1. **What is SQL injection and why is it dangerous?**

SQL injection is a web security vulnerability that allows attackers to interfere with the queries an application makes to its database. It occurs when untrusted input is inserted into a SQL query without proper sanitization or validation. This lets attackers alter the query logic, access restricted data, or execute unauthorized commands.

When exploited, SQL injection can expose sensitive information such as usernames, passwords, financial data, or personal records. Attackers may also modify, delete, or corrupt stored data, severely impacting business operations. In severe cases, it can lead to full system compromise if the attacker gains control of the underlying server.

Key Risks:

- Unauthorized access to confidential data
- Bypassing authentication mechanisms
- Data alteration or deletion
- Database shutdown or damage
- Reputational and financial losses

Prevention Measures:

- Use parameterized queries or prepared statements instead of dynamic SQL.
- Sanitize and validate all user inputs.
- Restrict database privileges to the minimum necessary.
- Conduct regular vulnerability testing and code reviews.

SQL injection remains one of the most common and dangerous cybersecurity threats. Its persistence highlights the ongoing need for secure coding practices and strict database access controls to maintain data confidentiality and system integrity.

2. **Explain the role of Cybercafes in Cybercrimes with examples.**

Cybercafes play a significant role in cybercrimes due to their public accessibility, shared systems, and weak identity verification. They provide anonymity and convenience for criminals to execute illegal online activities without direct traceability. Attackers exploit the lack of monitoring, outdated security configurations, and high user turnover to conduct offenses ranging from data theft to financial fraud.

Key Roles in Cybercrime:

1. Anonymity and Untraceability: Cybercafes allow users to operate under false identities, making it difficult for law enforcement to link crimes to individuals.
2. Use in Financial Fraud: Criminals often perform phishing, online banking fraud, or credit card scams using public systems to avoid detection.
3. Launching Attacks: Hackers may use cybercafes to send malicious emails, deploy ransomware, or carry out distributed denial-of-service (DDoS) attacks.
4. Data Theft: Users may install keyloggers or spyware on public machines to capture login credentials of subsequent users.
5. Illegal Communications: Terrorist or criminal organizations sometimes use cybercafes to communicate or coordinate illicit activities securely.

Examples:

- In several phishing and cyber fraud cases in India and Southeast Asia, attackers used cybercafes to send fake banking emails and withdraw stolen funds.
- Cybercafes have been used to access compromised accounts or purchase illegal items on the dark web.

- Law enforcement investigations have traced the origins of cyberstalking and online harassment cases to public café terminals.

Preventive Measures:

- Cybercafes should maintain user identity logs and CCTV surveillance.
- Systems must have updated antivirus software, restricted downloads, and disabled administrative privileges.
- Periodic system audits and browser data clearing after every session reduce exposure.

Cybercafes remain high-risk environments for cybercrime due to their transient, anonymous nature. Strengthening user verification and enforcing cybersecurity protocols are critical to minimizing their misuse in digital offenses.

3. What are the challenges to Indian cyberlaws?

Indian cyberlaws face multiple structural, technical, and enforcement-related challenges that limit their effectiveness in combating evolving cyber threats. The Information Technology (IT) Act, 2000—India's primary cyber legislation—was initially designed to address e-commerce authentication and digital signatures, not the complex modern threat landscape.

Major Challenges:

1. Outdated Legal Framework: The IT Act has not kept pace with emerging cybercrimes such as ransomware, cryptocurrency fraud, and AI-based phishing. Its amendments remain reactive rather than preventive.
2. Jurisdictional Limitations: Cybercrimes often transcend national boundaries, yet Indian law enforcement faces obstacles in cooperation, evidence collection, and extradition due to varying international laws.
3. Weak Enforcement Mechanisms: Limited technical expertise and inadequate cyber forensics infrastructure hinder effective investigation and prosecution.
4. Privacy and Data Protection Gaps: The absence of a comprehensive data protection law creates uncertainty regarding user rights, consent, and accountability in digital interactions.
5. Low Awareness and Reporting: Many victims, especially small businesses and rural users, fail to report cyber incidents due to lack of awareness or fear of legal complexity.
6. Inadequate Cyberpolice Training: Law enforcement agencies often lack specialized cybercrime investigation skills, leading to poor evidence handling and case dismissals.
7. Rapid Technological Evolution: The rise of IoT, blockchain, and AI has outpaced the regulatory and judicial system's ability to adapt, creating enforcement blind spots.

Illustrative Issues:

- Cases involving cryptocurrency scams often fall outside the IT Act's scope.
- Cross-border phishing attacks complicate evidence collection.
- Social media misuse and data breaches highlight insufficient deterrence under existing laws.

4. Explain Trojan horse and Steganography.

Trojan Horse:

A Trojan horse is a malicious software program disguised as legitimate or harmless. It tricks users into installing it, thereby granting unauthorized access to their systems. Unlike viruses or worms, a Trojan does not replicate itself but relies on deception and user action to spread. Once activated, it can steal data, install additional malware, or enable remote control by attackers.

Key Characteristics:

1. Deceptive Appearance: Often embedded in software downloads, email attachments, or fake updates.
2. Payload Execution: After installation, it may log keystrokes, steal passwords, or modify system files.
3. Remote Access: Attackers use Trojans to control victim systems through backdoors.
4. Common Types: Backdoor Trojans, Banking Trojans, Downloader Trojans, and Ransom Trojans.

Example:

A user downloads a seemingly free game that silently installs a backdoor, allowing attackers to access banking credentials.

Steganography:

Steganography is the practice of hiding secret data within non-secret files, such as images, audio, or text, so that its presence is undetectable. Unlike encryption, which conceals content, steganography conceals existence.

Key Characteristics:

1. Data Concealment: Hidden data is embedded in file structures without visibly altering them.
2. Mediums Used: Images, videos, audio files, and network packets.
3. Detection Difficulty: The cover file appears unchanged to ordinary users and software.
4. Applications: Used for confidential communication, copyright protection, or malicious data transmission.

Example:

An attacker hides malicious code inside an image file shared over social media; once extracted, it executes harmful actions.

5. Explain Credit Card frauds.

Credit card frauds are unauthorized uses of payment cards or card data to steal money, goods, or services. They exploit weak controls across physical, online, and merchant ecosystems. Successful fraud both extracts value immediately (unauthorized transactions) and enables later criminal activity (resold card data, synthetic identities). The problem is systemic: criminals blend social engineering, technical compromise, and insider access to bypass verification and reconcile stolen funds into usable assets.

Primary types and techniques:

- Card-present skimming: Devices or malware on ATMs/terminals capture magnetic stripe data and PINs; cloned cards are used for in-person purchases.
- Card-not-present (CNP) fraud: Online or phone transactions use stolen card numbers, CVV, and expiry dates; highest growth vector because physical verification is absent.
- Account takeover (ATO): Attackers gain control of a victim's issuer or merchant account via credential stuffing, phishing, or SIM swap, then add new payment methods or request transfers.

- Application fraud / synthetic identity: Fraudsters create new accounts using a mix of real and fake identity elements to obtain new cards and lines of credit.
- Friendly fraud / chargeback abuse: Legitimate cardholder disputes a valid transaction to reclaim funds; exploited by buyers or organized rings.
- Data breaches and card dumps: Large-scale breaches expose PANs, CVVs, and tokens sold on darknet markets; facilitates mass CNP fraud.
- Insider collusion: Employees at merchants, processors, or service centers misuse access to exfiltrate card data or approve fraudulent transactions.

Consequences and indicators:

- Financial losses for issuers, merchants, and consumers; liability shifts increase operational friction.
- Indicators: unusual high-value or cross-border purchases, multiple rapid transactions, mismatched shipping and billing addresses, sudden change in device/browser fingerprints.

Mitigation and controls:

- Tokenization and EMV/chip adoption to reduce usable data from stolen cards.
- Strong authentication: 3-D Secure, MFA, behavioral biometrics, device fingerprinting.
- Real-time fraud detection: ML models, rules combined with velocity checks and geolocation validation.
- Least-privilege and segmentation across merchant POS and payment processors; regular PCI DSS compliance.
- Customer and staff education to resist phishing and social-engineering.
- Rapid breach response and information sharing with banks, card networks, and law enforcement.

6. What is DoS and DDoS attack?

A Denial of Service (DoS) attack is a deliberate attempt to make a network, website, or service unavailable to its intended users by overwhelming it with excessive requests or exploiting system vulnerabilities. The main goal is disruption—causing performance degradation, crashes, or complete service unavailability.

Mechanism:

- A single attacker targets a system by flooding it with requests or sending malformed packets.
- Common targets include web servers, mail servers, and network routers.
- DoS attacks exploit resource limitations such as bandwidth, CPU cycles, or memory.

Types of DoS Attacks:

1. Volume-based attacks: Flooding bandwidth using ICMP floods, UDP floods, or ping of death.
2. Protocol attacks: Exploit weaknesses in network protocols, e.g., SYN flood or Smurf attack.
3. Application-layer attacks: Target specific services like HTTP or DNS to exhaust application resources.

Distributed Denial of Service (DDoS) attack is an advanced form of DoS involving multiple compromised systems—often part of a botnet—coordinated to attack a single target simultaneously. This distributed nature amplifies traffic volume, making it harder to detect and mitigate.

Key Characteristics of DDoS:

- Originates from thousands of infected devices globally.
- Masks the true attacker's identity through proxy systems or botnets.
- Causes large-scale outages and financial losses for organizations.

Examples:

- The 2016 Mirai botnet attack disrupted major websites like Twitter and Netflix by flooding DNS provider Dyn with massive traffic.
- Corporate networks often face DDoS assaults as part of extortion or political campaigns.

Preventive Measures:

- Use firewalls, intrusion prevention systems (IPS), and anti-DDoS solutions.
- Employ rate limiting, traffic filtering, and load balancing.
- Monitor network traffic continuously to detect anomalies early.

7. What is Identity theft?

Identity theft is the unlawful acquisition and misuse of another person's personal or financial information to commit fraud or other crimes. Attackers exploit digital, physical, or social vulnerabilities to impersonate victims and gain unauthorized access to assets, credit, or sensitive records. It undermines both individual privacy and institutional trust.

Core Mechanism:

- Criminals gather identifying data such as name, address, date of birth, Aadhaar number, bank account details, or login credentials.
- Information sources include phishing emails, data breaches, hacked databases, stolen documents, and compromised networks.
- Once obtained, the data is used to open fake accounts, withdraw funds, apply for loans, or conduct illegal activities in the victim's name.

Types of Identity Theft:

1. Financial Identity Theft: Use of another person's financial data to make unauthorized transactions or obtain credit.
2. Criminal Identity Theft: Offenders use stolen identities when apprehended, leading to false criminal records for victims.
3. Medical Identity Theft: Fraudsters use another's insurance or medical information to receive healthcare services.
4. Synthetic Identity Theft: Combination of real and fabricated data to create a new, counterfeit identity.
5. Child Identity Theft: Stolen data of minors used to create fraudulent accounts undetected for years.

Consequences:

- Financial loss, damaged credit score, and legal complications for victims.
- Psychological distress and difficulty restoring reputation.
- Reputational and compliance risk for organizations that fail to secure user data.

Prevention and Control:

- Use strong, unique passwords and enable multi-factor authentication.
- Avoid sharing personal data through unsecured channels.
- Regularly monitor bank and credit reports for anomalies.

- Organizations must implement encryption, data minimization, and secure verification procedures.

8. Explain the process of Scanning and Scrutinizing gathered information.

Scanning and scrutinizing gathered information are critical stages in cybersecurity reconnaissance and vulnerability assessment. These processes help attackers identify exploitable weaknesses and, conversely, assist security professionals in detecting system flaws before exploitation.

1. Scanning:

Scanning follows the information-gathering or footprinting phase. It involves actively probing target systems to identify open ports, active hosts, running services, and network configurations. The goal is to map the digital structure and discover potential entry points.

Types of Scanning:

- Port Scanning: Detects open or closed ports using tools like Nmap to reveal active services.
- Network Scanning: Identifies live hosts, IP ranges, and connected devices.
- Vulnerability Scanning: Examines systems for known security flaws or misconfigurations.
- Service Scanning: Determines the version and type of running services to match them with potential exploits.

Key Techniques:

- Ping Sweeps: Locate responsive systems within a network.
- Banner Grabbing: Collects service and version information for deeper vulnerability analysis.
- TCP/UDP Scans: Reveal communication protocols and possible weak points.

2. Scrutinizing Gathered Information:

After scanning, data is analyzed to evaluate risk and prioritize vulnerabilities. Scrutinizing involves correlating results with threat intelligence and assessing exploit feasibility.

Steps in Scrutiny:

1. Data Correlation: Matching scan results with known vulnerabilities (e.g., CVE databases).
2. Prioritization: Ranking weaknesses based on severity, exposure, and potential business impact.
3. Verification: Validating whether detected vulnerabilities are real or false positives.
4. Documentation: Recording findings for remediation planning and audit purposes.

Tools Commonly Used:

- Nmap, Nessus, OpenVAS, Qualys, and Nikto for automated scanning and analysis.

9. What is the role of cybercrime cells in India?

Scanning and scrutinizing gathered information are critical stages in cybersecurity reconnaissance and vulnerability assessment. These processes help attackers identify exploitable weaknesses and, conversely, assist security professionals in detecting system flaws before exploitation.

1. Scanning:

Scanning follows the information-gathering or footprinting phase. It involves actively probing target systems to identify open ports, active hosts, running services, and network configurations. The goal is to map the digital structure and discover potential entry points.

Types of Scanning:

- Port Scanning: Detects open or closed ports using tools like Nmap to reveal active services.
- Network Scanning: Identifies live hosts, IP ranges, and connected devices.
- Vulnerability Scanning: Examines systems for known security flaws or misconfigurations.
- Service Scanning: Determines the version and type of running services to match them with potential exploits.

Key Techniques:

- Ping Sweeps: Locate responsive systems within a network.
- Banner Grabbing: Collects service and version information for deeper vulnerability analysis.
- TCP/UDP Scans: Reveal communication protocols and possible weak points.

2. Scrutinizing Gathered Information:

After scanning, data is analyzed to evaluate risk and prioritize vulnerabilities. Scrutinizing involves correlating results with threat intelligence and assessing exploit feasibility.

Steps in Scrutiny:

1. Data Correlation: Matching scan results with known vulnerabilities (e.g., CVE databases).
2. Prioritization: Ranking weaknesses based on severity, exposure, and potential business impact.
3. Verification: Validating whether detected vulnerabilities are real or false positives.
4. Documentation: Recording findings for remediation planning and audit purposes.

Tools Commonly Used:

- Nmap, Nessus, OpenVAS, Qualys, and Nikto for automated scanning and analysis.

10. What do you mean by Cyber Stalking?

Cyberstalking is the use of the internet, digital devices, or electronic communication to harass, intimidate, or monitor an individual or group. It involves persistent, unwanted contact or surveillance that causes fear, distress, or violation of privacy. Unlike one-time online harassment, cyberstalking is characterized by continuous and deliberate digital intrusion.

Core Features:

- Repeated communication through emails, messages, or social media.
- Monitoring online activities, tracking location, or collecting personal data.
- Posting defamatory or private information publicly.
- Impersonating the victim online to damage reputation or relationships.

Common Methods:

1. Email and Message Harassment: Sending threats, obscene content, or excessive unwanted messages.
2. Social Media Exploitation: Creating fake profiles or spreading rumors to discredit the victim.
3. Surveillance Tools: Using spyware, GPS tracking, or hacking to monitor the victim’s digital presence.

4. Doxxing: Public release of private details such as address or contact information to incite harm.

Motives:

- Revenge, obsession, personal vendetta, or psychological gratification.
- In some cases, linked to domestic abuse or workplace conflicts.

Consequences:

- Severe psychological impact, including anxiety, trauma, and fear of online participation.
- Potential physical threats if digital stalking escalates to real-world encounters.

Legal Perspective (India):

- Addressed under Section 354D of the Indian Penal Code (IPC) and the Information Technology (IT) Act, 2000.
- Offenders face imprisonment and fines depending on the severity of harassment.

Preventive Measures:

- Avoid sharing excessive personal details online.
- Strengthen privacy settings and use two-factor authentication.
- Report incidents to cybercrime cells or law enforcement with digital evidence.

11. Explain Authentication Service Security.

Authentication service security refers to the mechanisms and controls used to verify user identities and ensure that only legitimate entities gain access to systems, networks, or data. It is the foundation of cybersecurity because it establishes trust before granting authorization. Weak authentication directly leads to data breaches, unauthorized access, and system compromise.

Core Components of Authentication Security:

1. Identification: The user claims an identity, typically through a username or ID.
2. Authentication: The system verifies that identity using credentials such as passwords, tokens, or biometrics.
3. Authorization (Post-Authentication): Once verified, the system grants permissions aligned with the user's role.

Authentication Factors:

- Something you know: Passwords, PINs, security questions.
- Something you have: Smart cards, hardware tokens, mobile OTPs.
- Something you are: Biometric identifiers like fingerprints, facial recognition, or iris scans.

Common Authentication Mechanisms:

1. Password-Based Authentication: Simple but vulnerable to brute-force and phishing attacks.
2. Multi-Factor Authentication (MFA): Combines multiple factors to strengthen security.
3. Token-Based Authentication: Uses digital tokens (e.g., OAuth, JWT) for session validation.
4. Biometric Authentication: Uses physical traits for identity confirmation.
5. Certificate-Based Authentication: Employs digital certificates issued by trusted authorities.

Security Threats to Authentication Services:

- Password reuse and weak credential hygiene.

- Phishing and credential-stealing malware.
- Man-in-the-middle (MITM) and replay attacks.
- Compromised authentication servers or insecure token storage.

Best Practices for Strengthening Authentication Security:

- Implement MFA for all critical systems.
- Use salted hashing and encryption for credential storage.
- Regularly update authentication protocols and enforce password policies.
- Employ adaptive authentication based on risk factors (location, device, behavior).
- Log and monitor authentication attempts for anomaly detection.

12. What is Phishing, Password cracking, key-loggers and Spyware?

Phishing:

Phishing is a deceptive technique used to trick individuals into revealing confidential information such as passwords, credit card details, or login credentials. Attackers impersonate legitimate entities—like banks, service providers, or government agencies—through fake emails, messages, or websites.

Key Characteristics:

- Uses social engineering to exploit trust.
- Common forms include email phishing, spear phishing (targeted), and smishing (SMS-based).
- Links or attachments redirect users to counterfeit websites or install malware.
  Example: A fake bank email asks users to "verify" account details through a malicious link, stealing their credentials.

Password Cracking:

Password cracking involves systematically recovering passwords from stored or transmitted data. Attackers use automated tools and algorithms to guess or decrypt passwords.

Techniques:

- Brute-force attacks test every possible combination.
- Dictionary attacks use common password lists.
- Rainbow table attacks exploit precomputed hash values.
  Goal: Gain unauthorized access to systems, emails, or financial accounts.

Key-Loggers:

A key-logger is malicious software or hardware that records every keystroke made on a computer or mobile device.

Functions:

- Captures usernames, passwords, and private messages.
- Operates silently in the background.
- Can transmit logged data to remote servers.
  Types: Software-based (installed via malware) and hardware-based (USB or embedded devices).

Spyware:

Spyware is software designed to secretly monitor user activity and collect data without consent. It often comes bundled with free software or through malicious downloads.

Capabilities:

- Tracks browsing history, login details, and system activity.
- Slows device performance and consumes bandwidth.

- Can enable remote surveillance or data theft.

13. Give Difference between Passive and Active attacks.

Cyberattacks are broadly categorized into **passive** and **active** based on how the attacker interacts with the target system. Both compromise data security but differ in execution, visibility, and intent.

Aspect	Passive Attack	Active Attack
Definition	An attack where the intruder monitors or intercepts data without altering system resources or communications.	An attack where the intruder modifies, disrupts, or injects data into the communication or system.
Primary Objective	To gather information secretly.	To damage, alter, or gain control over system resources.
Nature	Stealthy and non-disruptive.	Intrusive and disruptive.
Interaction with System	No direct modification of data or operations.	Direct interference or manipulation of data, system files, or communication channels.
Detection	Difficult to detect since operations remain normal.	Easier to detect due to system anomalies or performance degradation.
Examples	- Eavesdropping on network traffic. - Traffic analysis to infer communication patterns.	- Data modification or deletion. - Denial of Service (DoS) and Distributed Denial of Service (DDoS). - Masquerading or session hijacking.
Impact on Integrity and Availability	Compromises confidentiality only.	Affects confidentiality, integrity, and availability.
Goal	Information collection for later exploitation.	Immediate disruption or unauthorized access.

14. What are the counter measures of Identity theft? How to protect online identity?

Countermeasures of Identity Theft and Protection of Online Identity

Identity theft prevention relies on minimizing data exposure, securing credentials, and maintaining constant monitoring of personal and financial information. Countermeasures are both individual and organizational, focusing on proactive defense and incident response.

1. Technical Countermeasures:

- Strong Authentication: Use complex, unique passwords and enable multi-factor authentication (MFA) on all critical accounts.
- Encryption: Encrypt sensitive data during storage and transmission to prevent interception.
- Secure Networks: Avoid public Wi-Fi for financial transactions; use VPNs for secure connections.
- Regular Software Updates: Patch operating systems, browsers, and applications to close security vulnerabilities.

- Firewalls and Anti-Malware: Employ reputable antivirus and firewall solutions to detect malicious activity or phishing attempts.

2. Behavioral and Preventive Measures:
   - Limit Data Sharing: Avoid disclosing personal information (birth date, address, ID numbers) on unsecured websites or social media.
   - Verify Sources: Confirm authenticity of emails, messages, and websites before providing credentials.
   - Monitor Accounts: Regularly review bank statements, credit reports, and login history for suspicious activity.
   - Use Secure Websites: Ensure "https://" and valid SSL certificates before entering sensitive information online.
   - Dispose of Data Properly: Shred physical documents containing personal data and securely erase digital files before disposal.
3. Organizational and Legal Safeguards:
   - Data Protection Policies: Organizations must implement access controls, employee training, and encryption standards.
   - Incident Response Plans: Quick reporting and mitigation reduce financial and reputational damage.
   - Compliance with Regulations: Adherence to privacy laws like the IT Act, 2000, and upcoming data protection frameworks.
4. Protection of Online Identity:
   - Use privacy settings to restrict profile visibility on social platforms.
   - Avoid clicking unknown links or downloading unsolicited attachments.
   - Employ password managers to prevent reuse across multiple accounts.
   - Regularly clear browser history, cookies, and cache to reduce tracking.

15. What is Software Piracy?

Software Piracy is the illegal copying, distribution, or use of software without proper authorization or a valid license from the copyright owner. It violates intellectual property rights and undermines the software industry's economic and security foundations.

Forms of Software Piracy:

1. Softlifting: Installing a single licensed copy of software on multiple computers beyond the permitted limit.
2. Counterfeiting: Creating and selling fake software copies that appear genuine.
3. Internet Piracy: Distributing cracked or unauthorized software through websites, torrents, or file-sharing platforms.
4. Client-Server Overuse: Allowing more concurrent users than the license agreement allows in a networked environment.
5. Hard-Disk Loading: Vendors preinstall unlicensed software on computers sold to customers.
6. Rental Piracy: Renting software without the copyright holder's consent.

Consequences of Software Piracy:

- Legal: Copyright infringement leading to fines, lawsuits, or criminal charges.
- Economic: Loss of revenue for developers and reduced innovation incentives.
- Security: Pirated software often contains malware, spyware, or backdoors compromising user systems.

- Performance Risks: Lack of updates, patches, and technical support causes instability and data loss.

Preventive Measures:

- Use only licensed and verified software from authorized vendors.
- Employ digital rights management (DRM) and license verification systems.
- Educate users on legal and ethical aspects of software usage.
- Organizations should conduct periodic software audits to ensure compliance.

16. Explain Spamming and how it affects users.

Spamming refers to the practice of sending unsolicited, irrelevant, or inappropriate messages over the internet — usually in bulk — to promote products, spread malware, or conduct scams. Most spam is sent via email, but it can also occur through social media, messaging apps, or comment sections.

Types of Spamming:

1. Email Spam: Junk emails sent to advertise fake products or phishing links.
2. Social Media Spam: Fake posts, friend requests, or messages promoting scams.
3. Comment Spam: Irrelevant promotional comments on blogs, videos, or forums.
4. Messaging Spam: Unwanted promotional texts or links through SMS or chat apps.

Effects of Spamming on Users:

1. Security Risks:
   - Spam often contains malicious links or attachments that install malware, ransomware, or spyware.
2. Phishing Attacks:
   - Many spam messages try to trick users into revealing personal or financial information.
3. Wasted Time and Resources:
   - Sorting through unwanted emails reduces productivity and clogs inboxes.
4. Network Congestion:
   - Excessive spam traffic can slow down networks and consume bandwidth.
5. Financial Loss:
   - Clicking on fraudulent links or fake offers can lead to identity theft or money loss.

Preventive Measures:

- Use spam filters in email clients.
- Never click on suspicious links or attachments.
- Unsubscribe only from trusted sources (not from unknown senders).
- Report spam emails to your provider.
- Keep your antivirus and firewall updated.

17. What are the measures for handling mobile in an organization?

Measures for Handling Mobile Devices in an Organization

Mobile devices such as smartphones, tablets, and laptops introduce significant security risks due to their portability, connectivity, and data storage capacity. Effective management requires technical controls, policies, and user awareness to prevent data leaks, malware infections, and unauthorized access.

1. Policy and Governance Measures

- Mobile Device Management (MDM): Implement MDM software to monitor, configure, and secure all organizational devices remotely.
- Acceptable Use Policy: Define permissible usage, data access rules, and employee responsibilities.
- Bring Your Own Device (BYOD) Policy: Enforce security requirements for personal devices accessing corporate networks, including mandatory encryption and antivirus installation.
- Access Control: Restrict access to sensitive systems based on user role and device compliance.

2. Technical and Security Controls

- Encryption: Encrypt all stored data and communication channels to prevent interception.
- Authentication: Use strong passwords, biometric verification, and multi-factor authentication (MFA).
- Remote Wipe and Lock: Enable the ability to erase or disable lost or stolen devices immediately.
- Regular Updates: Ensure timely installation of OS and application security patches.
- App Management: Restrict installation of unverified or third-party applications.
- Network Security: Require use of secure Wi-Fi or VPN connections for remote access.

3. Monitoring and Incident Response

- Continuous Monitoring: Track device activity, detect policy violations, and log security events.
- Incident Handling: Establish a response plan for lost devices, data breaches, or unauthorized access.
- Backup and Recovery: Maintain encrypted backups to ensure data restoration in case of compromise.

4. Awareness and Training

- Educate employees about phishing, malicious apps, and secure handling of sensitive information.
- Conduct periodic security drills and compliance audits.

18. How do viruses and worms differ?

Basis of Difference	Virus	Worm
Definition	A malicious program that attaches itself to legitimate files or software and spreads when the host is executed.	A self-replicating malicious program that spreads automatically across networks without human action.

Basis of Difference	Virus	Worm
Dependency	Depends on a host file or program to execute and propagate.	Independent; does not require a host program to spread.
Replication Method	Replicates only when the infected file is run by the user.	Replicates itself automatically through networks or email systems.
Mode of Spread	Spreads via infected files, removable media, or email attachments.	Spreads through network vulnerabilities and internet connections.
User Interaction	Requires user action (e.g., opening a file or running a program).	Does not require user action; spreads autonomously.
Primary Damage	Corrupts or deletes files, damages programs, or alters system data.	Consumes network bandwidth, slows systems, or causes network congestion.
Speed of Spread	Relatively slower, as it depends on user activity.	Very fast; spreads exponentially across connected systems.
Examples	Michelangelo, Melissa, ILOVEYOU.	Code Red, Mydoom, Conficker.

19. What is social engineering? Write one example of it.

Social Engineering

Social engineering is a psychological manipulation technique used by cybercriminals to trick individuals into revealing confidential information, granting access, or performing actions that compromise security. Instead of exploiting technical vulnerabilities, it exploits human trust, curiosity, or fear.

Key Characteristics

- Relies on deception and persuasion, not hacking tools.
- Targets people, not systems.
- Often used to gain access to passwords, financial details, or system credentials.

Common Techniques

1. Phishing: Fake emails or messages designed to steal sensitive information.
2. Pretexting: Creating a false story or identity to gain trust (e.g., posing as an IT staff).
3. Baiting: Offering something tempting (like free software or USB drives) that actually contains malware.
4. Tailgating: Following authorized personnel into restricted areas.
5. Quid pro quo: Offering help or service in exchange for confidential information.

Example

A hacker sends an email appearing to be from a bank, asking the victim to “verify account details” by clicking a link. The link leads to a fake website that collects login credentials. This is a phishing attack, one of the most common forms of social engineering.