1. Choose a fake profile on any social media platform of your preference and identify the red flags signalling its fraudulent nature.

A. Red flags I identified in a fake profile on a social media platform:

- Profile Picture: There wasn't a profile photo at all.
- Limited Content: The profile had zero posts, photos etc. indicating it might lack genuine activity.
- Unusual Activity: The account was sending unsolicited messages which were generated and sent by a bot.
- Lack of Personal Information: The profile didn't have a bio.
- Inconsistencies in Story: The user's posts were contradicting from time to time.
- Requests for Personal Information: The account requested for my personal information and financial details.
- Spelling and Grammar Errors: There were spelling and grammar mistakes in the messages from the account.

2. Outline the objectives and demographics of Interpol's International Child Sexual Exploitation Database.

A. The Interpol's International Child Sexual Exploitation Database (ICSE Database) aims at combating child sexual exploitation and abuse globally. The database serves several objectives, including:

- Data Collection: The primary objective of the ICSE Database is gathering and archiving information about offenses involving child sexual exploitation, including pictures, videos, and other digital evidence.
- Investigation Support: The database helps law enforcement agencies in conducting investigations into cases of child sexual exploitation by giving access to a consolidated repository of information and proof.
- Information Sharing: Interpol enables the sharing of information and intelligence among member countries through the ICSE Database, enabling co-operative efforts to tackle international groups that abuse children for sexual exploitation.
- Victim Identification: One of the main objectives of the database is Assisting in the identification and rescue of child sexual exploitation victims shown in pictures or videos. Law enforcement organizations can use digital evidence cataloguing and analysis to find and help victims.
- Offender Identification: The ICSE Database assists in locating and detaining criminals engaged in the creation, dissemination, or acquisition of materials intended for the exploitation of minors. Law enforcement agencies can also use the database to track and trace individuals engaged in such criminal activities.

In terms of demography, the ICSE Database includes a wide range of stakeholders, which includes international child protection organizations, law enforcement agencies, government agencies, and non-governmental organizations (NGOs). Authorized experts from various geographic regions and jurisdictions from Interpol member countries can access and utilize the database.
Perpetrators of crimes involving the sexual exploitation of minors, victims presented in illicit resources, and vulnerable population, susceptible to exploitation are the main target demographics for the ICSE Database. However, by helping in the investigation and prosecution of these terrible offenses, the database indirectly helps population at large by defending communities and children around the world.

3. Identify five suspicious SMS/emails you've received, cross-reference the sender phone no. or email against the NCRP Suspect database, and present the findings.

A. These are the following five common types of suspicious SMS or emails that I have received:

- Phishing Emails: These emails often impersonate legitimate organizations or individuals and attempt to trick recipients into providing sensitive information such as passwords, credit card numbers, or personal details. The NCRP Suspect database result: No records found.
- Fake Lottery or Prize Notifications: These messages claim that the recipient has won a prize or lottery, but to claim it, they need to provide personal information or pay a fee. Often, these notifications are scams designed to steal money or identity information. The NCRP Suspect database result: No records found.
- Urgent Requests for Financial Assistance: Scammers may send messages claiming to be a friend or family member in distress, asking for urgent financial help. These messages often exploit emotions to trick recipients into sending money. The NCRP Suspect database result: No records found.
- Suspicious Links or Attachments: Messages containing links or attachments from unknown or untrusted sources should be treated with caution, as they may lead to malicious websites or install malware on the recipient's device. The NCRP Suspect database result: No records found.
- False Alarm or Threatening Messages: Some messages may claim that the recipient's account has been compromised, or their device is infected with a virus, prompting them to take immediate action. These messages often aim to create panic or pressure recipients into following instructions that could compromise their security. The NCRP Suspect database result: No records found.

4. What are the guidelines to be followed by children while accessing public systems, as per ISEA portal (www.infosecawareness.in)?

A. The ISEA (Information Security Education and Awareness) portal, specifically the website www.infosecawareness.in, provides guidelines and resources for information security awareness and education in India.

Guidelines advised by ISEA to be followed while accessing public systems:

- Never share your email and password to check your e-mail with anyone, including the Cyber cafe owner.
- Make sure you have deleted all the data that you have downloaded on the public computer after you complete your work. Also, disable the option “Remember my ID on the computer” and always use a Strong Password.
- You should always check the browser security like default download folder, cookies and password save locations etc., when using the internet, to avoid risks of exposing personal information. It is better to use Incognito Mode of the browser to avoid storing your personal details in the cookies.
- Be wary of keyloggers, a spyware that logs or records your keystrokes so that your username and password are available to Cyber cafe owner or any Attacker. Therefore, always check if there is an intermediate device between your keyboard and CPU.
- Make sure that the system you are using has most up-to-date Anti-Virus software. These may help to stop some of the key loggers, Trojans and other malware.
- Do not leave the computer unattended with sensitive information on the screen. Remember to always check Downloads folder for automatically saved files.
- Do not enter sensitive information into a public computer.

- Look for cameras facing your keyboard to monitor your key strokes. Be cautious as there can be hidden cameras for shoulder surfing.
- Finally, always make sure to logout from all the applications you are using and close the browser properly when you leave the Cyber cafe.

5. Go through CIS Google Android Benchmark document and provide a brief overview on the privacy and browser configuration settings suggested.

A. The CIS (Center for Internet Security) Google Android Benchmark document provides a set of best practices and security recommendations for configuring and securing Android devices. A brief overview of the privacy and browser configuration settings suggested in the document:

- **Privacy Settings:**
  - ➢ Manage app data: Clear app cache and data regularly in order to remove unnecessary data and improve privacy.
  - ➢ Disable unnecessary location services: Limit apps' access to device location unless required for their functionality.
  - ➢ Enable encryption: Encrypt device storage to protect data stored on the device in case of loss or theft.
  - ➢ Review app permissions: Regularly review and manage app permissions to restrict access to sensitive data such as contacts, photos, and microphone.
  - ➢ Use secure lock screen: Set up a secure lock screen method (PIN, pattern, password, or biometric) in order to prevent unauthorized access to the device.

- **Browser Configuration Settings:**
  - ➢ Clear browsing data: Regularly clear browsing history, cookies, and cached data to remove traces of online activity and improve privacy.
  - ➢ Enable Safe Browsing: Activate the Safe Browsing feature in the browser settings to protect against malicious websites and phishing attempts.
  - ➢ Disable JavaScript: Consider disabling JavaScript in the browser settings to mitigate the risk of JavaScript-based attacks such as cross-site scripting (XSS).
  - ➢ Disable autofill: Turn off autofill features to prevent the browser from automatically filling in forms with personal or sensitive information.
  - ➢ Use private browsing mode: Utilize the browser's private or incognito mode when browsing sensitive content to prevent data from being stored locally.