CCLI MP 2

2 marks

1. Write the different types of Cyber-crimes.

- Cyber-crimes are illegal activities committed using digital devices and networks.
- Types include hacking, phishing, identity theft, cyberbullying, malware distribution, online scams, cyberstalking, and ransomware attacks.

2. Define Phishing and Vishing.

- Phishing is a cybercrime tactic where attackers impersonate legitimate entities to trick individuals into providing sensitive information such as passwords, credit card details, or personal data.
- Vishing is similar to phishing but involves the use of phone calls or voice messages to deceive targets into divulging confidential information.

3. What is a salami attack?

- A salami attack is a type of cybercrime where the perpetrator steals small amounts of money or data over time, often from numerous accounts or transactions, with the intention of avoiding detection.
- The name comes from the idea of slicing small pieces, like salami, from a larger entity.

4. Write the Wi-Fi Security settings in the computer.

- Wi-Fi security settings on a computer include:
    - Encryption protocols such as WPA2 or WPA3 to secure data transmission.
    - Strong, unique passwords for the Wi-Fi network.
    - Network isolation to prevent unauthorized access to other devices.
    - Disabling SSID broadcasting to hide the network from view.
    - MAC address filtering to only allow specified devices to connect.

5. Define Hackers.

- Hackers are individuals with advanced computer skills who use their technical knowledge to gain unauthorized access to computer systems or networks.
- They may do this for various reasons, including testing system security, pursuing personal gain, activism, or malicious intent.

6. What is copyright and patent?

- Copyright is a legal right that grants the creator of an original work exclusive rights to its use and distribution, usually for a limited time, with the intention of encouraging creativity and protecting intellectual property.
- Patents, on the other hand, are exclusive rights granted by a government to an inventor for a limited period, in exchange for full disclosure of the invention, with the aim of encouraging innovation by providing inventors with a temporary monopoly over their invention.

5 marks

7. Steps of Filing an Offline/Online Cyber Complaint

Offline Filing:

1. **Contact Law Enforcement:**
    - Visit the nearest police station or cybercrime cell.
    - Explain the incident and provide necessary details like date, time, and nature of the cybercrime.
2. **Filing a Complaint:**
    - Fill out the required forms provided by the authorities.
    - Provide supporting evidence such as screenshots, emails, or transaction details.
3. **Investigation:**
    - Law enforcement may conduct an investigation based on the complaint filed.
    - Cooperation with authorities may be required during this process.
4. **Follow-up:**
    - Stay in touch with the investigating officer for updates on the case.
    - Provide any additional information or assistance requested.

Online Filing:

1. **Visit Cybercrime Portal:**

- Access the official cybercrime reporting portal provided by law enforcement or government agencies.

2. **Fill Complaint Form:**
    - Fill out the online complaint form with accurate details of the incident.
    - Attach any relevant documents or evidence electronically.
3. **Submit Complaint:**
    - Submit the completed form through the online portal.
    - Await acknowledgment or reference number for the complaint.
4. **Follow-up:**
    - Keep track of the complaint status using the reference number provided.
    - Respond promptly to any queries or requests from authorities.

8. Checklist for Security Settings on Popular Social Media Platforms

- **Privacy Settings:**
    - Review and adjust privacy settings to control who can see your posts, personal information, and photos.
    - Enable two-factor authentication for added security.
- **Friend/Follower Requests:**
    - Be cautious of accepting friend or follower requests from unknown or suspicious accounts.

    - Verify the identity of new connections before accepting requests.
- **Content Sharing:**
    - Think before sharing personal information, photos, or location details publicly.
    - Avoid sharing sensitive information that could be used for identity theft or fraud.
- **Third-Party Apps and Permissions:**
    - Regularly review and revoke access to third-party apps that have access to your social media accounts.
    - Limit the amount of information shared with third-party applications.
- **Reporting and Blocking:**
    - Familiarize yourself with the platform's reporting and blocking features.
    - Report any abusive or inappropriate behavior encountered on the platform.

9. Applying Security Settings on Mobile Wallets and UPIs

- **PIN/Password Protection:**
    - Set up a strong PIN or password to access your mobile wallet or UPI application.
    - Avoid using easily guessable PINs or passwords.
- **Biometric Authentication:**
    - Enable biometric authentication methods such as fingerprint or facial recognition where available.

    - This adds an extra layer of security to your transactions.
- **Transaction Limits:**
    - Set transaction limits to control the amount of money that can be transferred or spent in a single transaction.
    - Lower limits can minimize the impact of unauthorized transactions.
- **Secure Network Connection:**
    - Only use secure Wi-Fi networks or mobile data when making transactions.
    - Avoid using public Wi-Fi networks for financial transactions to prevent interception of sensitive data.
- **Regular Updates:**
    - Keep your mobile wallet or UPI application updated with the latest security patches and versions.
    - Updates often contain fixes for known security vulnerabilities.

10. Different Tools for Cybersecurity

- **Firewalls:**
    - Monitor and control incoming and outgoing network traffic based on predetermined security rules.
    - Helps prevent unauthorized access to or from private networks.
- **Antivirus Software:**
    - Detects and removes malicious software, including viruses, worms, and Trojans, from computers and networks.

    - Provides real-time protection against malware threats.
- **Intrusion Detection Systems (IDS):**
    - Monitors network or system activities for malicious activities or policy violations.
    - Alerts administrators to potential security breaches.
- **Vulnerability Scanners:**
    - Identifies weaknesses in a system's security posture by scanning for known vulnerabilities.
    - Helps prioritize and address security issues before they are exploited by attackers.
- **Encryption Tools:**
    - Encrypts sensitive data to protect it from unauthorized access during transmission or storage.
    - Utilizes algorithms to encode information in a way that can only be decrypted with the appropriate key.

11. Steps for Installation and Configuration of Antivirus in Computers

1. **Download Antivirus Software:**
    - Visit the official website of the antivirus provider or download from a trusted source.
2. **Install the Software:**
    - Run the downloaded installer and follow the on-screen instructions to install the antivirus software on your computer.
3. **Update Virus Definitions:**

- After installation, update the antivirus program to ensure it has the latest virus definitions and security updates.

4. **Perform Full System Scan:**
    - Initiate a full system scan to check for any existing malware or threats on your computer.
5. **Configure Real-Time Protection:**
    - Enable real-time protection features to monitor file downloads, email attachments, and web browsing activities for potential threats.
6. **Schedule Regular Scans:**
    - Set up scheduled scans to automatically check your computer for malware at specified intervals.
7. **Customize Settings:**
    - Customize antivirus settings according to your preferences, such as scanning exclusions or quarantine actions.
8. **Activate Firewall (if included):**
    - If the antivirus software includes a firewall, configure it to monitor and control incoming and outgoing network traffic.

12. Short Note on Patent Registration

- **Definition:**
    - Patent registration is the process of obtaining exclusive rights to an invention or innovation from a government authority for a specified period.

    - It grants the patent holder the legal authority to prevent others from making, using, selling, or distributing the patented invention without permission.
- **Importance:**
    - Encourages innovation by providing inventors with a temporary monopoly over their inventions.
    - Protects intellectual property and incentivizes investment in research and development.
- **Process:**
    - Conduct a patent search to ensure the invention is novel and not already patented.
    - Prepare and file a patent application with the relevant patent office, providing detailed descriptions and claims of the invention.
    - Pay the required fees and comply with all formalities and deadlines set by the patent office.
    - The patent office examines the application to determine if the invention meets the criteria for patentability.
    - If approved, the patent is granted, and the inventor gains exclusive rights to the invention for the duration of the patent term.
- **Duration:**
    - The duration of a patent varies depending on the country and type of patent but typically lasts for 20 years from the filing date.
- **Protection:**

- Once granted, the patent holder can take legal action against any unauthorized use, manufacture, or sale of the patented invention.
- Patent rights can be enforced through civil litigation, resulting in injunctions, damages, or royalties for the patent holder.

- **Conclusion:**
  - Patent registration is essential for inventors and innovators to protect their intellectual property rights and benefit from their creations commercially.

8 marks

13. Steps for Identifying Phishing Emails

Understanding Phishing Emails:

Phishing emails are fraudulent messages sent by cybercriminals with the intention of tricking recipients into revealing sensitive information, such as login credentials, financial details, or personal data. Identifying phishing emails is crucial to protect oneself from falling victim to such scams.

Steps for Identifying Phishing Emails:

1. **Check the Sender's Email Address:**
   - Examine the sender's email address carefully for any discrepancies or irregularities.
   - Look for misspellings or variations of legitimate domain names, which are common tactics used by phishers to deceive recipients.

2. **Review the Salutation and Content:**
    - Phishing emails often use generic salutations like "Dear Customer" instead of addressing recipients by name.
    - Pay attention to the content of the email for grammatical errors, unusual language, or urgent requests, which are common red flags of phishing attempts.
3. **Inspect Hyperlinks and URLs:**
    - Hover over hyperlinks embedded in the email to reveal the actual URL.
    - Verify that the URL matches the legitimate website it claims to link to.
    - Be cautious of shortened URLs or links that lead to suspicious domains.
4. **Examine Attachments:**
    - Avoid opening attachments from unknown or untrusted senders.
    - Verify the legitimacy of attachments by scanning them with antivirus software before opening.
5. **Verify Requests for Personal Information:**
    - Legitimate organizations typically do not request sensitive information like passwords, credit card numbers, or social security numbers via email.
    - Treat any such requests with skepticism and verify their authenticity through alternate channels.
6. **Look for Branding and Logos:**

- Phishing emails often lack official branding or contain poorly replicated logos of reputable organizations.
- Compare the email's design and branding with previous communications from the purported sender to identify inconsistencies.

7. **Be Wary of Urgency or Threats:**
    - Phishing emails often create a sense of urgency or use threats to coerce recipients into taking immediate action.
    - Take a step back and carefully evaluate the legitimacy of such demands before responding or clicking on any links.
8. **Report Suspected Phishing Attempts:**
    - If you suspect an email to be a phishing attempt, report it to your organization's IT security team or the appropriate authorities.
    - Reporting phishing emails helps protect others from falling victim to similar scams.

By following these steps and exercising caution, individuals can effectively identify and avoid falling prey to phishing emails, safeguarding their personal and sensitive information from cyber threats.

14. Short Note on Important Sections in IT Act

The Information Technology (IT) Act, enacted in 2000, is an important legislation in India that addresses various aspects of electronic commerce, digital signatures, cybercrimes, and data protection. Several sections of the IT Act play a significant role in regulating and governing digital transactions, cybersecurity, and online activities.

Important Sections in the IT Act:

1. **Section 43A - Data Protection:**
    - This section mandates the protection of sensitive personal data and prescribes penalties for unauthorized disclosure of such information.
    - It requires organizations handling sensitive personal data to implement reasonable security practices and procedures to protect the confidentiality and integrity of the data.
2. **Section 66 - Cybercrime Offenses:**
    - Section 66 of the IT Act deals with various cybercrimes, including unauthorized access to computer systems, data theft, hacking, and introduction of malware.
    - It prescribes penalties for offenses related to computer systems, networks, and data, with imprisonment and fines for perpetrators.
3. **Section 66A - Communication Offenses:**
    - This section addresses offenses related to communication over computer networks, such as sending offensive or menacing messages.
    - However, Section 66A was struck down by the Supreme Court of India in 2015 for being unconstitutional and violating freedom of speech and expression.
4. **Section 69 - Government's Power to Monitor:**
    - Section 69 grants the government the authority to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource.

- It empowers government agencies to undertake surveillance for national security purposes, subject to certain safeguards and procedures.

5. **Section 72 - Breach of Confidentiality:**
    - This section prohibits the disclosure of personal information obtained through legal access to computer systems in breach of a lawful contract.
    - It imposes penalties for wrongful disclosure of information with the intent to cause wrongful loss or gain to oneself or another person.

These sections, among others, form the legal framework under the IT Act to address various aspects of cybersecurity, data protection, and digital transactions in India. Understanding and adhering to the provisions of the IT Act are essential for promoting secure and lawful use of information technology in the country.

15. Various Data Protection Laws in India

India has seen significant developments in data protection laws aimed at safeguarding the privacy and security of individuals' personal data. Several key legislations and regulations govern data protection in the country, each addressing specific aspects of data privacy and security.

Major Data Protection Laws in India:

1. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:**
    - These rules, framed under Section 43A of the IT Act, prescribe standards for the protection of sensitive personal data or information by body corporates.

- They require entities handling sensitive personal data to implement reasonable security practices and procedures to protect the data from unauthorized access, use, disclosure, or destruction.

2. **The Personal Data Protection Bill, 2019:**
    - The Personal Data Protection Bill, 2019 aims to provide a comprehensive framework for the protection of personal data in India.
    - It introduces principles such as data minimization, purpose limitation, and accountability, along with provisions for consent, data localization, and rights of individuals over their data.
3. **General Data Protection Regulation (GDPR) Compliance:**
    - While not a domestic law, the GDPR has implications for Indian entities processing personal data of individuals in the European Union (EU).
    - Indian organizations handling EU data must comply with the GDPR's requirements regarding data protection, privacy rights, and cross-border data transfers.
4. **Sector-Specific Regulations:**
    - Various sector-specific regulations and guidelines mandate data protection measures in specific industries such as banking, healthcare, telecommunications, and e-commerce.
    - These regulations often require entities operating in these sectors to implement industry-specific standards and safeguards for protecting personal data.
5. **International Agreements and Standards:**

- India is a signatory to international agreements and standards that promote data protection and privacy, such as the Convention on Cybercrime (Budapest Convention) and ISO/IEC 27001 standards for information security management.

16. Implementation of Security Features in Net Banking

Security Features in Net Banking:

Net banking, also known as online banking or internet banking, enables users to conduct banking transactions and manage their accounts over the internet. Implementing robust security features is essential to protect the confidentiality, integrity, and availability of sensitive financial information in net banking platforms.

Key Security Features in Net Banking:

1. **User Authentication:**
    - Implement multi-factor authentication (MFA) mechanisms, requiring users to provide multiple credentials such as passwords, security tokens, or biometric data for access.
    - Use strong password policies, enforcing complex passwords and regular password changes to mitigate the risk of unauthorized access.
2. **Secure Communication Protocols:**
    - Utilize encrypted communication channels such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to ensure secure data transmission between the user's device and the banking server.
    - Employ digital certificates to authenticate the identity of the banking website and establish a secure connection.

3. **Session Management:**
    - Implement session timeout mechanisms to automatically log out users after a period of inactivity, reducing the risk of unauthorized access due to session hijacking.
    - Enable single-use session tokens or cookies to prevent replay attacks and session fixation vulnerabilities.
4. **Transaction Authorization:**
    - Require additional authorization for high-risk transactions or sensitive operations, such as fund transfers above a certain threshold or changes to account settings.
    - Implement transaction signing mechanisms using cryptographic techniques to verify the authenticity and integrity of transactions.
5. **Fraud Detection and Monitoring:**
    - Deploy advanced fraud detection algorithms and real-time monitoring systems to detect suspicious activities, anomalies, or unauthorized access attempts.
    - Enable alerts and notifications for unusual account activities, such as login attempts from unfamiliar locations or multiple failed authentication attempts.
6. **Device and Browser Security:**
    - Encourage users to keep their devices and web browsers up-to-date with the latest security patches and updates to mitigate vulnerabilities.

- Implement device fingerprinting or device recognition techniques to identify and authenticate trusted devices used for net banking access.

7. **Customer Education and Awareness:**
    - Educate customers about safe net banking practices, such as avoiding public Wi-Fi networks, safeguarding login credentials, and recognizing phishing attempts.
    - Provide tips and guidance on how to securely use net banking services and protect against common cyber threats.