SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 14

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

Ans:

Imagine a fake profile on a social media platform like Facebook:

Profile Picture: The profile picture might look too perfect or like a stock photo, lacking any personalization.

Limited Content: There's a lack of personal posts, photos, or updates over time, suggesting the profile was recently created.

Friend Count: The profile might have an unusually high number of friends or followers, often acquired through fake accounts.

Unrealistic Bio: The bio may contain generic phrases or information that seems too good to be true.

Activity Patterns: The profile might engage in suspicious behavior like sending friend requests to many people at once or liking/commenting on numerous posts rapidly.

Inconsistencies: Details in the profile may not add up, such as location not matching with stated job or education history.

Links to Suspicious Sites: The profile might share links to phishing websites or other malicious content.

No Personal Interaction: When messaged, the user may respond with generic, automated replies or avoid direct questions.

Stolen Content: The profile might share images or posts stolen from other users or websites.

Asking for Personal Information: The user might try to solicit personal information or financial details through private messages.

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

Ans:

The objectives and demographics of Interpol's International Child Sexual Exploitation Database (ICSE) are as follows:

Objectives:

Combat Child Sexual Exploitation: The primary goal of ICSE is to combat the sexual exploitation of children globally by facilitating the exchange of information, intelligence, and expertise among member countries.

Data Centralization: ICSE aims to centralize data related to child sexual exploitation cases, including images and videos, to enhance law enforcement's ability to investigate and prosecute offenders.

Identification of Victims: By cataloging and sharing images and videos of child sexual abuse, ICSE helps law enforcement agencies identify victims and rescue them from abusive situations.

Investigation Support: The database provides crucial support to law enforcement investigations by assisting in the identification of perpetrators, victims, and patterns of abuse.

International Cooperation: ICSE fosters international cooperation among law enforcement agencies, enabling them to collaborate across borders to combat child sexual exploitation effectively.

Demographics:

Law Enforcement Agencies: ICSE primarily serves law enforcement agencies worldwide, including police departments, investigative bodies, and other relevant authorities involved in combating child sexual exploitation.

Victims: While not directly accessing the database, victims of child sexual exploitation benefit indirectly through the identification and apprehension of offenders, leading to their rescue and protection.

Offenders: The database targets offenders involved in the production, distribution, and consumption of child sexual abuse material, aiming to identify and bring them to justice.

International Organizations: International organizations, NGOs, and other entities involved in combating child exploitation may also have access to ICSE data or collaborate with Interpol in its efforts.

3Q) 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.

Ans:

Here are five examples of suspicious messages:

SMS: "Congratulations! You've won a free vacation. Click the link to claim your prize."

Sender: +123456789

Findings: The sender's phone number is not found in the NCRP Suspect database.

Email: "URGENT: Your account has been compromised. Click the link to secure your account."

Sender: security.alerts@example.com

Findings: The email address is not found in the NCRP Suspect database.

SMS: "Your bank account has been locked. Please provide your login details to unlock."

Sender: 9876543210

Findings: The sender's phone number is associated with a known phishing scam in the NCRP Suspect database.

Email: "You've won a lottery! To claim your prize, reply with your personal information."

Sender: lotteryclaims@winners.com

Findings: The email address is flagged as suspicious in the NCRP Suspect database due to previous reports of lottery scams.

SMS: "Your package delivery failed. Click the link to reschedule delivery."

Sender: +4433221100

Findings: The sender's phone number is not found in the NCRP Suspect database.

These examples demonstrate common tactics used in phishing, scam, and fraud attempts. While the specific sender information may not be real, they illustrate the importance of verifying the legitimacy of messages and cross-referencing sender information against databases like the NCRP Suspect database when possible to avoid falling victim to scams

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

Ans:

some guidelines children should follow when accessing public systems:

Use Secure Passwords: Encourage children to use strong, unique passwords for their accounts and avoid sharing them with anyone.

Be Wary of Strangers: Teach children to be cautious when interacting with strangers online, including not sharing personal information or meeting them in person.

Avoid Suspicious Links: Instruct children to avoid clicking on links or downloading attachments from unknown or suspicious sources to prevent malware infections.

Privacy Settings: Ensure children understand how to adjust privacy settings on social media and other online accounts to limit who can see their information and posts.

Report Concerns: Teach children to report any inappropriate or concerning behavior they encounter online to a trusted adult or authority figure.

Browsing Safety: Encourage safe browsing habits, such as avoiding websites with adult content and being cautious when downloading or installing software.

Cyberbullying Awareness: Educate children about the risks of cyberbullying and encourage them to speak up if they or someone they know are being bullied online.

Parental Supervision: Monitor children's online activities and set appropriate limits on screen time to ensure their safety and well-being.

These guidelines promote responsible and safe internet usage for children, helping to protect them from potential online threats and dangers.

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

Ans:

A general overview of common privacy and browser configuration settings that are often recommended for Android devices:

Privacy Settings:

Limit App Permissions: Review and adjust app permissions to restrict access to sensitive data like location, contacts, and camera/microphone.

Location Services: Enable location services only when necessary and disable for apps that don't require it.

Personalization: Disable personalized ads and limit ad tracking in device settings.

Biometric Data: Secure biometric data (fingerprint, face recognition) with strong authentication methods.

Data Encryption: Enable device encryption to protect data stored on the device.

App Installations: Allow installations only from trusted sources (Google Play Store) and disable installation of apps from unknown sources.

Browser Configuration Settings:

Clear Browsing Data: Regularly clear browsing history, cookies, and cached data to maintain privacy.

Disable Autofill: Turn off autofill features to prevent the browser from storing sensitive information such as passwords and credit card details.

Safe Browsing: Enable safe browsing features to protect against phishing sites, malware, and harmful downloads.

Disable JavaScript: Consider disabling JavaScript in the browser settings to enhance security and prevent certain types of attacks.

Private Browsing Mode: Use the browser's private or incognito mode for sensitive browsing sessions to prevent the storage of browsing history and cookies.

Browser Extensions: Be cautious when installing browser extensions and only install those from trusted sources to avoid potential security risks.