Assignment – 14

Gumma V L Prasad
(H.T.No: 2406CYS107)

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

Answer:- Identifying Red Flags of a Fraudulent Social Media Profile: A Case Study

Platform: Instagram

Target Profile: @luxury_life_guru

Analysis:

Here's a breakdown of red flags that suggest @luxury_life_guru might be fraudulent:

1. Inconsistent Profile Information:

- **Username:** Generic usernames with underscores or excessive numbers often indicate fake accounts.
- **Bio:** An excessively vague bio with no details about the person's background or interests raises suspicion.
- **Location:** If the location is inconsistent with the profile's theme or frequently changes, it could be a sign of inauthenticity.

2. Unrealistic Photos and Videos:

- **Highly edited or stock photos:** Extremely filtered or photos that look too perfect to be real can be red flags.
- **Inconsistent photo quality:** A mix of high-quality professional shots and blurry phone pictures might indicate stolen content.
- **Photos lacking context:** Images with no clear location or surrounding details can be suspicious.
- **Excessive use of luxury brands or staged wealth displays:** Profiles boasting excessive wealth with no explanation of income source might be attempting to scam viewers.

3. Follower Discrepancy:

- **High follower count with low engagement:** A large number of followers with minimal likes, comments, or shares suggests purchased followers.
- **Suspicious follower list:** A follower list filled with inactive accounts or profiles from another region entirely can be a sign of inauthenticity.

4. Content & Posting Habits:

- **Frequent posts promoting unrealistic get-rich-quick schemes or miracle products.**
- **Generic captions with excessive use of emojis or hashtags unrelated to the content.**
- **Sudden shift in content style or themes.**
- **Constant messaging or following requests soon after connecting.**

5. Direct Messages:

- **Immediate requests for personal information or money.**
- **Offers of "exclusive" deals or access that seem too good to be true.**
- **Pressuring you to click on suspicious links.**

Remember: Not all profiles with a few of these red flags are fraudulent. However, if you notice several of these indicators, it's best to proceed with caution and avoid engaging with the account.

Professionalism in Social Media Interactions:

By being aware of these red flags, you can protect yourself from potential scams and cultivate a more secure and authentic social media experience.

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

Answer:- Interpol's International Child Sexual Exploitation (ICSE) Database is a crucial tool in combating child sexual exploitation and abuse on a global scale. Here are the main objectives and demographic details associated with the ICSE Database:

Objectives

1. Identification of Victims:

- Primary Goal: To identify victims of child sexual exploitation and abuse.

- Method: Using advanced image and video analysis technology to recognize and locate victims.

2. Identification and Prosecution of Offenders:

- Support for Law Enforcement: Provide law enforcement agencies worldwide with the tools and data needed to identify and apprehend perpetrators.

- Evidence Sharing: Facilitate the sharing of evidence and intelligence among international law enforcement bodies.

3. Global Cooperation:

- International Collaboration: Promote cooperation and coordination among member countries to tackle cross-border child exploitation cases.

- Resource Sharing: Provide a platform for sharing best practices, strategies, and resources.

4. Reduction of Duplication Efforts:

- Efficiency: Minimize redundant investigations by allowing agencies to check if images or videos are already in the database, thus saving time and resources.

5. Support for Ongoing Investigations:

- Real-time Access: Provide law enforcement with real-time access to the database to support ongoing investigations.

- Technical Assistance: Offer technical assistance and expertise to agencies using the database.

6. Training and Capacity Building:

- Education: Train law enforcement officials on the use of the database and the latest techniques in identifying and rescuing victims.

- Capacity Building: Strengthen the capabilities of national law enforcement agencies in handling child exploitation cases.

Demographics

1. Geographic Reach:

- Global Participation: The database is used by law enforcement agencies in over 60 countries, making it a truly global initiative.

2. User Base:

- Law Enforcement Agencies: Primarily used by national police forces, cybercrime units, and other relevant law enforcement bodies.

- Interpol Specialists: Managed and supported by a dedicated team of Interpol specialists.

3. Age and Gender of Victims:

- Wide Age Range: Victims can be of any age, but the database often focuses on identifying minors (under 18 years old).

- Gender Distribution: Victims can be of any gender, though statistics and cases often show a higher prevalence of female victims.

4. Types of Cases:

- Variety of Exploitation Forms: Cases can involve a wide range of exploitative actions, including the production, distribution, and possession of child sexual abuse material.

- Case Severity: The database includes cases ranging from single incidents to large-scale organized crime operations.

By maintaining and expanding the ICSE Database, Interpol aims to create a safer world for children and to bring offenders to justice through enhanced international cooperation and resource sharing.

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

Answer:- Here are the guidelines for children while accessing public systems as per general information security awareness practices, including those typically covered by ISEA:

1. Never Share Personal Information:

- Do not share your personal details such as name, address, phone number, or school name with anyone online.

2. Keep Passwords Confidential:

- Do not share your passwords with anyone, including friends or cyber café owners.

- Use strong and unique passwords for different accounts.

3. Log Out After Use:

- Always log out of your accounts when you finish using a public computer.

- Close all browser windows and clear the cache to prevent others from accessing your information.

4. Avoid Financial Transactions:

- Refrain from conducting any financial transactions, such as online banking or shopping, on public computers.

5. Be Wary of Public Wi-Fi:

- Avoid using public Wi-Fi for accessing sensitive information. If necessary, use a VPN to secure your connection.

6. Do Not Download or Install Software:

- Do not download or install any software on public systems as it might contain malware.

7. Check for Security Features:

- Ensure the public system has up-to-date antivirus software and other security measures in place.

8. Monitor for Suspicious Activity:

- Be alert to any unusual activity on the system or your accounts. Report any suspicious behavior immediately.

9. Use Two-Factor Authentication:

- Enable two-factor authentication for your accounts for an added layer of security.

10. Avoid Accessing Sensitive Information:

- Try to avoid accessing personal or sensitive information on public computers. If necessary, limit the amount of sensitive data you enter.

11. Stay Informed and Updated:

- Keep yourself updated on the latest cybersecurity threats and safety tips.

These guidelines help ensure children can use public systems safely and minimize the risk of their personal information being compromised. For more detailed guidelines, please visit the ISEA portal directly when accessible.

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 provides a set of recommendations for configuring Android devices to enhance security and privacy. Here's a summary of the key points related to privacy and browser settings:

Privacy Settings:

- **Lock Screen:** The benchmark suggests disabling notifications on the lock screen to prevent sensitive information from being displayed without unlocking the device.
- **App Permissions:** It emphasizes reviewing and adjusting app permissions to minimize data access by applications. This might involve denying unnecessary permissions like location tracking for apps that don't genuinely require it.
- **Advertising ID:** Disabling the Advertising ID is recommended, which helps limit personalized advertising based on user data.
- **Location Services:** The benchmark suggests enabling location services only for trusted apps and disabling location history to minimize location data collection.
- **Biometric Authentication:** Enabling strong biometric authentication (fingerprint, PIN, etc.) for screen lock is recommended for improved security.

Browser Settings:

- **Pop-ups & Redirects:** Blocking pop-ups and redirects helps prevent users from being lured to malicious websites.
- **JavaScript:** Disabling JavaScript may be recommended in some cases, but it can also break certain website functionalities.
- **Cookies:** The benchmark might suggest managing cookies, like blocking third-party cookies, to limit data collection by advertising networks and other trackers.
- **Incognito/Private Browsing:** Enabling incognito mode for browsing sessions where privacy is a major concern is recommended.

Important Note:

- The specific recommendations in the CIS Google Android Benchmark may vary depending on the Android version. It's crucial to consult the latest version of the document for the most accurate information for your device's Android version.
- You can find the latest CIS Google Android Benchmark here: https://www.cisecurity.org/benchmark/google_android