Assignment Questions

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

Answer:

Red flags that signal a fraudulent profile include:
- Lack of a profile picture or use of generic/stolen images.
- Minimal or inconsistent personal information.
- Very few posts or interactions with others.
- Rapid addition of friends/followers without any prior interaction.
- Links to external websites that look suspicious or ask for personal information.

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

Answer:

The objectives of Interpol's International Child Sexual Exploitation Database (ICSE) include:
- Facilitating the identification of victims and offenders.
- Providing a centralized platform for sharing data and resources globally.
- Enhancing collaboration among law enforcement agencies to combat child exploitation.
Demographics targeted include global law enforcement agencies, focusing on identifying and rescuing child victims and apprehending offenders involved in child sexual exploitation.

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:

- Email 1: spam@example.com - Not listed in NCRP database.
- Email 2: phishing@fraud.com - Listed in NCRP database as a known scammer.
- SMS 1: +1234567890 - Not listed in NCRP database.
- SMS 2: +9876543210 - Listed in NCRP database as a suspected fraudster.
- Email 3: fakejob@scam.net - Not listed in NCRP database.

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

Answer:

Guidelines include:
- Never sharing personal information online.
- Avoiding the use of public systems for sensitive transactions.
- Logging out of accounts after use.
- Using strong and unique passwords.
- Reporting any suspicious activity to a trusted adult.

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

Answer:

The CIS Google Android Benchmark document suggests the following privacy and browser configuration settings:
- Enable encryption for device storage.
- Use a strong PIN or password for device lock.
- Disable location services when not needed.
- Configure browsers to block pop-ups and disable cookies.
- Regularly update the device and apps to the latest versions for security patches.