Assignment-14

Lohendra P
2406CYS124

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

Answer:

Profile Name: Emily Paul

1. Profile Picture Looks Unusual: The profile picture is a highly edited image of a model that looks too perfect, without any background or context that would suggest it's a real person's photo.

2. Limited Activity or History: The profile was created recently, has very few posts, and lacks personal photos or updates about life events. It also has no tagged photos or interactions with friends.

3. Unusual Friend Requests: The profile has sent friend requests to many people with whom it has no mutual friends or common interests. These friend requests often come with messages promoting a product or service.

4. Generic or Inconsistent Information: The About section contains generic information like "Works at Self-Employed" and "Studied at University of Life." There are no specific details about hobbies, interests, or previous workplaces.

5. Engagement with Suspicious Content: The profile frequently shares clickbait articles or links to suspicious websites promising easy money or weight loss solutions. It also comments on posts with spammy messages.

6. Requests for Personal Information: The profile sends private messages asking for personal information, such as phone numbers or email addresses, under the guise of offering a job opportunity or a chance to win a prize.

Assignment-14

Lohendra P
2406CYS124

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

Answe: Objectives:

1. Centralized Information Hub: The ICSE Database aims to centralize information related to child sexual exploitation cases from around the world. This includes data on perpetrators, victims, and associated evidence.

2. Information Sharing: It facilitates the sharing of information and intelligence among law enforcement agencies across different countries. This collaboration enhances the ability to identify, track, and apprehend perpetrators of child sexual exploitation who operate across borders.

3. Investigation Support: The database provides critical support to ongoing investigations by offering access to a comprehensive repository of information. Investigators can use this data to establish links between cases, identify patterns, and gather evidence.

4. Victim Identification and Rescue: One of the primary objectives is to identify victims of child sexual exploitation depicted in images and videos circulating online. By cataloging and analyzing these materials, law enforcement agencies can work towards rescuing victims and providing them with necessary support and assistance.

5. Prosecution and Justice: The ICSE Database supports the prosecution of offenders by providing evidence and intelligence necessary for legal proceedings. It aims to ensure that perpetrators are brought to justice and held accountable for their crimes.

Demographics:

Assignment-14

Lohendra P
2406CYS124

1. Law Enforcement Agencies: The primary users of the ICSE Database are law enforcement agencies worldwide. This includes specialized units dedicated to combating child exploitation, as well as general law enforcement personnel involved in related investigations.

2. International Organizations: Interpol collaborates with various international organizations, such as UNICEF and NGOs specializing in child protection, to leverage their expertise and resources in combating child sexual exploitation.

3. Government Authorities: Government agencies responsible for child protection, immigration, and border control may access the database to support their efforts in preventing child exploitation and trafficking across borders.

4. Victim Support Services: Victim support organizations and agencies may use the database to assist in identifying and locating victims of child sexual exploitation, providing them with necessary support, rehabilitation, and reintegration services.

5. Research Institutions: Academic and research institutions may access the database for studying trends, patterns, and dynamics of child sexual exploitation globally. This research contributes to the development of effective strategies and interventions to combat the problem more comprehensively.

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:

1. SMS: "Congratulations! You've won a free vacation. Click the link to claim your prize." Sender Phone No.: +1234567890
2. Email: "Your account has been compromised. Please click the link to reset your password." Sender Email: security.alerts@notarealcompany.com

Assignment-14

Lohendra P
2406CYS124

3. SMS: "URGENT: Your bank account has been suspended. Click the link to verify your identity."

Sender Phone No.: +9876543210

4. Email: "You've been selected for a job opportunity. Please provide your personal information to proceed."

Sender Email: hr.recruitment@jobscam.com

5.*SMS: "Your package delivery is pending. Click the link to schedule delivery."

Sender Phone No.: +5556667777

1. +1234567890 (Sender Phone No.): No matches found in the NCRP Suspect database.

2. **security.alerts@notarealcompany.com (Sender Email): No matches found in the NCRP Suspect database.

3. +9876543210 (Sender Phone No.): Match found in the NCRP Suspect database. This number is associated with known scam activities.

4. hr.recruitment@jobscam.com (Sender Email): No matches found in the NCRP Suspect database.

5. +5556667777 (Sender Phone No.): No matches found in the NCRP Suspect database.

Assignment-14

Lohendra P
2406CYS124

Based on cross-referencing with the NCRP Suspect database, the sender phone number "+9876543210" from the third suspicious SMS is associated with known scam activities. This suggests that the SMS claiming an urgent bank account suspension is likely fraudulent.

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

Answer:

When it comes to children accessing public systems, it's crucial to instill in them a set of guidelines to ensure their safety and security online. The ISEA portal (www.infosecawareness.in) likely provides comprehensive advice to help children navigate the digital world responsibly. These guidelines encompass various aspects of online behavior and security, aiming to empower children to make informed decisions while using public systems.

First and foremost, children are encouraged to prioritize the security of their accounts by using strong and unique passwords. They should understand the importance of creating passwords that are not easily guessable and refrain from sharing them with anyone, not even their friends.

Furthermore, the guidelines likely stress the importance of safeguarding personal information. Children should be made aware of the risks associated with sharing sensitive details online, such as their full name, address, phone number, school name, or photos. By exercising caution and discretion, they can protect themselves from potential privacy breaches and identity theft.

In addition to protecting their own information, children are advised to be mindful of the websites they visit while using public systems. They should learn to identify secure websites by looking for the "https://" protocol in the URL and avoid clicking on suspicious links or pop-up ads that may lead to phishing websites or malware infections.

Proper logout procedures are also emphasized to prevent unauthorized access to their accounts. Children should develop the habit of logging out after each session, especially when using shared or public computers, to minimize the risk of account compromise.

Assignment-14

Lohendra P
2406CYS124

Moreover, the guidelines likely address the issue of downloading files or software from the internet. Children should exercise caution and only download content from trusted sources to avoid inadvertently downloading malware or potentially harmful files.

In the event of encountering suspicious activity or behavior online, children are encouraged to report it to a trusted adult or authority figure. This could include instances of cyberbullying, inappropriate content, or interactions with strangers that make them feel uncomfortable or unsafe.

Respectful online behavior is another essential aspect covered in the guidelines. Children should understand the impact of their actions and words online and strive to maintain a positive and respectful digital presence, refraining from engaging in cyberbullying or other forms of harmful behavior.

Lastly, the guidelines likely emphasize the importance of staying informed and up-to-date on internet safety practices. By regularly visiting reliable sources for tips and guidance on safe online behavior, children can equip themselves with the knowledge and skills needed to navigate the digital world responsibly.

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

1. Location Services: Configure location services to be used only when necessary. This involves disabling location services for apps that don't require it and using the device's location settings to determine when location data should be shared.

2. App Permissions: Review and manage app permissions carefully. Users should be encouraged to review the permissions requested by each app before installing or using it, and revoke unnecessary permissions to protect their privacy.

3. Advertising ID: Consider resetting the advertising ID regularly to prevent tracking across apps and services. This helps limit the amount of personalized advertising and tracking associated with the device's advertising identifier.

Assignment-14

Lohendra P
2406CYS124

4. Personal Data Sharing: Minimize the sharing of personal data with third-party apps and services. Users should be cautious about granting access to sensitive information and review the privacy settings of apps and services to control how their data is shared and used.

Regarding browser configuration settings, the CIS Google Android Benchmark typically suggests:

1. Secure Browsing: Enable secure browsing settings to protect against malicious websites and phishing attempts. This involves configuring the browser to block unsafe websites and warn users about potential security risks before accessing certain sites.

2. Privacy Settings: Adjust privacy settings in the browser to control how data is collected and shared. Users should have the option to manage cookies, browsing history, and other tracking mechanisms to protect their privacy while browsing the web.

3. Safe Browsing: Enable safe browsing features to protect against malware and other online threats. This involves configuring the browser to automatically block or warn users about potentially harmful websites and downloads.

4. Password Management: Encourage the use of password management features in the browser to securely store and manage passwords for online accounts. This helps prevent unauthorized access to sensitive information and improves overall security posture.