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

ANSWER:

Here are some telltale signs of a fraudulent social media profile:

1. **Profile Photos**:
	* **Too Perfect**: If the profile picture looks like it belongs in a magazine or a shampoo ad, be suspicious.
	* **Reverse Image Search**: Run a reverse image search. If the same photo appears in unrelated contexts (like an ad for hair loss treatment), something’s fishy.
2. **Activity and Interaction**:
	* **Social Wasteland**: Real profiles usually have interactions—likes, comments, shares. If it’s eerily quiet, raise an eyebrow.
	* **Offbeat Posts**: Look for posts that seem out of place or don’t match the user’s supposed interests.
3. **Friend Lists and Connections**:
	* **Bots vs. Humans**: Genuine accounts have connections that make sense—friends, family, colleagues. If it’s a random list of profiles that look like they were created by bots, beware.
4. **Language and Communication Style**:
	* **Misspellings and Generic Comments**: Poor grammar, misspelled words, or generic comments are red flags.
	* **Inconsistent Story**: If their communication style changes dramatically or they can’t keep their story straight, you might be dealing with a fake profile.

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

ANSWER:

**Objectives of the ICSE Database:**

1. **Victim Identification and Connection**:
	* The primary goal is to help victim identification specialists worldwide.
	* By analyzing and comparing child sexual abuse images, investigators can connect victims, abusers, and locations.
	* It facilitates collaboration among specialized investigators across borders.
2. **Efficiency and Time-Saving**:
	* The database prevents duplication of effort.
	* Investigators can quickly determine if a series of images has already been discovered or identified elsewhere.
	* It saves precious time by avoiding redundant work.

**Demographics and Impact:**

* **Coverage**: The ICSE database involves specialized investigators from more than 68 countries.
* **Data Repository**: It holds over 4.9 million images and videos related to child sexual exploitation.
* **Victim Identification**: To date, it has helped identify 41,900 victims worldwide.

**Alarming Trends Revealed by the ICSE Database:**

1. **Age of Victims**:
	* Very young children, including infants and toddlers, are victims of sexual abuse.
	* The younger the victim, the more severe the abuse.
2. **Content Severity**:
	* 84% of images contain explicit sexual activity.
	* Severe abuse images often feature boys.
3. **Gender Distribution**:
	* 65% of unidentified victims are girls.
	* 92% of visible offenders are male.

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.

ANSWER:

However, I can offer some general advice on identifying suspicious SMS or emails:

1. **Unsolicited Requests for Personal Information**:
	* Be cautious if you receive messages asking for sensitive data (e.g., passwords, credit card details) without a valid reason.
2. **Too Good to Be True Offers**:
	* If an email promises huge rewards, lottery winnings, or unexpected gifts, it’s likely a scam.
3. **Urgency and Threats**:
	* Scammers often create urgency (e.g., “Your account will be suspended!”) to pressure recipients.
	* Threats of legal action or consequences are red flags.
4. **Mismatched URLs or Email Addresses**:
	* Hover over links to check if they lead to legitimate websites.
	* Verify sender email addresses—look for misspellings or suspicious domains.
5. **Poor Grammar and Spelling**:
	* Many fraudulent messages contain errors.
	* Be wary of poorly written emails.

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

ANSWER:

**Guidelines for Children Accessing Public Systems:**

1. **Never Share Email and Password**:
	* Avoid telling anyone, including the cyber cafe owner, your email and password.
	* Information theft risks are real, even if you’re a child.
2. **Delete Personal Information After Use**:
	* If you store or download personal information on a public system (like a cyber cafe desktop), delete it after completing your work.
3. **Disable “Remember My ID” Option**:
	* When surfing the internet, ensure the browser’s “Remember my ID on this computer” option is disabled.
	* Use strong passwords.
4. **Check Browser Security Settings**:
	* Regularly review browser settings related to downloads, cookies, and password storage.
	* Consider using the browser’s Incognito Mode to avoid storing personal details in cookies.
5. **Beware of Keyloggers**:
	* Keyloggers record keystrokes, potentially exposing your username and password.
	* Check if there’s an intermediate device between your keyboard and CPU.
	* Use on-screen keyboards where possible.
6. **Ensure Updated Antivirus Software**:
	* Use systems with up-to-date antivirus and anti-spam software.
	* Insist that cyber cafe owners provide computers with updated protection.
7. **Don’t Leave Sensitive Information Unattended**:
	* Never leave a public computer unattended with sensitive information on the screen.
8. **Log Out Properly**:
	* Always log out from all applications and close the browser when leaving a cyber cafe.

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

ANSWER:

**CIS Google Android Benchmark Overview:**

1. **Objective**:
	* The benchmark aims to enhance the security of Android devices by providing prescriptive guidance for configuration settings.
2. **Scope**:
	* The benchmark covers Android 9.0.x and Android 10.0.x.
	* It applies to all hardware devices supporting these OS versions.
3. **Key Areas**:
	* **Privacy Settings**:
		+ **App Permissions**: Review and manage app permissions. Limit unnecessary access (e.g., location, contacts, camera).
		+ **Location Services**: Disable location services for apps that don’t require it.
		+ **Personal Data Sharing**: Minimize data sharing with third-party apps.
	* **Browser Configuration**:
		+ **Secure Browsing**: Use secure browsers (e.g., Chrome) with automatic updates.
		+ **Disable Autofill**: Prevent browsers from saving sensitive information.
		+ **Clear Browsing Data**: Regularly clear cookies, cache, and browsing history.
	* **Device Security**:
		+ **Screen Lock**: Set a strong PIN, pattern, or password.
		+ **Encryption**: Enable full-disk encryption.
		+ **Remote Wipe**: Configure remote wipe settings in case of device loss.
	* **Network Security**:
		+ **Wi-Fi Security**: Avoid public Wi-Fi networks. Use VPNs for secure connections.
		+ **Bluetooth**: Disable Bluetooth when not in use to prevent unauthorized pairing.
4. **Regular Updates**:
	* Keep the Android OS and apps up to date to patch security vulnerabilities.