CYBER SECURITY

ASSIGNMENT -14

NAME:B.Shanmukh

Reg.no: 282023-024

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

Ans:

Let's create a fake profile on a popular social media platform like Facebook. Here are some red flags that could signal its fraudulent nature:

1. **Profile Picture**: The profile picture is often a stock photo or a picture of a celebrity, rather than a real person. It might look too professional or staged.
2. **Limited Content**: The profile has very few posts, photos, or interactions despite claiming to be active for a while. This indicates it was created recently or is not maintained regularly.
3. **Incomplete Profile Information**: The profile may lack detailed information about the person, such as hometown, education, job, etc. Fraudulent profiles often skip these details to avoid scrutiny.
4. **Friend List**: The friend list consists mostly of unknown or suspicious accounts. If the profile has thousands of friends but very few interactions or mutual friends, it's a red flag.
5. **Unusual Activity**: The profile engages in unusual activity such as sending friend requests or messages to random people, posting spammy links, or joining dubious groups.
6. **Inconsistent Information**: Details provided in the profile (such as age, location, education, job) may not align with each other or seem too good to be true.
7. **Requests for Personal Information**: The profile may try to solicit personal information from others or send unsolicited messages with suspicious links.
8. **Poor Language Skills**: Scammers often have poor grammar and spelling in their messages due to being non-native English speakers or using automated translation tools.
9. **Lack of Interaction**: The profile does not respond to messages or comments, or its responses seem automated and generic.
10. **Reported or Blocked Accounts**: If the profile has been reported multiple times or has a history of being blocked by other users, it's a clear indication of fraudulent behavior.

These red flags can help users identify and avoid fraudulent profiles on social media platforms.

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

ANS:

Interpol's International Child Sexual Exploitation Database (ICSE Database) serves several key objectives aimed at combating child sexual exploitation and protecting vulnerable children globally. Here's an outline of its objectives and demographics:

1. **Objective 1: Centralized Information Repository**: The primary objective of the ICSE Database is to serve as a centralized repository for information related to child sexual exploitation cases. It collects and stores data on offenders, victims, and related incidents from Interpol member countries.

2. **Objective 2: Facilitating Law Enforcement Cooperation**: The database facilitates international law enforcement cooperation by providing member countries with access to critical information and intelligence on child sexual exploitation cases. This enables collaborative efforts to identify, track, and apprehend offenders operating across borders.

3. **Objective 3: Supporting Investigations and Prosecutions**: By providing law enforcement agencies with access to comprehensive data on offenders and victims, the database supports investigations and prosecutions related to child sexual exploitation. It helps build stronger cases against perpetrators and ensures justice for victims.

4. **Objective 4: Enhancing Victim Identification and Protection**: The ICSE Database plays a crucial role in victim identification and protection efforts. It contains information that can help identify and locate victims of child sexual exploitation, enabling authorities to rescue and provide them with necessary support and protection services.

5. **Objective 5: Preventing Recurrence and Disruption**: Through the analysis of data and trends stored in the database, law enforcement agencies can identify patterns of criminal behavior, modus operandi of offenders, and emerging threats. This information can be used to develop preventive measures, disrupt criminal networks, and prevent the recurrence of child sexual exploitation incidents.

Demographics:

- **Victims**: The database contains information on child victims of sexual exploitation, including their demographic details such as age, gender, nationality, and circumstances of exploitation.
- **Offenders**: It also stores data on individuals involved in the sexual exploitation of children, including their identities, criminal histories, methods of operation, and known associations.
- **Incidents**: Information related to specific incidents of child sexual exploitation, including locations, dates, and details of the offenses, is recorded in the database.

- **Geographical Coverage**: The ICSE Database covers a wide range of geographical regions, with participation from Interpol's member countries across the globe, reflecting the global nature of child sexual exploitation and the need for international cooperation to address it effectively.

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.

ANS:

I can provide some of suspicious messages or emails i have received and suggest steps you can take to verify their legitimacy:

1. **"You've won a lottery you didn't enter!":** Be cautious of unsolicited messages claiming you've won a lottery, especially if you haven't entered any. These are often phishing attempts to trick you into providing personal information or paying fees to claim your "prize."

2. **"Your account has been compromised, click here to reset your password":** Watch out for emails or texts that claim your account has been hacked or compromised. Instead of clicking on any links provided, independently verify the legitimacy of the message by contacting the company or organization directly through their official website or customer support channels.

3. **"Urgent message from your bank - Verify your account details":** Fraudulent messages posing as your bank or financial institution may request sensitive information like your account number, PIN, or password. Always double-check the sender's email address or phone number and contact your bank directly using their official contact information to confirm if the message is genuine.

4. **"Free trial subscription - Enter your credit card details to claim":** Be wary of unsolicited offers for free trials, especially if they require you to enter your credit card information. These could be attempts to sign you up for unwanted subscriptions or steal your financial information.

5. **"Job offer with high pay, no experience required":** Emails or texts promising high-paying jobs with minimal qualifications or experience should raise suspicion. Research the company offering the job, verify their legitimacy, and be cautious of any requests for upfront payments or personal information.

If you receive any suspicious messages or emails, you can report them to relevant authorities, such as the National Cyber Security Centre (NCSC) in your country, or forward them to organizations like the Anti-Phishing Working Group (APWG) for further investigation. Always prioritize your online safety and verify the legitimacy of any unsolicited communications before taking any action.

There are many other such type of messages or emails such as :

1. **”An email from your boss asks for the name, addresses, and credit card information of the company’s top clients. The email says it’s urgent and to please reply right away. You should reply right away.”**

2. **"You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website."**

3. **"If you get an email that looks like it's from someone you didn't know, if you click on any link your system may get hacked or virused."**

   These are some of the phising attacks going on in daily life.

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

ANS:
The guidelines to be followed by children while accessing public systems, as per ISEA portal (www.infosecawareness.in) are:

Accessing computers in public places, when necessary has its own risks which every user should be aware of to take necessary precautions.

Guidelines to be followed while accessing public systems :

- Never pass or tell the Cyber Cafe Owner or anyone else about your email and password to check your e-mail.
- ***Fact*** **:** *surveys say that small kids or many old aged persons have no idea about the risks of information theft.*
- If you store or download any personal information on Desktop in cyber cafe make sure you delete all the documents after you complete your work. Disable the option "Remember my ID on the computer" and use Strong Password.
- When surfing the Internet, you should always check the browser security like default download folder, cookies and password save locations etc., to avoid risks of exposing personal information. As a precaution use Incognito Mode of the browser to avoid storing your personal details in the cookies.
- A keylogger is basically spyware, it logs or records your keystrokes so that your username and password are made available to Cyber cafe owner or any Attacker. The records you enter maybe typed directly into Hacker's machine or collected afterwards through a file transfer.Always check if there is an intermediate device between your keyboard and CPU. Where ever possible, prefer using on screen keyboards.
- Ensure that that the system you are using has most up-to-date Anti Virus and Anti spam software. These may help to stop some of the key loggers, Trojans and other malware. You can insist cyber cafe Owner to allocate you a computer loaded with updated antivirus software.
- Do not leave the computer unattended with sensitive information on the screen. Remember to check Downloads folder for automatically saved files.
- Do not enter sensitive information into a public computer.
- Look for camera facing your keyboard to monitor your key strokes. There can be hidden cameras also for such shoulder surfing. Be cautious.
- Finally, Always make sure to logout from all the applications you are using and close the browser properly when you leave Cyber cafe.

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

ANS:

The CIS (Center for Internet Security) Google Android Benchmark provides comprehensive guidelines for securing Android devices. Here's a brief overview of the privacy and browser configuration settings suggested in the benchmark:

Privacy Settings:

1. **Location Services**: Disable location services when not needed or restrict access to specific apps. This helps prevent apps from tracking your location without your consent.
2. **App Permissions**: Review and manage app permissions regularly. Only grant permissions that are necessary for the app's functionality and revoke unnecessary permissions from apps that don't need them.
3. **Security Updates**: Ensure that your device receives regular security updates from the manufacturer. Keeping your device updated helps patch known vulnerabilities and enhances overall security.
4. **Screen Lock**: Enable a strong screen lock method such as a PIN, pattern, or biometric authentication (e.g., fingerprint or face recognition) to prevent unauthorized access to your device.
5. **Device Encryption**: Encrypt your device's storage to protect sensitive data stored on the device in case it's lost or stolen. Most modern Android devices offer built-in encryption options.

Browser Configuration Settings:

1. **Secure Connection**: Configure your browser to use secure HTTPS connections whenever possible, especially when accessing sensitive websites or entering personal information.
2. **Privacy Settings**: Adjust privacy settings in your browser to control cookies, site data, and other tracking mechanisms. You can choose to block third-party cookies, clear browsing history, and disable tracking features.
3. **Safe Browsing**: Enable safe browsing features in your browser to protect against phishing websites, malware, and harmful downloads. Most modern browsers offer built-in safe browsing protection.
4. **Auto-Fill and Password Management**: Use caution when enabling auto-fill and password management features in your browser. While convenient, these features can pose security risks if your device falls into the wrong hands.
5. **Browser Extensions**: Be selective about installing browser extensions and only choose those from trusted sources. Some browser extensions may compromise your privacy or security by tracking your browsing activity or injecting malicious code.

- These are just a few of the privacy and browser configuration settings recommended by the CIS Google Android Benchmark. It's essential to review the full benchmark document for detailed guidance on securing your Android device and protecting your privacy while browsing the web.