3. Install Malicious Software or Commands

- Now the attacker runs **malware**, viruses, or special commands to:
  - Steal more data
  - Damage or control the system
  - Create a **backdoor** for future access

Example: Installing a Trojan to secretly monitor everything the user does.

.

Social Engineering and Classification of Social Engineering:

- "Social engineering is the method to manipulate people to obtain sensitive or confidential information"
- Criminals make use of social engineering strategies since it is generally effortless to utilize your natural liking to trust than it is to find out ways to hack your software.

Classification of Social Engineering: Types of Social Engineering

1. Human-Based Social Engineering

This involves **direct human interaction** (face-to-face, phone calls, or observation) to fool someone into giving access or information.

1. **Impersonating an Employee or Valid User**
   - Attacker pretends to be a **genuine employee** of the organization.
   - Tries to **gain physical or system access** by acting confident or wearing a company ID.
   - Example: Enters office claiming, "I forgot my access card."
2. **Posing as an Important Person (VIP Fraud)**
   - Pretending to be a **senior officer**, manager, or CEO.
   - Pressures lower staff to **share information quickly** without verification.
   - Uses urgency or authority tone.
3. **Using a Third Person's Identity**
   - Claims to have **permission** from another real person (who may be on leave or unavailable).
   - Example: "Mr. Sharma told me to take this report."
4. **Calling Technical Support / Helpdesk**
   - Pretends to be a **user who forgot their password**.
   - Tries to get the support team to **reset or reveal login details**.
   - Uses sympathy or urgency.
5. **Shoulder Surfing**
   - **Looking over someone's shoulder** to watch them typing their password or PIN.
   - Can happen in public places like ATMs, cyber cafés, or offices.
6. **Dumpster Diving**
   - **Searching through trash bins** to find discarded papers or items.
   - Looks for documents, sticky notes, printed passwords, or confidential printouts.

2. Computer-Based Social Engineering

This uses **computers, the internet, or digital communication** to deceive users and steal data.

1. **Fake Emails (Phishing)**
   - Emails appear to come from **trusted companies** (like banks or websites).
   - Ask users to click links or provide login details.
   - The link leads to a **fake website** that looks like the real one.
   - Example: "Your account is blocked. Click here to unlock."
2. **Email Attachments**
   - Emails come with **attachments** that may seem like invoices, offers, or resumes.
   - When opened, they **install malware, keyloggers, or trojans**.
   - These programs **steal data silently**.
3. **Pop-up Windows (Fake Alerts or Ads)**
   - Fake pop-ups saying things like:
     - "You've won a prize!"
     - "Your system is infected. Click to fix."
   - Clicking downloads harmful software or redirects you to malicious sites.

Cyberstalking:

- Cyberstalking is the way to harass or stalk an individual, group or the organization.

- Cyberstalking is a type of cyber crime, which is conducted using any electronic devices or internet such as messages on discussion forum, websites, e- mail. It may include monitoring, blackmail, identity theft, etc.

❖ Types of Cyberstalking:

1] E-mail Stalking: Email stalking is the way to directly communicate through E-mail.Unsolicited e-mails are one of the most popular kind of harassment, like hatred, or threatening mail. It also includes other types of harassment like online junk mails in huge number, delivering target viruses.

2] Internet Staking: In this kind of stalking, stalkers can widely utilize the internet in order to insult and jeopardize their victims.

3] Computer Stalking: Computer stalking is the way to have unauthorized control over another person's computer.A cyber stalker frequently interacts with their victim directly as soon as the victim device connects to the internet in some way.The only way to stop the stalker is to completely disconnect the line, and then reconnect with a completely new number.

❖ Types of Stalkers

1] Psychotic: A study shows that often the stalkers have past psychotic history. Or psychotic disorder such as schizoaffective, hallucinationdisorder.

2] Nonpsychotic: On the other hand, the majority stalkers are nonpsychotic and might show disordersincluding adjustment disorder, major depressionThe nonpsychotic stalkers' hunt of victims is mainly angry,projection of blame,jealousy.

Types of stalkers

1] Rejected stalkers: Rejected stalkers are the stalkers who track their victims in order to reverse, or avenge a refusal (such as divorce, separation)

2] Resentful stalkers: are the stalkers who make a vendetta due to a sense of complaint against the victims.desire to panic and distress the victim.

3] Predatory stalkers: Predatory stalkers are the stalkers who spy on the victim to prepare as well as plan an attack.

Cybercafe and Cybercrimes:

- Cybercafe is known as hotspot for the cybercrime. It is the preferred place of the criminals to attempt cyber-attack.
- Criminals usually target a single personal computer PC and prepare it for their usage.Cybercriminals will frequently visit these cafés at a predetermined time and frequency, such as every other day or twice a week.

❖ **some safety and security tips for using a computer in a cybercafé:**

1] Always logout: Always click "logout" or "sign out" before leaving the system while checking e-mails, logging into messaging services such as instant messaging, or using any other service that requires a login and password.

2] Stay with the computer: It is not advisable to leave the computer unattended while surfing or browsing. If you need to leave the house, log out and close any browser windows before leaving.

3] Clear history and temporary files:clear history & temporary files. Pages you've viewed are saved in the history folder and temporary internet files in internet explorer. If that option was enabled on the machine you used, your passwords could also be saved in the browser.

4]Be alert: When using a public computer, one should be vigilant and mindful of their surroundings. Getting your username and password by looking over your shoulder is a simple process.

5] Avoid online financial transactions: Online banking, shopping, and other transactions that involve personal, confidential, or sensitive information, such as credit card or bank account information, should be avoided

What is a Botnet?

1. **Definition**:
   The word *Bot* stands for **robot**, and *net* means **network**.
   So, **Botnet = Robot + Network**.
2. **Meaning**:
   A **botnet** is a **network of hijacked (compromised) internet-connected devices** infected with **malicious software (malware)**.
3. **Terminology**:
   - Infected devices are called **Bots** or **Zombies**.
   - The person who controls them is called a **Bot Herder**.
4. **Control**:
   The **Bot Herder** can remotely send commands to all bots from a **central location**.
5. **Purpose**:
   A botnet is used to perform **large-scale illegal activities**, such as:
   - Data theft
   - Server crashing (DDoS attacks)
   - Spamming emails
   - Spreading malware
   - Generating fake internet traffic

Botnet Architecture

Botnets can be controlled using two main methods:

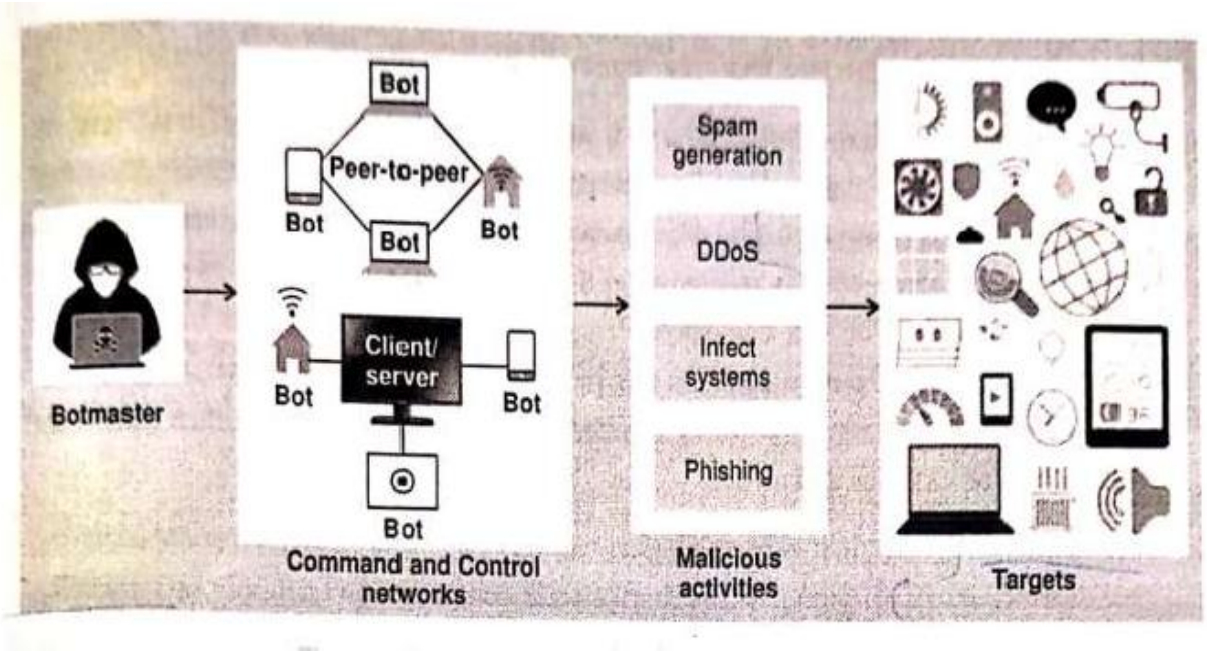
1. Client-Server Botnet

1. In this setup, a **central Command and Control (C&C) server** is used.
2. All bots (infected devices) **connect to this central server** to receive instructions.
3. Communication often happens via protocols like **IRC (Internet Relay Chat)**.
4. Bots usually stay **inactive (dormant)** until they get a command from the C&C server.
5. This method is **easier to control** but also **easier to detect and shut down** by cybersecurity teams.

---

2. Peer-to-Peer (P2P) Botnet

1. Instead of using a central server, **each infected device (bot) communicates with other bots directly**.
2. Bots can **search for other infected devices or malicious websites** to get updates.
3. Bots **share new commands or updated malware** with one another.
4. This method is **decentralized**, making it **harder to detect** and **harder to stop**.
5. It's becoming **more popular** because **cybercriminals want to avoid detection** from law enforcement and cybersecurity systems.



Fuel for Cyber Crime:

1] Money:

Many types of cybercrimes, such as ransomware, phishing, and data theft, are motivated by monetary gain. Extorting money from victims directly, whether individuals or through an organisation, is the financial gain associated with these forms of cybercrimes.

2] Government:

Cybercrime is becoming increasingly popular as a technique for achieving political objectives. Hacking or shutting down a country's power supply, manipulating elections are all *examples* of this. Public administration, defense, energy, and utilities are common targets, with the goal of gaining information or disrupting or damaging operations.

3] Competition:

Organizations utilize hackers to evaluate their own security, but they are also used for corporate espionage on a regular basis. Some of these attacks are aimed at preventing competitors from taking part in important events, while others aim to shut down internet enterprises for months at a time. The goal of this type of attack is to cause havoc and attract customers away from competitors' establishments.

4] **Cyberwarfare:**

The use of digital attacks (such as computer viruses and hacking) by one government to impair the computer systems of another is known as cyberwarfare. The goal is to weaken the target country's key systems.

Attack Vector:

Attack Vector **means the way an attacker uses to get into a computer or network to cause harm.**

❖ Common Attack Vectors:

1. **Attack by E-mail:**
   - Email is a common way to send **malware, viruses, ransomware**.
   - These emails may look genuine but often contain **suspicious links or attachments**.
   - Example: You receive an email saying "Your package is delayed" with a link—once clicked, it downloads a virus.
2. **Attachments:**
   - Files like `.exe`, `.pdf`, `.docx` might contain **Trojan horses or spyware**.
   - Example: You open an invoice in an email from an unknown sender, and it secretly installs spyware.
3. **Deception Attacks (Social Engineering):**
   - Hackers **manipulate people** into revealing confidential data (passwords, PINs).
   - Techniques: Fake job offers, fake tech support, urgent banking messages.
   - Example: A call pretending to be from your bank asking for your OTP.
4. **Hackers:**
   - Individuals or groups using advanced tools to **bypass security systems**.
   - They may install **Trojans, keyloggers, backdoors** to access and control systems.
   - Example: A hacker exploits an outdated operating system to install malware.
5. **Heedless Guests (via webpages):**
   - Fake or cloned websites look real and ask for **login details or credit card info**.
   - Example: A site that looks like Facebook but is actually a trap to steal passwords.
6. **Worms:**
   - Self-replicating malware that spreads via **networks, emails, USB drives**.
   - Example: Opening a shared folder infected with a worm that copies itself to your PC.
7. **Malicious Macros:**
   - Embedded scripts in **MS Word or Excel files**.
   - Example: Opening a Word resume with macros that activate malware.
8. **Foistware (Sneakware):**
   - Software installed **without your knowledge**, often bundled with other apps.
   - Example: You install a free media player, but it also installs spyware.
9. **Viruses:**
   - Programs that attach to other files and activate when opened.
   - Example: A cracked game download contains a virus that corrupts your files.

CYBERCRIME: MOBILE AND WIRELESS DEVICES

Mobile devices are **prime targets** for hackers due to:

- High personal data storage
- Constant internet connectivity
- Often weaker security setups

Key Points:

- Mobile devices hold emails, passwords, bank details, location data.
- Attacks can come through Wi-Fi, Bluetooth, or by physically accessing the device.

Proliferation of Mobile Devices

- Devices are getting **smaller and smarter** (smartphones, tablets, smartwatches).
- Example: 10 years ago, phones were mostly for calling. Today, they are **mini-computers**, making them more vulnerable.

Trends in Mobility

- Modern mobile phones have **fast internet, apps, and cloud access**.
- **iPhones and Android** are examples of devices that are commonly targeted because:
  - They store important data.
  - They are always online.
  - Users install unknown apps.

Mobile Network Attacks

Attacks happen via:

1. Outside Mobile Network:

- Through **public internet, rogue Wi-Fi hotspots**, phishing links.

2. Inside Mobile Network:

- Through **devices connected to the mobile network** like phones, laptops, tablets.

Types of Attacks:

1. **Malwares, Viruses, Worms**
   - Example Malware:
     - **Skull Trojan**: Disables apps and replaces icons with skulls.

- **Cabir Worm**: Spreads via Bluetooth.
- **Mosquito Trojan**: Comes in games, secretly sends messages.
- **Brador Trojan**: Gives hackers remote access to your mobile.
- **Lasco Worm**: Spreads files via Bluetooth using the phone's contacts.

2. **DoS (Denial of Service):**
    - Overloads a phone's network or resources.
    - Example: A hacker floods your phone's internet, causing it to hang or lose signal.
3. **Overbilling Attacks:**
    - Hijack your internet or SMS service to make you **pay extra unknowingly**.
4. **Spoofed PDP Attacks:**
    - Exploit mobile internet protocols to **intercept or manipulate data**.
5. **Signaling-level Attacks:**
    - Target the **phone's calling and messaging setup** to disrupt or intercept communication

❖ Credit Card Frauds in Mobile and Wireless Computing Era:

- In today's world, electronic gadgets had become an important part of business. So, it brings many challenges for the business to secure these devices from being a target of cybercrime.
- E-commerce transactions from mobile devices. It is most frequently utilized by businesses that work mainly in a mobile environment.

Basic flow of credit card transactions involves:

1]Cardholder magnetic stripe card swiped to obtain magnetic stripe data.
2] Merchant sends a transaction to bank.
3] Security control module with PIN pad asks PIN **of** cardholder for transaction.

4] The credit card transaction is complete.

❖ Types of credit card frauds :

➢ Traditional Techniques

1. Paper-Based Application Fraud

Criminals use **fake documents** like false ID proof, fake address or utility bills to apply for a credit card in someone else's name.

- **ID Theft:** Pretending to be another person.
  - **Example:** A criminal uses your Aadhaar number and fake documents to get a credit card in your name.
- **Financial Fraud:** Giving fake salary or job details to get a credit card.
  - **Example:** A person lies about their income and employer to get a credit card and then doesn't repay the bill.

2. Illegal Use of Lost/Stolen Cards

Stolen cards are used to make purchases **before the real owner can block them**.

- **Example:** A thief steals your wallet and uses your credit card at petrol pumps or online shopping within minutes before you report it.

➢ II. Modern Techniques

1. Skimming

Criminals use **fake card readers** or software to **copy your card's magnetic strip or chip data**.

- **Example 1:** A skimming device is secretly attached to an ATM or payment machine. When you swipe your card, the device saves your details.

- **Example 2:** A phishing website looks like a bank login page. When you enter your card info, it gets saved by hackers.

2. Triangulation

Involves three parts:

1. A **fake website** offers cheap goods.
2. You enter your **credit card info**.
3. The criminal uses that info to buy goods from a **real website**.

- **Example:** You order a smartphone for ₹4999 from a fake site. Your card details are stolen and used to buy expensive gadgets from Amazon, shipped to another address.

3. Credit Card Generators

Hackers use **software to create random valid credit card numbers** (based on common algorithms).

- **Example:** A criminal uses a card generator tool, gets a valid number, and uses it for trial subscriptions or online purchases.

SECURITY CHALLENGES POSED BY MOBILE DEVICES

Challenges at Two Levels:

- ***Micro-Level (Device Side):***

1. Weak passwords
2. No antivirus protection
3. Risky app permissions
4. Outdated operating systems

- **Example:** You install a free photo editing app that asks for SMS, contacts, and camera access—then sends your data to a hacker's server.

- ***Macro-Level (Organization Side):***

Companies allowing employees to use their own phones for work (BYOD - Bring Your Own Device) can lead to data breaches.

- **Example:** An employee opens a malware-infected link on their phone which is also used to access company emails—compromising company data.

Key Mobile Security Techniques:

- **Manage app permissions:** Allow only necessary permissions.
- **Use encryption:** Encrypt phone data to keep it safe even if lost.
- **Biometric Authentication:** Face ID, fingerprint lock.
- **Disable unused features:** Turn off Bluetooth, NFC, etc. when not needed.

UTHENTICATION SERVICE SECURITY

There are **two major types of security** in mobile computing:

1. Device Security:

Protect the mobile device using:

- PINs, passwords
- Biometric locks
- App-lockers
- Disk encryption

Example: Setting up Face ID and strong password on your phone.

2. Network Security:

Ensure **only trusted and authorized devices** can access the network (like mobile data or Wi-Fi).

- **Example:** A mobile operator verifies your device's IMEI number before allowing data usage.

Types of Attacks:

Push Attack:

Harmful data is **sent directly** to your device.

- **Example:** You receive a push notification from a fake app update, and when you click it, malware is downloaded.

Pull Attack:

Your device **requests harmful data** unknowingly.

- **Example:** Your phone automatically connects to a fake Wi-Fi and downloads harmful content.

Crash Attack:

The hacker sends a **huge amount of traffic or files** to your phone to **make it crash** or freeze.

- **Example:** A sudden flood of pop-ups makes your phone unresponsive.

ATTACKS ON MOBILE PHONES

Factors for Increased Mobile Attacks:

1. Mobile phones contain **lots of personal data** (photos, emails, passwords).
2. Phones are **always connected** (Wi-Fi, mobile data).
3. People use **public Wi-Fi** without protection.
4. Many users **don't understand mobile security**.

4 Types of Mobile Threats:

1. App-Based Threats

- Dangerous apps can access personal data.
- **Example:** A flashlight app that secretly sends your contact list to a server.

2. Web-Based Threats

- Fake links (via email, SMS, WhatsApp) asking for card details or login info.
- **Example:** An SMS saying "You won ₹10,000. Click here." You click and enter your bank details—then money is stolen.

3. Network Threats

- Hackers set up **free public Wi-Fi** to trap data.
- **Example:** You connect to free café Wi-Fi, but it's a fake one. All your activity is being monitored.

4. Physical Threats

- Lost or stolen phones that are not locked properly can be easily misused.
- **Example:** A thief finds an unlocked phone and accesses your apps, bank info, and social media.

.

Questions

1. **Define attack vector**
2. **What is social engineering**
3. **What is cyber stalking**
4. **Explain different types of credit card fraud**
5. **Explain human based and computer based social engineering**
6. **What are the different attack launched with attack vector and explain it**
7. **Explain how botnets can be used as a fuel to cybercrime**
8. **Describe active and passive attacks Discuss types of active and passive attack.**