Times asked: 6 times
5 times
4 times
3 times
2 times
1 time

# indicates 5-mark question

Cyber Security Laws Question bank

1. Introduction to Cybercrime

1. What is Cybercrime? Who are Cybercriminals? Explain.
2. Explain the classification of Cybercrimes with examples.
3. How Cybercrimes differ from most terrestrial crimes? #

2. Cyber offenses and Cybercrime

4. What are the steps involved in planning of cyberattacks by a criminal.
5. Explain the basic security precautions to be taken to safeguard Laptops and Wireless devices.
6. What are the illegal activities observed in Cyber Cafés? What are the safety and security measures while accessing the public computers in Cyber Café?
7. What are the different Security risks for Organizations? #
8. What are botnets? How is it exploited by an attacker to cause cyber-attack?
9. What are the vulnerabilities and security challenges faced by mobile devices? #
10. Explain various types of credit card frauds.
11. Write a short note on: Cyberstalking and harassment. #
12. Write a short note on: Mobile/Cell phone attacks. #

3. Tools and Methods used in Cyberline

13. Explain the different types of buffer overflow attacks and describe the techniques used to mitigate them.
14. Explain the SQL Injection attack with its steps. Mention countermeasures to prevent it.
15. Explain DOS and DDOS attacks in detail.
16. What is a vishing attack? How does it work, and how can it be prevented?
17. Explain phishing attacks, their types, and prevention methods.
18. Write a short note on Trojan horse and backdoor. #
19. Explain different password cracking techniques. #
20. Difference between virus and worm. #

4. The concept of Cyberspace

21. What is digital evidence? Mention its types and common sources.
22. Explain e-contracts and its different types.
23. What is e-commerce? Discuss types of e-commerce.
24. Explain why do we need cyber laws? Discuss about the challenges to Indian cyber laws.
25. Write a note on Intellectual Property Aspects in cyber law.
26. Explain electronic banking in India and what are laws related to electronic banking in India.

5. Indian IT act

27. Explain the objectives and features of IT Act 2000.

6. Information Security Standard Compliances

28. Write a short note on HIPAA. #
29. Write a short note on SOX. #

	1	2	3	4	5	6
2025 May	15	45	30	35	5	5
2024 Dec	20	50	30	20	0	5
2024 May	15	50	45	15	0	10
2023 Dec	10	15	40	40	10	10
2023 May	15	45	35	35	0	5
2022 Dec	15	30	35	25	10	10
Estimate	**15**	**45**	**35**	**25-35**	**5-10**	**5-10**
Total	90	235	215	170	25	45

Asked once:

# indicates 5-mark question

1. Introduction to Cybercrime

1. Differentiate between Cybercrime and Cyber fraud. #

2. Cyber offenses and Cybercrime

2. Explain about the impact of Cybercrimes in Social Engineering.
3. Outline the challenges for securing data in business perspective. #
4. List general guidelines for password policies. #
5. Explain various threats associated with cloud computing. #
6. Explain different attack vectors in cyber security. #

3. Tools and Methods used in Cyberline

7. Write a short note on Salami attack. #
8. Explain Identity theft in detail. #
9. Write a short note on Steganography. #

4. The concept of Cyberspace

10. What is WIPO? List treaties prepared by WIPO.
11. Write a short note on Cyberdefamation. #

5. Indian IT act

-

6. Information Security Standard Compliances

12. Explain what the Information Security Standard is. #

Cyber Security Laws Answer bank

# indicates 5-mark question

1. Introduction to Cybercrime

1. What is Cybercrime? Who are Cybercriminals? Explain.

Cybercrime:

Cybercrime refers to any illegal activity performed using computers, networks, mobile devices, or internet as a tool, target, or both. Cybercrime targets confidentiality (stealing data), integrity (altering data), and availability (denying access) of systems.

Cybercrime can be:

- **Against individuals** (identity theft, harassment)
- **Against property** (hacking, system damage)
- **Against governments/organizations** (hacking government databases, DDoS attacks)
- **Against society** (fake news, illegal online activities)

Cybercriminals:

Cybercriminals are individuals or groups who commit cybercrimes for personal gain, revenge, political motives, or disruption. They can be:

- **Hackers** – Gain unauthorized access to systems to steal, alter, or destroy data.
- **Fraudsters** – Use deception online to obtain money, credentials, or other valuables.
- **Cyber terrorists** – Launch attacks on critical systems to cause fear, chaos, or long-term disruption.
- **Insiders** – People within an organization who exploit their access for theft, sabotage, or leaking information.
- **Script kiddies** – Inexperienced attackers who use ready-made hacking tools without real technical knowledge.

2. Explain the classification of Cybercrimes with examples.

Cybercrimes can be classified based on the target, intention, and impact of the offense. The major classifications are:

1. Cybercrime Against Individuals

Crimes that directly target a person's identity, privacy, or personal data.

1. **Phishing** – Tricking users through fake emails/websites to steal login credentials.
   Example: Fake "bank verification" email stealing password.
2. **Identity Theft** – Stealing Aadhaar, PAN, bank details for fraudulent transactions.
   Example: Using stolen card details for online purchases.
3. **Cyberstalking** – Monitoring or harassing someone online without consent.
   Example: Constant messages and tracking social media activity.
4. **Online Defamation** – Posting false/obscene content to damage reputation.
   Example: Fake posts targeting someone's character.
5. **Password Cracking** – Illegally guessing or brute-forcing passwords.
   Example: Using keyloggers or dictionary attacks.

2. Cybercrime Against Property

Crimes that target digital data or computer systems.

1. **Hacking** – Breaking into systems to steal or alter data.
   Example: Hacking a company server to steal customer records.
2. **Ransomware Attack** – Encrypting files and demanding ransom.
   Example: WannaCry ransomware locking hospital databases.
3. **SQL Injection** – Injecting malicious SQL code into database queries.
   Example: Extracting credit card numbers from an e-commerce website.

3. Cybercrime Against Organizations / Government

Crimes that disrupt operations or steal sensitive institutional information.

1. **Cyber Espionage** – Stealing government or corporate intelligence.
   Example: Hacking defense ministry systems.
2. **Website Defacement** – Altering website content to display unauthorized messages.
   Example: Defacing a university homepage with political messages.
3. **DDoS Attack** – Flooding servers with traffic to crash services.
   Example: Bringing down online banking portals.

4. Cybercrime Against Society

Crimes that negatively impact the public or violate social and legal norms.

1. **Online Drug Trafficking** – Selling banned substances on dark web markets.
2. **Fake News Distribution** – Spreading harmful misinformation to create panic.
3. **Illegal Online Gambling** – Running unauthorized betting websites.
   Example: Illegal IPL betting platforms.

3. How Cybercrimes differ from most terrestrial crimes? #

Aspect	Cybercrime	Terrestrial Crime
Location	Can be committed from anywhere in the world.	Usually requires physical presence at the crime scene.
Speed & Scale	Happens instantly and can impact millions at once.	Limited by time, location, and physical reach.
Anonymity	Criminals hide behind fake IDs, VPNs, and encryption.	Harder to hide identity in physical crimes.
Evidence	Digital, intangible, and easy to delete or alter.	Physical evidence is harder to destroy completely.
Jurisdiction	Complex due to cross-border nature of attacks.	Mostly handled within one country's legal system.
Cost to Commit	Low cost but high impact (just a laptop and internet needed)	Requires resources, tools and physical effort.
Detection	Attacks may go unnoticed for long periods.	Usually detected quickly due to visible impact.
Example	Phishing attack stealing 1,000 credit cards in minutes.	Robbing a bank branch with limited cash and higher risk.

2. Cyber offenses and Cybercrime

4. What are the steps involved in planning of cyberattacks by a criminal.

Cybercriminals follow a structured process while planning and executing cyberattacks. The planning phase is typically divided into three major stages, and each stage may include multiple sub-steps depending on the attacker's goal.

1. Reconnaissance (Information Gathering)

The attacker collects maximum information about the target before attacking.

- **Passive Reconnaissance:** Gathering public information (websites, job postings, social media, WHOIS).
- **Active Reconnaissance:** Scanning the target using tools like Nmap, Shodan, Wireshark.
- **Goal:** Identify IP ranges, open ports, technologies used and basic weaknesses.

2. Scanning & Identifying Vulnerabilities

Here the attacker performs a deeper technical analysis to map the system's weaknesses.

- **Port Scanning:** Identify open ports and active services.
- **Vulnerability Scanning:** Check for outdated software, weak passwords, misconfigurations.
- **Enumeration:** Gather system details like user accounts and network shares.
- **Weaponization:** Attacker prepares a malicious payload based on the target's weaknesses.
- **Delivery Preparation:** Decide how to deliver the payload (phishing emails, malicious links).
- **Goal:** Find the exact entry point and suitable exploit for the attack.

3. Launching the Attack / Gaining Access

The attacker executes the final stage to break into the system and achieve the desired objective.

- **Exploitation:** Use the chosen vulnerability (SQL injection, malware, credential attack).
- **Installation:** Install backdoors, keyloggers, Trojans for persistent access.
- **Command & Control (C2):** Establish communication channels with the infected system using encrypted or hidden connections.
- **Actions on Objectives:**
    - Data theft or exfiltration
    - Encrypting files for ransom (ransomware)
    - Sabotage or destruction of data
    - Creating admin accounts for long-term control
- **Covering Tracks:** Delete logs, hide tools, or use VPNs/proxies to avoid detection.

5. Explain the basic security precautions to be taken to safeguard Laptops and Wireless devices.

A) Security Precautions for Laptops

1) **Use Strong Passwords / PINs**
   Use complex passwords and avoid easy combinations.
2) **Install Antivirus & Antimalware**
   Keeps the system protected from viruses, trojans, ransomware, and spyware.
3) **Keep OS and Software Updated**
   Regular updates fix security vulnerabilities and reduce exploit risks.
4) **Use a Firewall**
   Blocks unauthorized access attempts and protects network traffic.
5) **Avoid Public / Unsecured Wi-Fi**
   Prevents Man-in-the-Middle (MITM) attacks and data interception.
6) **Take Regular Backups**
   Ensures data recovery in case of device theft, malware infection, or hardware failure.
7) **Be Careful While Clicking Links / Attachments**
   Prevents phishing-based infections and malware attacks.
8) **Do Not Store Sensitive Data Unprotected**
   Avoid keeping confidential files without encryption or password protection.

B) Security Precautions for Wireless Devices (Phones, Tablets, Wi-Fi Devices)

1) **Enable Device Lock**
   Use PIN, pattern, password, or biometric lock to prevent unauthorized use.
2) **Install Apps Only from Trusted Sources**
   Reduces malware risk from fake or malicious apps.
3) **Use Secure Wi-Fi Networks**
   Connect only to WPA3/WPA2 encrypted networks. Avoid open/free networks.
4) **Update Operating System and Apps Regularly**
   Fixes security loopholes and strengthens device protection.
5) **Enable Remote Tracking & Wipe**
   Helps locate a lost device and erase data remotely.
6) **Be Cautious of Public Charging Ports**
   Use your own charger or a USB data blocker for safety.
7) **Monitor App Permissions**
   Give apps only required permissions (camera, location, storage).

6. What are the illegal activities observed in Cyber Cafés? What are the safety and security measures while accessing the public computers in Cyber Café?

A) Illegal Activities Observed in Cyber Cafés

1) **Hacking and Unauthorized Access**
   Using café computers to hack websites, servers, or social media accounts.
2) **Phishing and Online Fraud**
   Sending fake emails, creating fake login pages, or stealing banking credentials.
3) **Identity Theft**
   Misusing saved passwords, autofill data, or personal details left by previous users.
4) **Online Scams & Fraudulent Transactions**
   Lottery scams, job scams, advance-fee frauds, or illegal money transfers.
5) **Cyberbullying and Harassment**
   Sending abusive emails, threatening messages, or posting defamatory content.
6) **Distribution of Malware**
   Uploading viruses, trojans, ransomware, or using infected USB drives.
7) **Accessing Illegal or Prohibited Websites**
   Dark web browsing, gambling sites, or illegal marketplaces.

B) Safety & Security Measures While Using Public Computers in Cyber Cafés

1) **Avoid Logging into Sensitive Accounts**
   Don’t access banking, UPI, payment apps, or personal email on public systems.
2) **Use Private/Incognito Mode**
   Prevents browser history, cookies, and temporary data from being stored.
3) **Always Clear Browsing Data Before Leaving**
   Delete cache, cookies, passwords, and form data to avoid identity theft.
4) **Do Not Save Passwords**
   Never click “Save Password” on shared computers.
5) **Enable Two-Factor Authentication (2FA)**
   Provides an additional layer of security if your password gets compromised.
6) **Check for HTTPS Before Logging In**
   Ensures encrypted connection and protects against MITM attacks.
7) **Avoid Downloading or Plugging In USB Drives**
   Prevents malware infections or accidental virus transfer.
8) **Log Out of All Accounts Completely**
   Ensure proper logout from email, social media, and cloud storage.

7. What are the different Security risks for Organizations? #

Organizations face several cybersecurity risks that affect their data, systems, and overall business operations. Major security risks include:

1. **Malware Attacks**
   Viruses, worms, ransomware, or spyware can infect systems and damage or steal data.
2. **Phishing & Social Engineering**
   Employees may be tricked into revealing passwords or clicking malicious links.
3. **Insider Threats**
   Employees or contractors misuse access by leaking data or causing accidental damage.
4. **Network Security Weaknesses**
   Weak firewalls, open ports, or insecure Wi-Fi allow unauthorized access.
5. **Data Breaches**
   Sensitive information is exposed due to weak passwords, poor encryption, or cloud misconfigurations.
6. **DDoS / DoS Attacks**
   Attackers overload servers, causing downtime and service disruption.
7. **Weak Authentication Practices**
   Using weak passwords, no multi-factor authentication, or shared logins increases risk.
8. **Mobile & BYOD Risks**
   Unsecured personal devices connected to the company network can introduce malware or lead to data leaks.

8. What are botnets? How is it exploited by an attacker to cause cyber-attack?

Botnets:

- A botnet is a group of computers, mobile devices, or IoT devices infected with malware and controlled remotely by a cybercriminal (botmaster).
- Each infected device becomes a "bot" or "zombie" and follows commands without the user's knowledge.
- Botnets are used to launch large-scale attacks because hundreds or thousands of devices work together under the attacker's control.

How an Attacker Exploits a Botnet:

1. **Infecting Devices**
   Attackers spread malware through emails, malicious downloads, or infected websites to convert devices into bots.
2. **Establishing Command & Control (C2)**
   All bots connect to a central server that allows the attacker to send instructions.
3. **Launching Large-Scale Attacks**
   Bots work together to send traffic, spam, or malicious requests.
4. **DDoS Attacks**
   Thousands of bots flood a server or website, causing it to slow down or crash.
5. **Sending Spam & Phishing Emails**
   Bots send bulk spam or phishing messages to steal information or spread malware.
6. **Credential Theft & Keylogging**
   Some botnets collect usernames, passwords, and banking details from infected devices.
7. **Click Fraud**
   Bots generate fake ad clicks to earn illegal revenue for the attacker.
8. **Cryptojacking**
   Infected devices are used to secretly mine cryptocurrency.

Example:

- **Scenario:** A botnet of 1,000 infected computers starts sending fake login requests to a company's website at the same time.
- **Result:** The server becomes overloaded and crashes, making the website unavailable to all real users.

9. Explain various types of credit card frauds.

A] Traditional Techniques

1) Assumed Identity Fraud

- Fraudster uses someone else's identity or a fake name to apply for a credit card.
- Uses temporary or false addresses so the card can be delivered without detection.

2) Financial Fraud

- Fraudster provides false income details or forged documents to get a higher credit limit.
- Banks verify income via salary slips, bank statements, and employer checks.

3) Intercept Fraud

- Card is applied for legitimately but stolen from postal mail before reaching the owner.
- Fraudster activates or uses the card before the real customer receives it.

4) Lost or Stolen Card Fraud

- Criminal uses a lost or stolen physical credit card until the cardholder blocks it.

B] Modern Techniques

1) Skimming

- A skimmer device copies data from the magnetic strip when the card is swiped (ATM/POS).
- Stolen data is later used for unauthorized transactions.

2) Card Cloning / Counterfeit Cards

- Data stolen by skimming is written onto a blank card to create a duplicate.
- Fraudster uses the cloned card to make unauthorized transactions.

3) Site Cloning / Fake Merchant Sites

- Fake websites mimic real shopping sites to trick users.
- Victims enter credit card details, which go directly to the fraudster.

4) Triangulation Fraud

- A fake seller offers cheap products and collects the victim's credit card details.
- The fraudster uses a stolen card to buy the real product and ships it to the victim.
- The fraudster keeps the victim's card details for future misuse.

5) Credit Card Generators

- Fraudsters use software that creates valid-looking credit card numbers.
- These numbers are used on weakly secured websites to make small unauthorized transactions.

10. What are the vulnerabilities and security challenges faced by mobile devices? #

1. **Malware & Malicious Apps**
   Harmful apps can steal data, track activity, or install spyware/trojans.
2. **Unsecure Public Wi-Fi**
   Attackers can intercept data using MITM attacks on open networks.
3. **Phishing / Smishing / Vishing**
   Fake emails, SMS, or calls trick users into revealing passwords or OTPs.
4. **Outdated OS or Apps**
   Failing to update leaves known security vulnerabilities unpatched.
5. **Weak Device Lock or No Encryption**
   No PIN/password/biometrics makes it easy for attackers to access data if the device is lost.
6. **Permission Misuse by Apps**
   Apps requesting unnecessary access (camera, mic, location) can leak personal information.
7. **Loss or Theft of Device**
   Physical loss exposes photos, emails, accounts, and banking apps.

11. Write a short note on: Cyberstalking and harassment. #

Cyberstalking and online harassment refer to using the internet, social media, emails, messages, or digital tools to threaten, monitor, intimidate, or repeatedly disturb someone. It is a serious cybercrime that affects a person's safety, privacy, and mental well-being.

1. Cyberstalking

Cyberstalking means continuously tracking or following someone online without their consent.

- Stalker watches the victim's posts, location, or activities.
- Sends repeated messages, tries to hack accounts, or misuses personal details.

2. Online Harassment

Online harassment includes abusive messages, trolling, threats, insults, and spreading false or embarrassing content about someone.

- Happens through comments, chats, emails, or public posts.
- Done to disturb, humiliate, or mentally pressure the victim.

Legal Provisions in India: Cyberstalking and harassment are punishable under: Section 354D (stalking), Section 507 (anonymous threats).

Example: Repeated threatening messages on Instagram or WhatsApp and monitoring a person's online activity is cyberstalking.

12. Write a short note on: Mobile/Cell phone attacks. #

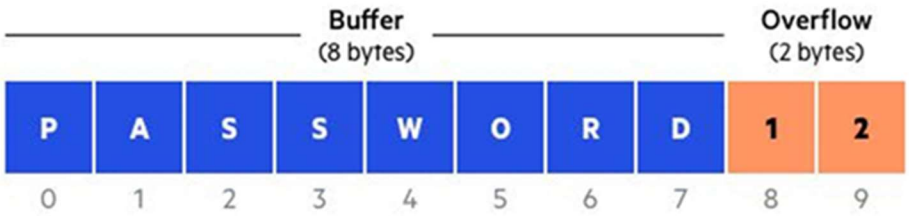
Mobile or cell phone attacks target smartphones by exploiting weak apps, insecure networks, and user behaviour. Common mobile attacks include:

1. **Malicious Apps**
    - Fake or infected apps steal data, track activity, or install spyware/trojans.
    - Often distributed through unofficial app stores or phishing links.
2. **SMS/Call-Based Attacks (Smishing & Vishing)**
    - Attackers send fake SMS messages or phone calls asking for passwords, OTPs, or banking details.
    - Users are tricked into giving sensitive information.
3. **Bluetooth & NFC Exploits**
    - Attackers exploit open Bluetooth/NFC to send malicious files or connect without permission.
    - Can lead to unauthorized data transfer or malware installation.
4. **Public Wi-Fi Attacks**
    - On open Wi-Fi, attackers perform Man-in-the-Middle (MITM) attacks to intercept browsing data, passwords, and logins.
5. **Mobile Malware (Spyware, Ransomware, Keyloggers)**
    - Malware secretly records keystrokes, steals photos, listens through the microphone, or encrypts files for ransom.
6. **Physical Access Attacks**
    - If the device is stolen and there is no PIN/biometric lock, the attacker can access stored data, apps, and accounts.

3. Tools and Methods used in Cyberline

13. Explain the different types of buffer overflow attacks and describe the techniques used to mitigate them.

A buffer overflow occurs when a program writes more data into a memory buffer than it can handle, causing the extra data to overwrite adjacent memory locations.
This allows attackers to crash the program, corrupt data, or inject malicious code to gain control of the system.



Types of Buffer Overflow Attacks

1) Stack Overflow Attack

- Occurs when excessive data is written to a stack buffer.
- Attackers overwrite the return address to redirect execution to malicious code.

2) Heap Overflow Attack

- Happens in the heap memory (used for dynamic allocation).
- Attackers modify function pointers or metadata to control program behaviour.

3) Format String Attack

- Occurs when user input is incorrectly used as a format string (e.g., printf(user_input)).
- Attackers use %x, %n to read/write memory and crash or control the program.

4) Integer Overflow Attack

- When the result of an arithmetic operation exceeds the maximum value an integer can hold.
- Can cause buffer allocation errors leading to memory corruption.

Mitigation Techniques for Buffer Overflow:

1. **Bounds Checking / Input Validation:** Validate input length before copying data into buffers to prevent writing beyond the buffer size.
2. **Use of Safe Functions:** Replace unsafe C functions (gets, strcpy, sprintf) with safer alternatives (fgets, strncpy, snprintf) to reduce overflow risk.
3. **Stack Canaries:** Use a special value placed before the return address; if it gets overwritten, the program detects tampering and stops execution.
4. **ASLR (Address Space Layout Randomization):** Randomizes memory address locations so attackers cannot predict where malicious code will run.
5. **DEP / NX-bit (Data Execution Prevention):** Marks memory regions as non-executable, preventing injected code in buffers from running.

14. Explain the SQL Injection attack with its steps. Mention countermeasures to prevent it.

SQL Injection is a web application attack where an attacker inserts malicious SQL code into input fields to access, modify, or delete database data. It occurs when user input is directly included in SQL queries without proper validation.

Steps of an SQL Injection Attack

1. **Finding Input Points**
    - Attacker identifies vulnerable inputs such as login forms, search bars, or URL parameters where user input is directly used in SQL queries.
2. **Testing for Vulnerability**
    - Attacker enters special characters or test payloads (e.g.: ', '', --, ' OR '1'='1) to see if the application executes unexpected SQL commands or behaves abnormally.
3. **Injecting Malicious SQL Code**
    - Attacker sends crafted SQL commands to manipulate the query logic; for example, bypassing login authentication or retrieving hidden data.
4. **Extracting or Manipulating Data**
    - After gaining access, the attacker may:
        - View confidential data like usernames, passwords or credit card details
        - Modify or delete records.
        - Download the entire database.
5. **Taking Control of the System**
    - In advanced attacks, the attacker can:
        - Gain administrator-level privileges
        - Access the file system
        - Install backdoors for persistent access

Countermeasures to prevent SQL Injection:

1. **Use Prepared Statements / Parameterized Queries** – Ensures user input is treated as data, not executable SQL code, preventing injection.
2. **Input Validation** – Allow only expected formats (e.g., numbers for ID fields) and blocks dangerous characters like ', '', --, ;.
3. **Stored Procedures** – Use predefined database routines instead of dynamic SQL queries.
4. **Least Privilege Principle** – Use least-privilege access for application database accounts.
5. **Web Application Firewall (WAF)** – Filters malicious requests.
6. **Error Message Control** – Avoid showing detailed database error messages to users.

15. Explain DOS and DDOS attacks in detail.

A] DoS Attack

A Denial of Service (DoS) attack is an attempt to make a system, website, or network unavailable by overwhelming it with excessive traffic or malicious requests. It usually comes from one attacker or one system.

How a DoS Attack Works

1. The attacker sends a huge number of requests to the target server.
2. The server becomes overloaded and cannot respond to legitimate users.
3. The system slows down, crashes, or stops responding completely.

Types of DoS Attacks

1) Volume-Based Attacks

Definition: Flood the target with massive traffic to overload network bandwidth.
Example – ICMP Flood (Ping Flood):

- Sends a large number of ICMP Echo Requests.
- Consumes bandwidth and processing power, making the system unreachable.

2) Protocol Attacks

Definition: Exploit weaknesses in TCP/IP protocols to exhaust server resources like memory or CPU.
Example – SYN Flood:

- Sends many SYN requests without completing the TCP handshake.
- Keeps server resources tied up, blocking new legitimate connections.

B] DDoS Attack

A Distributed Denial of Service (DDoS) attack is similar to DoS but is launched from multiple compromised systems (botnet) at the same time, making it far more powerful and difficult to stop.

How a DDoS Attack Works

1. The attacker infects many computers/devices to create a botnet.
2. All infected systems send large volumes of traffic simultaneously.
3. The massive load overwhelms the target server and brings it down.

Types of DDoS Attacks

1) Volumetric DDoS Attacks

Definition: Use thousands of bots to generate huge traffic, overloading the target's bandwidth.
Example – DNS Amplification:

- Attackers misuse open DNS servers to multiply traffic.
- Sends extremely high-volume responses to the victim's server.

2) Application Layer DDoS Attacks

Definition: Target specific applications like websites, APIs, or login pages.
Example – HTTP GET/POST Flood:

- Botnet sends massive page load requests.
- Overloads web servers by mimicking real users.

16. What is a vishing attack? How does it work, and how can it be prevented?

Vishing (voice phishing) is a social engineering attack where cybercriminals use phone calls or voice messages to pretend they are from trusted sources such as banks, telecom companies, government departments, or customer support.
Their goal is to trick victims into revealing confidential information like OTP, PIN, CVV, account numbers, passwords, or personal details, or to make the victim perform harmful actions.

How Vishing Works

1. **Fake Caller Identity**
    - The attacker pretends to be a trusted authority (bank officer, RBI, courier service, telecom provider).
    - Caller ID spoofing is used to display an official-looking number.
2. **Creating Urgency or Fear**
    - The attacker pressures the victim with messages like "Your account will be blocked," "KYC expired".
    - This urgency forces the victim to respond quickly without verifying.
3. **Information Extraction**
    - The victim is asked to provide OTP, ATM PIN, card details, or login credentials.
    - Sometimes attackers ask victims to install remote-access apps to "fix" the issue.
4. **Executing Fraud**
    - Stolen information is used for unauthorized bank transactions, SIM swap, identity theft, or account takeover.
    - Attackers may transfer money instantly before the victim realizes.

How to Prevent Vishing:

1. **Never share sensitive details:** Banks never ask for OTP, PIN, or passwords over calls.
2. **Verify the caller:** Always disconnect and call back using the official customer care number.
3. **Do not trust caller ID:** Numbers can be spoofed, so always verify separately.
4. **Ignore urgency tactics:** Real organizations don't threaten immediate blocking; stay calm and confirm.
5. **Do not install unknown apps:** Never install remote-access apps suggested by callers.
6. **Use call filtering/spam detection:** Phone filters and Truecaller-type apps can flag scam calls.
7. **Report vishing attempts:** Inform your bank and report to the cybercrime helpline 1930.

17. Explain phishing attacks, their types, and prevention methods.

Phishing is a social engineering attack where attackers trick users into revealing sensitive information (passwords, OTPs, bank details) by pretending to be a trusted organization through emails, messages, or fake websites.

Types of Phishing Attacks

1. **Email Phishing**
    - Fake emails impersonating banks, services, or government agencies.
    - Contains malicious links or asks users to "verify" account details.
2. **Spear Phishing**
    - Targeted phishing aimed at a specific person or organization.
    - Uses personalized information to appear more convincing.
3. **Smishing (SMS Phishing)**
    - Fake SMS messages with malicious links or urgent alerts.
    - Example: "Your bank account will be blocked. Click here."
4. **Vishing (Voice Phishing)**
    - Fraudulent phone calls pretending to be bank/telecom officials.
    - Victims are tricked into sharing OTP, PIN, or card details.
5. **Pharming**
    - Redirects users from a legitimate website to a fake website without their knowledge.
    - Achieved through DNS poisoning or malware.

Prevention Methods:

1. **Verify the Sender:** Check email address, spelling errors, and suspicious URLs.
2. **Do Not Click Unknown Links:** Type the website URL manually instead of clicking.
3. **Enable Two-Factor Authentication (2FA):** Protects accounts even if passwords leak.
4. **Use Anti-Phishing Filters & Security Software:** Blocks unsafe sites and emails.
5. **Check for HTTPS:** Ensure the site is secure before entering sensitive information.
6. **Avoid Sharing Personal Details:** Banks never ask for PIN, CVV, or OTP via email/SMS/call.
7. **Report Suspicious Messages:** Inform your bank, email provider, or cybercrime helpline.

18. Write a short note on Trojan horse and backdoor. #

1. Trojan Horse

- A Trojan horse is a malicious program that appears to be a legitimate software but secretly performs harmful activities.
- Unlike viruses or worms, Trojans do not self-replicate; they rely on the user to install or run them.
- Once installed, a Trojan can steal data, install malware, record keystrokes, or give remote access to the attacker.
- **Example:** A fake "free game" or "software update" that silently installs a keylogger.

2. Backdoor

- A backdoor is a hidden entry point in a system that bypasses normal authentication.
- Attackers use backdoors to gain remote, unauthorized access even after the main vulnerability is patched.
- Backdoors are often installed by Trojans, malware, or sometimes left intentionally by software developers.
- **Example:** A remote access tool (RAT) that lets the attacker control the device anytime.

19. Explain different password cracking techniques. #

Attackers use various techniques to guess, steal, or break user passwords. Common password cracking techniques include:

1. **Brute Force Attack**
    - Tries every possible combination of characters until the correct password is found.
    - Very time-consuming but guaranteed to work if unlimited attempts are allowed.
2. **Dictionary Attack**
    - Uses a list of common words, names, or frequently used passwords.
    - Faster than brute force because it tests only likely passwords.
3. **Phishing Attack**
    - Tricks the user into entering their password on a fake website, email link, or message.
    - Most successful method because it targets humans, not systems.
4. **Keylogging**
    - Malware records every key pressed on the keyboard.
    - Captures passwords directly as the user types them.

5. **Shoulder Surfing**
    - Attacker observes the user typing their password physically or via CCTV.
    - Common in public places like ATMs or cyber cafés.
6. **Social Engineering**
    - Manipulates users to reveal passwords (e.g., pretending to be IT support).
    - Depends on human error rather than technical flaws.
7. **Password Guessing**
    - Attacker manually guesses passwords based on personal information.
    - Uses details like birthdates, pet names, hobbies, or phone numbers.

20. Differentiate between virus and worm. #

Parameter	**Virus**	**Worm**
Definition	Malicious program that attaches to a host file and spreads when the file runs.	Standalone malware that spreads on its own without any host file.
Objective	Damages or modifies files and data.	Consumes system/network resources and causes disruption.
Spread Method	Spreads only when the user opens an infected file or attachment.	Spreads automatically through networks or by exploiting vulnerabilities.
Dependency	Needs a host file or program to execute.	Independent – no host file needed.
Harmful Level	More harmful to stored data and software.	Less harmful to data but heavily disrupts systems.
Speed of Spread	Slower, depends on user action.	Very fast, spreads widely without user action.
Control	Cannot be remotely controlled.	Can be remotely controlled (often part of botnets).
Detection & Protection	Removed by antivirus tools.	Requires antivirus + strong network/firewall protection.
Example	Melissa Virus.	WannaCry Worm.

4. The concept of Cyberspace

21. What is digital evidence? Mention its types and common sources.

Digital evidence:

Digital evidence refers to any information stored, processed, or transmitted in digital form that can be used during investigation or in legal proceedings.
It includes data from computers, mobiles, networks, cloud services, and digital devices, and is essential because most cybercrimes leave electronic footprints.

Legal Recognition in India:

- Digital evidence is recognized under the Indian Evidence Act, 1872 (amended by IT Act 2000).
- Sections 65A & 65B govern admissibility of electronic records.
- 65B certificate confirms authenticity of secondary evidence.

Types of Digital Evidence:

A) Primary Digital Evidence

Primary evidence refers to the original electronic device or original data where the information is first stored.
Examples:

- Original hard disk, mobile phone, laptop.
- Original server logs or CCTV DVR.
- Original email stored in the actual device.

Importance:

- Considered the best evidence because it is directly taken from the original source.
- Requires strict handling, chain-of-custody, and forensic imaging to avoid tampering.

B) Secondary Digital Evidence

Secondary evidence refers to copies or outputs of the original digital data.
Examples:

- Printouts of emails.
- Screenshots of chats or CCTV footage.
- PDF copies, backups, cloud-retrieved logs.

Key Point:

- Valid in court only when accompanied by a Section 65B certificate (proving authenticity).
- Used when original evidence cannot be produced.

Common Sources of Digital Evidence:

1. **Computers and Laptops** – Contain system logs, browsing activity, documents, emails, and deleted data.
2. **Mobile Phones and Tablets** – Store calls, messages, app chats, photos, and location information.
3. **Network Devices** –Routers, firewalls, and servers provide IP logs and packet data.
4. **Social Media Accounts** – Posts, messages, comments, and account activity useful for investigations.
5. **CCTV & Surveillance Systems** – Offer video footage and recorded movement patterns.
6. **External Storage Media** – USB drives, SD cards, and hard disks store backed-up files.
7. **Websites & Online Portals** – Record login activity, transaction logs, and digital receipts.

22. Explain e-contracts and its different types.

E-Contract:
An e-contract is a legally valid agreement created and accepted electronically without physical signatures. In India, it is governed by the Indian Contract Act, 1872 and the Information Technology Act, 2000.

E-contracts cover agreements made through emails, websites, online platforms, e-commerce sites, and online banking.

They are legally valid if it satisfies the essential elements of a contract: offer, acceptance, lawful consideration, capacity of parties, and intention to create legal relations.

Examples:

- Clicking "I Agree" on terms and conditions.
- Buying products online (e.g., Amazon).
- Online banking agreements.
- Submitting online forms or applications.

Types of E-Contracts:

1. Click-Wrap Agreement

Users actively agree by clicking "I Agree" before accessing a service.
Common in software installation, app downloads, and online subscriptions.

2. Browse-Wrap Agreement

The terms are posted on a website (often in the footer), and using the site implies acceptance.
Seen on news websites, informational websites and online stores.

3. Shrink-Wrap Agreement

Terms and conditions are included inside packaged goods like software CDs or manuals.
Opening the package or installing the product means acceptance.

4. E-Mail Contract

Offer and acceptance happen through email exchange.
Common in business negotiations, purchase orders, and service agreements.

5. Digital Signature Contract

Contracts signed using digital signatures issued by a Certifying Authority under the IT Act.
Used in banking and income tax filings.

23. What is e-commerce? Discuss types of e-commerce.

E-Commerce:
E-Commerce (Electronic Commerce) refers to the buying and selling of goods and services over the internet. Unlike traditional commerce, all transactions are conducted electronically, without physical interaction.

Key Features of E-Commerce:

- **Online Transactions:** All buying and selling happen over the internet, making it fast and convenient.
- **Electronic Payments:** Payments are made digitally using credit/debit cards, UPI and other online methods.
- **Global Reach:** Businesses can reach customers worldwide, breaking geographical barriers.
- **24/7 Availability:** Online stores are open all the time, allowing customers to shop anytime.
- **Paperless Process:** Orders, invoices, and receipts are all digital, reducing paperwork.

Types of E-Commerce:

1. **B2B (Business to Business):** Transactions between businesses, e.g., wholesalers selling to retailers.
2. **B2C (Business to Consumer):** Businesses sell directly to customers, e.g., Amazon, Flipkart.
3. **C2C (Consumer to Consumer):** Consumers sell to other consumers via online platforms, e.g., OLX, eBay.
4. **C2B (Consumer to Business):** Individuals offer products or services to businesses, e.g., freelance work.
5. **B2G (Business to Government):** Businesses provide goods or services to government agencies, e.g., online tenders.
6. **G2C (Government to Citizen):** Government services provided to citizens through online platforms, for example online tax filing and Aadhaar services.

24. Explain why do we need cyber laws? Discuss about the challenges to Indian cyber laws.

A] Need for Cyber Laws

With the rapid growth of the internet, online transactions, and digital services, we need cyber laws to ensure safety, trust, and legal protection in the digital world. Cyber laws help regulate online activities, prevent misuse, and protect users from cybercrimes.

1. **Rising Cybercrimes**
   Cyber laws are needed to address hacking, phishing, identity theft, cyberstalking, and online fraud, and to punish offenders.
2. **Legal Recognition for Online Transactions**
   They make e-commerce, digital signatures, online contracts, UPI payments, and e-governance services legally valid and enforceable.
3. **Protection of Digital Data & Privacy**
   Cyber laws safeguard personal data, financial records, and confidential information from unauthorized access or misuse.
4. **Regulation of Online Content & Communication**
   Helps control misuse of social media, copyright violations, fake news, and illegal online activities.

B] Challenges to Indian Cyber Laws

1. **Fast-Changing Technology**
   New threats such as ransomware, crypto scams, AI-based attacks, and deepfakes evolve faster than the law can keep up.
2. **Cross-Border Jurisdiction Issues**
   Cybercrimes often involve servers and criminals located in other countries, making investigation and enforcement difficult.
3. **Lack of Cyber Awareness**
   Many users fall victim to fraud due to limited awareness on online safety.
4. **Limited Technical Expertise**
   Law enforcement often lacks advanced digital forensics tools and skilled personnel to investigate complex cybercrimes.
5. **Gaps in the IT Act 2000**
   Certain issues like data protection, social media regulation, cyberbullying, and modern financial frauds are not clearly covered.

25. Write a note on Intellectual Property Aspects in cyber law.

Intellectual Property Rights (IPR) are legal rights given to creators and owners of intellectual works such as inventions, software, artistic content, designs, symbols, and brand elements. The goal of IPR is to promote innovation and creativity by giving exclusive rights to use, produce, or sell the creation for a certain period.

Forms of Intellectual Property in Cyberspace

- Software programs and source code
- Websites and domain names
- Logos, brand names, and digital trademarks
- Digital art, music, videos, e-books

Key IPR Types and Issues in Cyber Law

1. Copyright

- Protects original creative works such as software, music, videos, and digital content.
- **Issues:** Online piracy, illegal downloads, unauthorized copying or sharing, plagiarism.

2. Trademark

- Protects brand names, logos, slogans, and domain names used on the internet.
- **Issues:** Misuse of brand identity, fake websites.

3. Patent

- Protects new inventions, software algorithms, and technical processes.
- **Issues:** Reverse engineering, unauthorized replication of patented technologies.

4. Trade Secrets

- Protects confidential business information like algorithms, source code, client data.
- **Issues:** Hacking, insider leaks, theft of source code or proprietary data.

5. Domain Names (as IP Assets)

- Domain names are treated similar to trademarks in cyber law.
- **Issues:** Domain disputes and cybersquatting; resolved under UDRP.

Relevant Legal Provisions

- **Indian Copyright Act, 1957** (amended for digital works)
- **Trade Marks Act, 1999**
- **Patent Act, 1970**
- **IT Act, 2000** (for electronic records, cybercrimes, and digital rights)

26. Explain electronic banking in India and what are laws related to electronic banking in India.

Electronic Banking:
Electronic Banking (E-Banking) refers to delivering banking services and products through electronic channels such as ATMs, internet banking, mobile apps, and electronic fund transfers. It enables customers to conduct transactions like balance inquiry, bill payments, and fund transfers conveniently without visiting a branch.

Features of E-Banking in India:

- Online & Mobile Banking for real-time access to accounts.
- Fund transfer systems like NEFT, RTGS, IMPS, UPI.
- ATMs and Debit/Credit cards for self-service banking.
- Digital wallets and e-payment gateways for e-commerce.

Key Legal Provisions in India

1. **Information Technology Act, 2000**
    - Section 4 – Legal recognition of electronic records.
    - Section 5 – Legal recognition of digital signatures for authentication.
    - Section 66C & 66D – Punishment for identity theft and cheating via electronic means.
2. **Reserve Bank of India (RBI) Guidelines**
    - Payment and Settlement Systems Act, 2007 – Governs electronic payment systems.
    - RBI Circular on Internet Banking Security – Two-factor authentication, encryption, customer liability norms.
    - KYC Norms – Mandatory for electronic transactions.
3. **Indian Contract Act, 1872**
    - Governs electronic contracts between bank and customer (terms & conditions of internet banking).
4. **Negotiable Instruments Act, 1881 (Amendment)**
    - Recognizes cheques in electronic form and digitally scanned copies of cheques.

5. Indian IT act

27. Explain the objectives and features of IT Act 2000.

A] Objectives of the IT Act 2000

1. **To provide legal recognition to electronic records and digital signatures** so online documents are treated the same as paper documents.
2. **To promote e-governance** by allowing people to file forms, applications, and documents electronically with government departments.
3. **To support and encourage e-commerce** by giving legal backing to online contracts, transactions, and business communication.
4. **To prevent and control cybercrimes** such as hacking, data theft, identity theft, and cyberstalking by defining offenses and penalties.
5. **To ensure secure digital communication** by using digital signatures and encryption to maintain authenticity and integrity of online messages.
6. **To establish a regulatory framework** by creating authorities like the Controller of Certifying Authorities (CCA) to issue digital certificates and manage cyber investigations.

B] Features of the IT Act 2000

1. **Legal Status to Digital Signatures**
   Digital signatures are treated as equivalent to handwritten signatures.
2. **Recognition of Electronic Records**
   Electronic documents are legally acceptable in courts and official processes.
3. **Defines Cybercrimes & Penalties**
   Covers offenses such as hacking, tampering with computer source code, publishing obscene content, and unauthorized access.
4. **Establishment of Certifying Authorities (CA)**
   Introduces licensed CAs to issue digital signature certificates.
5. **Provision for Cyber Appellate Tribunal**
   Provides a mechanism for appeal and resolution of cyber-related disputes.
6. **Applicable to All Electronic Transactions in India**
   Covers e-commerce, e-governance, banking, and corporate electronic communication across the country.

6. Information Security Standard Compliances

28. Write a short note on HIPAA. #

HIPAA (Health Insurance Portability and Accountability Act), 1996 is a U.S. law that protects the privacy, security, and confidentiality of patient health information (PHI). It applies to hospitals, clinics, insurance companies, and any organization that stores or handles electronic medical data.

Important Aspects of HIPAA

1. **Protection of Patient Data**
   HIPAA safeguards medical records and personal health information (PHI) from misuse or unauthorized access.
2. **Privacy Rule**
   Defines how PHI can be collected, used, or shared.
   Gives patients' rights to view and request corrections to their records.
3. **Security Rule**
   Requires hospitals and healthcare providers to implement technical, physical, and administrative safeguards like encryption, passwords, and secure storage.
4. **Standardization of Electronic Health Data**
   Ensures uniform rules for handling electronic health records (EHR), billing, and health transactions.
5. **Penalties for Violations**
   Heavy fines and legal action are imposed if patient data is leaked, shared without consent, or mishandled.

Example

If a hospital employee shares a patient's medical report on social media, it is a HIPAA violation.

29. Write a short note on SOX. #

The Sarbanes–Oxley Act (SOX), 2002 is a U.S. law created to prevent corporate fraud and ensure that companies maintain accurate and secure financial records. It was introduced after major scandals like Enron and WorldCom to restore trust in financial reporting.

Important Aspects of SOX

1. **Protects Financial Data**
   Companies must keep financial information accurate, secure, and tamper-proof.
2. **Strong Internal Controls**
   Businesses must implement policies and checks to prevent fraud and ensure reliable financial reporting.
3. **Record Keeping & Audit Logs**
   Financial documents and electronic records must be safely stored and available for audits.
4. **Management Responsibility**
   CEOs and CFOs must personally certify the truthfulness of financial statements.
5. **Strict Penalties**
   Fines and jail time for falsifying records, destroying data, or failing to follow SOX rules.

Relevance to Cybersecurity:
SOX requires companies to keep financial systems secure by maintaining logs, preventing data breaches, and using basic controls like access management and monitoring.

Asked once:

# indicates 5-mark question

1. Introduction to Cybercrime

1. Differentiate between Cybercrime and Cyber fraud. #

Aspect	Cybercrime	Cyber Fraud
Definition	Any illegal activity using computers or the internet.	A cybercrime done to cheat people for money.
Objective	To damage systems, steal data, or disrupt services.	To steal money or financial information.
Scope	Very broad (hacking, malware, DDoS, bullying, etc.).	Limited to online scams and financial deception.
Impact	Can affect individuals, companies, and governments.	Mainly causes financial loss to individuals or businesses.
Methods	Hacking, malware, DDoS, data breaches.	Phishing, fake websites, identity theft, online scams.
Motivation	Can be political, personal, or disruptive.	Always money-motivated.
Legal Area	Covered under general IT and cybercrime laws.	Covered under financial fraud and cyber fraud laws.
Example	Hacking a server and deleting files.	Phishing email stealing credit card details.

2. Cyber offenses and Cybercrime

2. Explain about the impact of Cybercrimes in Social Engineering.

Social engineering is a cyber technique where attackers manipulate people into giving confidential information or performing harmful actions. Cybercrimes heavily strengthen and expand social engineering attacks. Their major impacts are:

1. **Higher Success of Scams**
   Cybercriminals use leaked personal data to make phishing, smishing, and vishing attacks more convincing and targeted.
2. **Identity Theft & Impersonation**
   Stolen information allows attackers to pose as banks, companies, or even friends to trick victims into sharing sensitive details.
3. **Financial Losses**
   Victims can lose money through fraudulent transactions, fake offers, online scams, and unauthorized withdrawals.
4. **Unauthorized Access to Systems**
   Employees are manipulated into revealing passwords or clicking malicious links, allowing attackers to enter company networks.
5. **Spread of Malware & Ransomware**
   Social engineering tricks users into opening infected attachments or fake updates, leading to system compromise.
6. **Data Theft & Information Leakage**
   Once criminals gain access, they steal customer data, financial details, or internal documents for further exploitation.
7. **Reputation & Trust Damage**
   Organizations lose customer trust when scams or social engineering attacks misuse their name, causing long-term reputation harm.

3. Outline the challenges for securing data in business perspective.

1. **Growing Cyber Threats**
   Businesses face malware, phishing, ransomware, and data theft attempts that are increasing every year.
2. **Insider Threats**
   Employees may leak data intentionally or accidentally due to negligence or poor security practices.
3. **Data Stored in Multiple Locations**
   Companies store data on servers, cloud platforms, laptops, mobiles, and USB drives, making protection harder.
4. **Lack of Strong Access Control**
   Weak passwords, shared accounts, and improper permission settings increase risk of unauthorized access.
5. **Third-Party and Vendor Risks**
   Outsourced services and external partners may not follow strict security standards, exposing business data.
6. **Cost and Resource Limitations**
   Small and medium businesses often lack budget, skilled staff, or tools needed for strong data security.

4. List general guidelines for password policies.

1. **Use Strong Passwords:**
   Include a mix of uppercase/lowercase letters, numbers, and special characters.
2. **Minimum Length Requirement:**
   Passwords should be at least 8–12 characters long.
3. **Avoid Common or Personal Information:**
   Do not use names, birthdays, phone numbers, or easily guessable words.
4. **Regular Password Changes:**
   Users should update passwords periodically and avoid reusing old ones.
5. **Enable Multi-Factor Authentication (MFA):**
   Adds an extra layer of security even if the password is compromised.
6. **Do Not Share or Write Down Passwords:**
   Avoid sharing passwords and do not store them in easily accessible places.

5. Explain various threats associated with cloud computing.

1. **Data Breaches**
   Sensitive data stored in the cloud can be accessed by attackers if accounts, databases, or storage buckets are misconfigured or compromised.
2. **Account Hijacking**
   Weak passwords or phishing can allow attackers to take control of cloud accounts and access or modify data.
3. **Insecure APIs**
   Cloud services rely on APIs; poorly secured APIs can expose data, allow unauthorized access, or enable attacks.
4. **Data Loss**
   Accidental deletion, ransomware attacks, or provider failures can lead to permanent loss of business data.
5. **Insider Threats**
   Employees or cloud provider staff with excessive access may misuse data intentionally or accidentally.
6. **Denial of Service (DoS) Attacks**
   Attackers overload cloud services with excessive traffic, making applications slow or unavailable.

6. Explain different attack vectors in cyber security.

1. **Phishing Attacks**
   Attackers use fake emails, messages, or websites to trick users into sharing passwords, banking details, or clicking malicious links.
2. **Malware Infections**
   Viruses, worms, trojans, spyware, and ransomware enter through downloads, attachments, or infected devices.
3. **Social Engineering**
   Attackers manipulate people through calls, texts, or impersonation to reveal sensitive information or perform harmful actions.
4. **Unpatched Software Vulnerabilities**
   Hackers exploit bugs or outdated software to gain unauthorized access to systems.
5. **Brute Force Attacks**
   Attackers try large numbers of password combinations to break into accounts.
6. **Network-Based Attacks**
   Includes MITM (Man-in-the-Middle), packet sniffing, and DDoS attacks that target network traffic or availability.

3. Tools and Methods used in Cyberline

7. Write a short note on Salami attack.

A Salami attack is a type of cyber fraud where the attacker commits many very small, almost unnoticeable actions that individually cause tiny losses but collectively result in large financial gain. The idea is that each "slice" (action) is too small to be detected.

Key Points:

1. **Small, Incremental Theft**
   The attacker steals extremely small amounts (like a few paise or cents) from many accounts.
2. **Difficult to Detect**
   Individual losses are so tiny that victims do not notice or report the fraud.
3. **Targets Financial Systems**
   Common in banking, payroll systems, billing systems, or interest calculations.
4. **Automated Execution**
   Attackers often use scripts or programs to repeatedly transfer these small amounts automatically.

Example: An employee programs the banking system to deduct ₹0.10 from every customer transaction and transfer it to their own account. No single customer notices the loss, but the attacker collects a large sum.

8. Explain Identity theft in detail.

Identity theft is a cybercrime in which an attacker steals someone's personal information such as name, address, phone number, Aadhaar, PAN, bank details, passwords, or card information and uses it without permission for fraudulent activities.

Key Points:

1. **Stealing Personal Information**
   Attackers obtain data through phishing, data breaches, social engineering, or stolen documents/devices.
2. **Financial Fraud**
   Stolen identity is used to make unauthorized transactions, open fake bank accounts, apply for loans, or misuse credit cards.
3. **Account Takeover**
   Criminals reset passwords, control email or social media accounts, and impersonate the victim.

4. **Misuse of Digital Identity**
   Attackers use the victim's identity for SIM swapping, fake KYC, tax fraud, or illegal online activities.

5. **Impact on Victim**
   Leads to money loss, reputation damage, legal issues, and difficulty proving that the fraud was not committed by them.

Example: A fraudster uses a victim's stolen Aadhaar and PAN details to apply for an online loan in the victim's name.

9. Write a short note on Steganography.

Steganography is the technique of hiding secret information inside another normal-looking file such as an image, audio, video, or text so that no one notices a hidden message exists. In cybercrime, steganography is used to secretly transmit malicious data without raising suspicion.

Key Points:

1. **Hiding Malicious Content**
   Attackers hide malware, commands, or stolen data inside harmless-looking files (images, videos) to bypass detection.

2. **Stealthy Communication**
   Cybercriminals use steganography to secretly communicate with other attackers or infected systems.

3. **Bypassing Security Tools**
   Hidden data inside images or audio files is difficult for antivirus or firewalls to detect.

4. **Data Exfiltration**
   Stolen information (passwords, documents) is embedded inside media files and sent out so organizations don't notice the breach.

5. **Used in Malware Campaigns**
   Modern malware downloads payloads hidden in JPEG/PNG files using LSB (Least Significant Bit) techniques.

Example: An attacker hides ransomware code inside a normal JPEG image; when the victim opens the file, the malware extracts and executes the hidden payload.

4. The concept of Cyberspace

10. What is WIPO? List treaties prepared by WIPO.

WIPO (World Intellectual Property Organization) is a specialized agency of the United Nations responsible for promoting and protecting intellectual property (IP) globally.
It helps countries develop IP laws, resolves international IP disputes, and manages global IP registration systems like patents, trademarks, and copyrights.

Treaties Prepared by WIPO

1. **Berne Convention** – Protects literary and artistic works (copyright).
2. **Paris Convention** – Protects industrial property (patents, trademarks).
3. **Patent Cooperation Treaty (PCT)** – Single international patent filing system.
4. **Madrid Agreement / Madrid Protocol** – International system for registering trademarks.
5. **WIPO Copyright Treaty (WCT)** – Copyright protection for digital works.
6. **WIPO Performances and Phonograms Treaty (WPPT)** – Protects performers and producers of sound recordings.
7. **Budapest Treaty** – International deposit of microorganisms for patent procedures.
8. **Hague Agreement** – International registration of industrial designs.

11. Write a short note on Cyberdefamation.

Cyberdefamation refers to damaging a person's reputation by posting false, harmful, or misleading information about them on the internet. It is defamation committed through digital platforms such as social media, emails, websites, blogs, forums, or messaging apps.

Key Points

1. **Online False Statements**
   Spreading untrue or defamatory content (posts, comments, videos, screenshots) that harms someone's image.
2. **Anonymity of Attackers**
   Offenders often hide behind fake accounts, making it difficult to trace them.
3. **Legal Provisions**
   In India, cyberdefamation is punishable under Section 66A/67 of the IT Act for online abuse and defamatory content.

Example: Posting a false rumour on Instagram claiming a person committed fraud, causing damage to their reputation.

6. Information Security Standard Compliances

12. Explain what the Information Security Standard is.

Information Security Standards are formal guidelines and rules created to protect an organization's data, systems, and processes.
They define best practices for maintaining confidentiality, integrity, and availability of information.

Important Aspects

1. **Provide Security Framework**
   Give structured procedures for managing and protecting data.
2. **Reduce Risks**
   Help organizations identify, control, and minimize security threats.
3. **Ensure Compliance**
   Organizations must follow these standards to meet legal and industry requirements.
4. **Improve Trust**
   Following standards increases customers' and partners' confidence in data handling.
5. **Examples:**
   HIPAA, SOX, GLBA, FISMA.