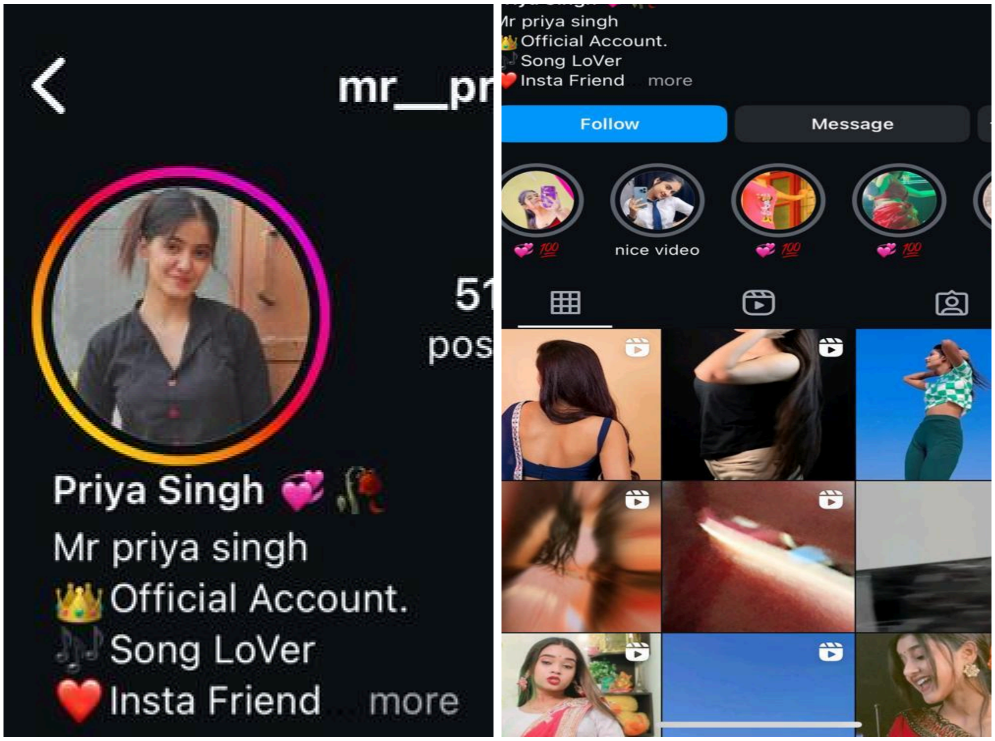
## 1.Choose a fake profile on any social media platform of your preference and identify the red flags signaling its fraudulent nature.

Identifying fake social media accounts has become a significant challenge nowadays. Depending on certain indicators, we can make informed decisions about whether an account is likely fake or genuine.
Impersonation is a common issue on social media platforms, where individuals create pages pretending to be celebrities, politicians, or sports figures. These accounts often use the names and profile pictures of the actual individuals, and may even repost their photos, reels, or videos to appear legitimate.

**Profile Picture and Photos**: Some profiles have different profile pictures and posts with photos of different individuals, that makes it not a generic profile. This will help in identifying the profile and by looking at the description below the picture.



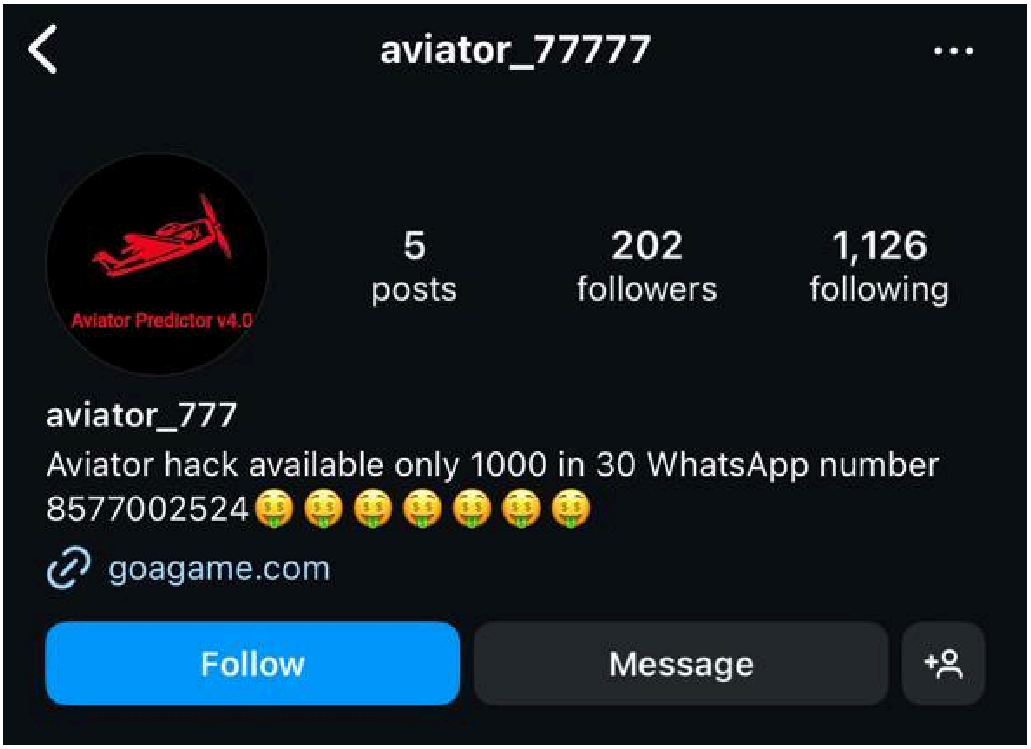
mr__pr

Priya Singh 💞🥀
Mr priya singh
👑Official Account.
🎶Song LoVer
❤️Insta Friend ... more

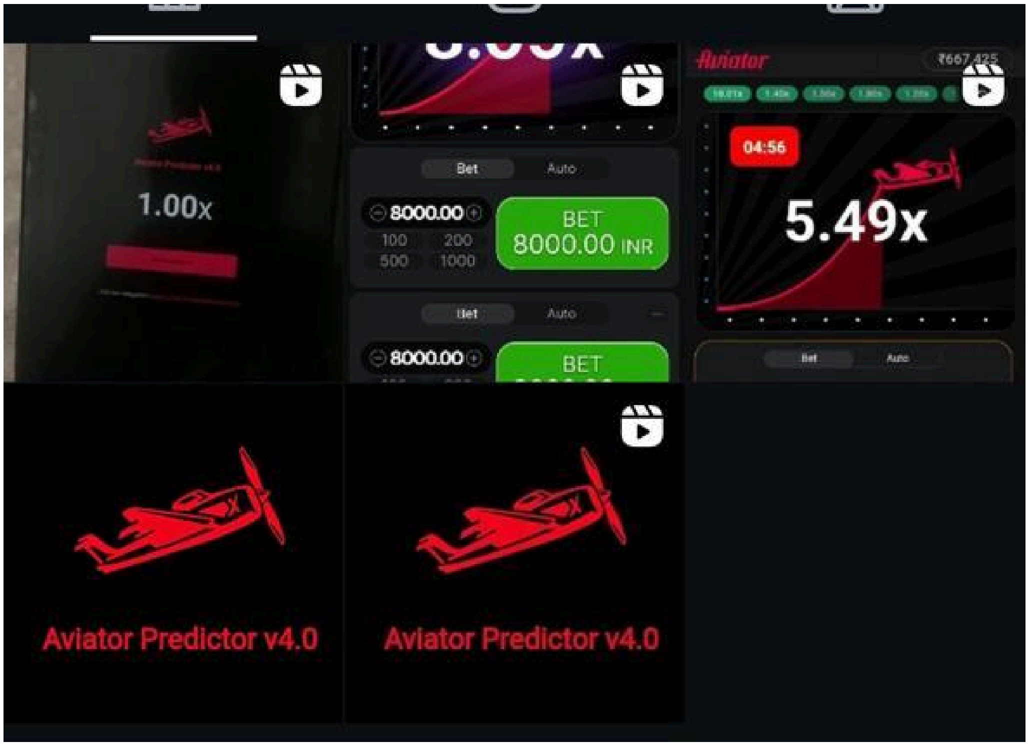
r priya singh
👑Official Account.
🎶Song LoVer
❤️Insta Friend ... more

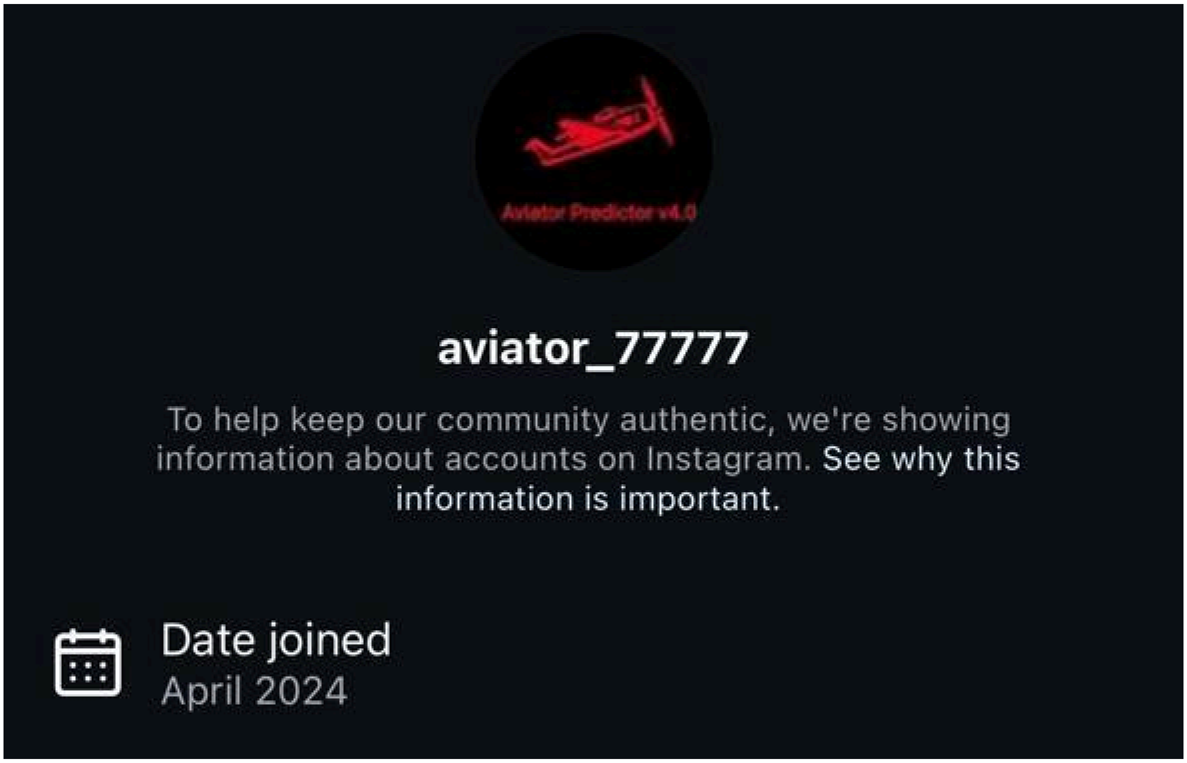
**Information and Details:** Some profile names which are used of a company names or celebrities names and posts are used for betting ads or other information. The below profile is created in the name of a brand "AVIATOR" which is a bettting or a trading app, They have impersonated the apps name and making it be their homepage to predict the price and speculate the trading.

Making people download the app and use it so that they can get the reference bonus. In the profile information he added the mobile number which can be seen as a fake profile. The date of creating the profile and the organization beginning date is not so similar.



aviator_777
Aviator hack available only 1000 in 30 WhatsApp number 8577002524🤑🤑🤑🤑🤑🤑🤑
goagame.com





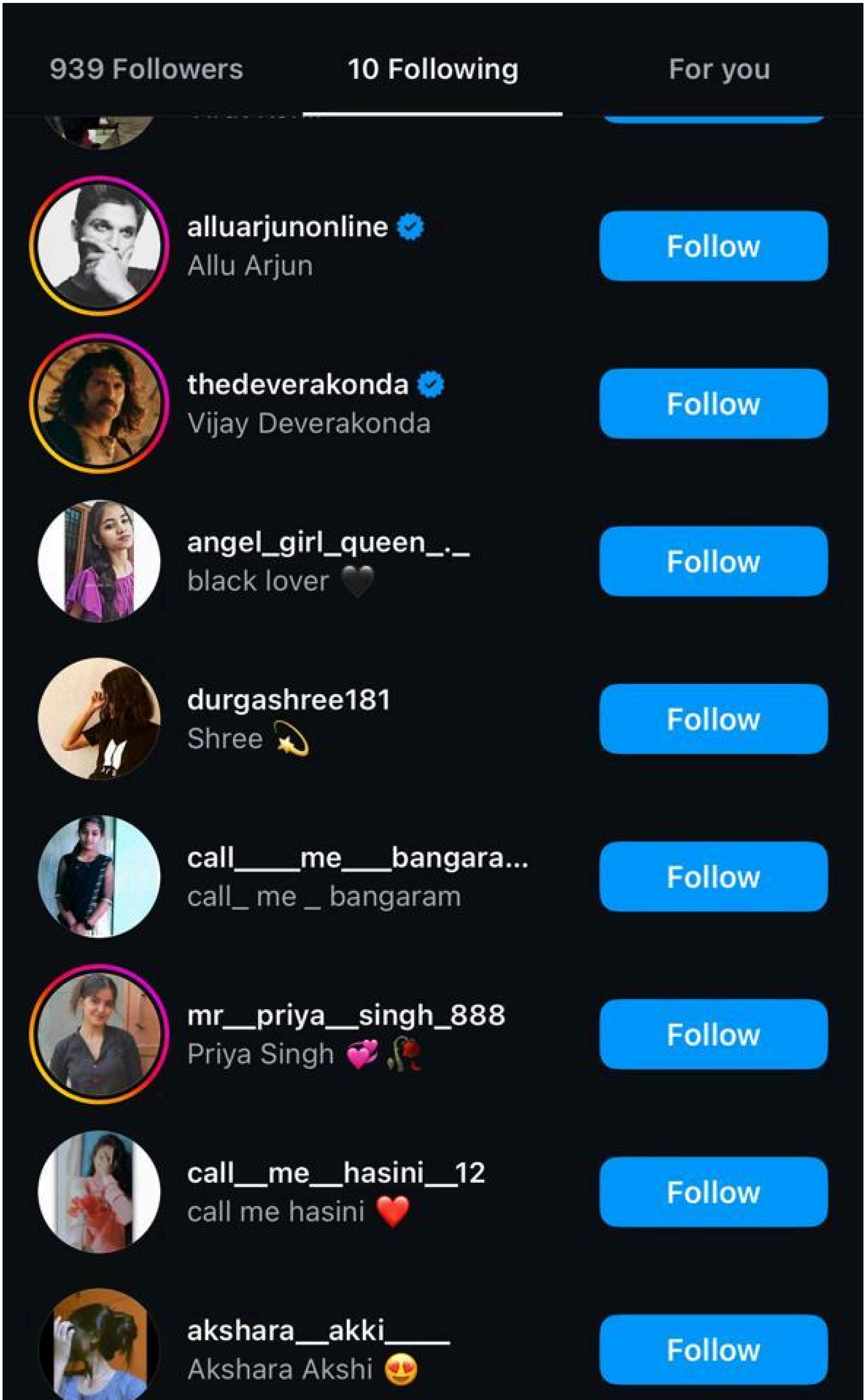
**aviator_77777**

To help keep our community authentic, we're showing information about accounts on Instagram. See why this information is important.

Date joined
April 2024

**Friend or Follower Count**: One of the important thing to check their followers and following profiles. Whom they are following and who are liking their posts commenting tagging all these will show the legitimacy of the account.

How they are posting the reels posts, when they are posting. **Bulk posting is the most significant is found in fake profile.** Posting many Posts in same day , irrespective of the location or the dress in the image.



939 Followers | 10 Following | For you

alluarjunonline
Allu Arjun
Follow

thedeverakonda
Vijay Deverakonda
Follow

angel_girl_queen_._
black lover 🖤
Follow

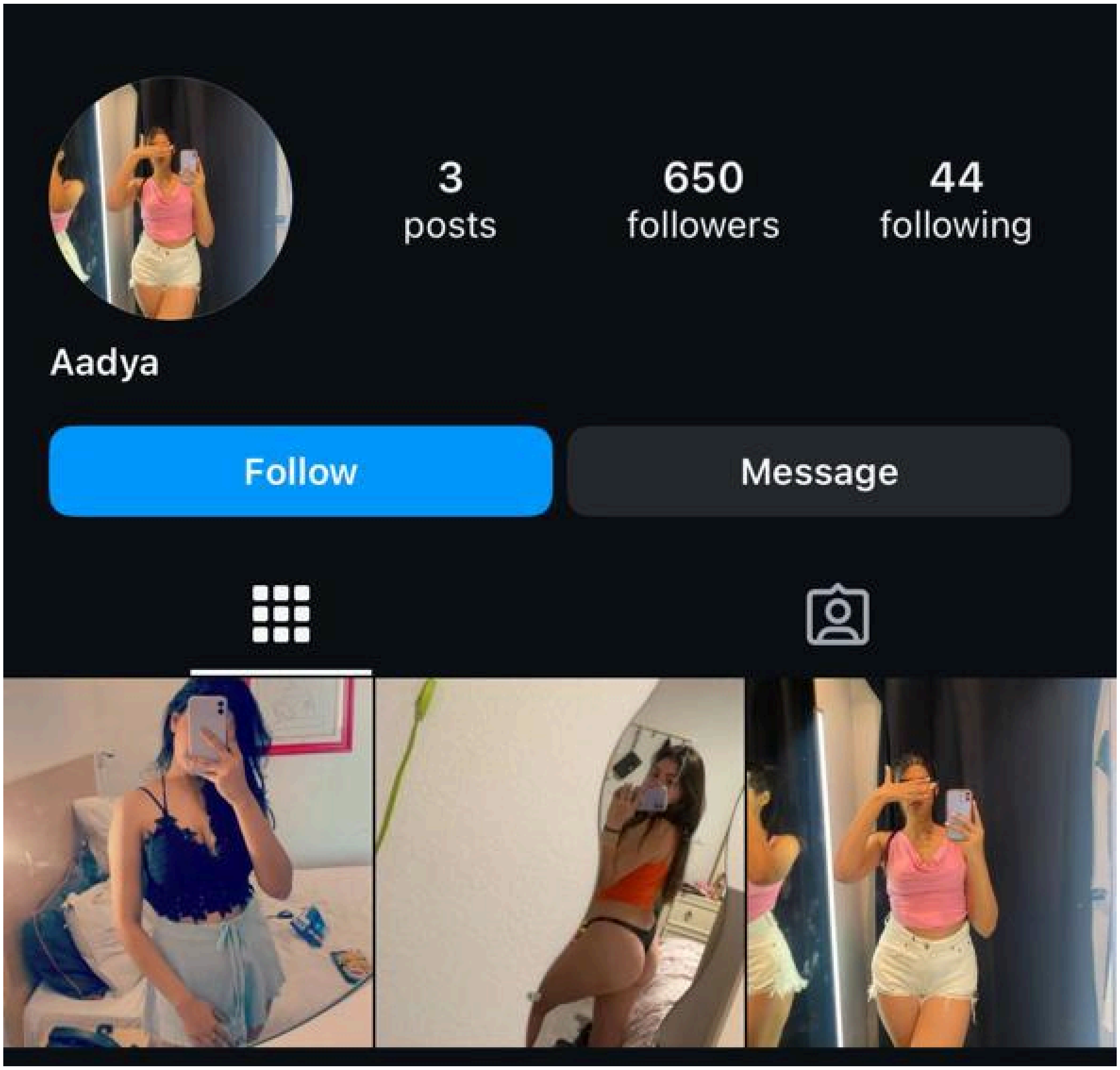
durgashree181
Shree 💫
Follow

call____me___bangara...
call_ me _ bangaram
Follow

mr__priya__singh_888
Priya Singh 💞🥀
Follow

call__me__hasini__12
call me hasini ❤️
Follow

akshara__akki____
Akshara Akshi 😍
Follow

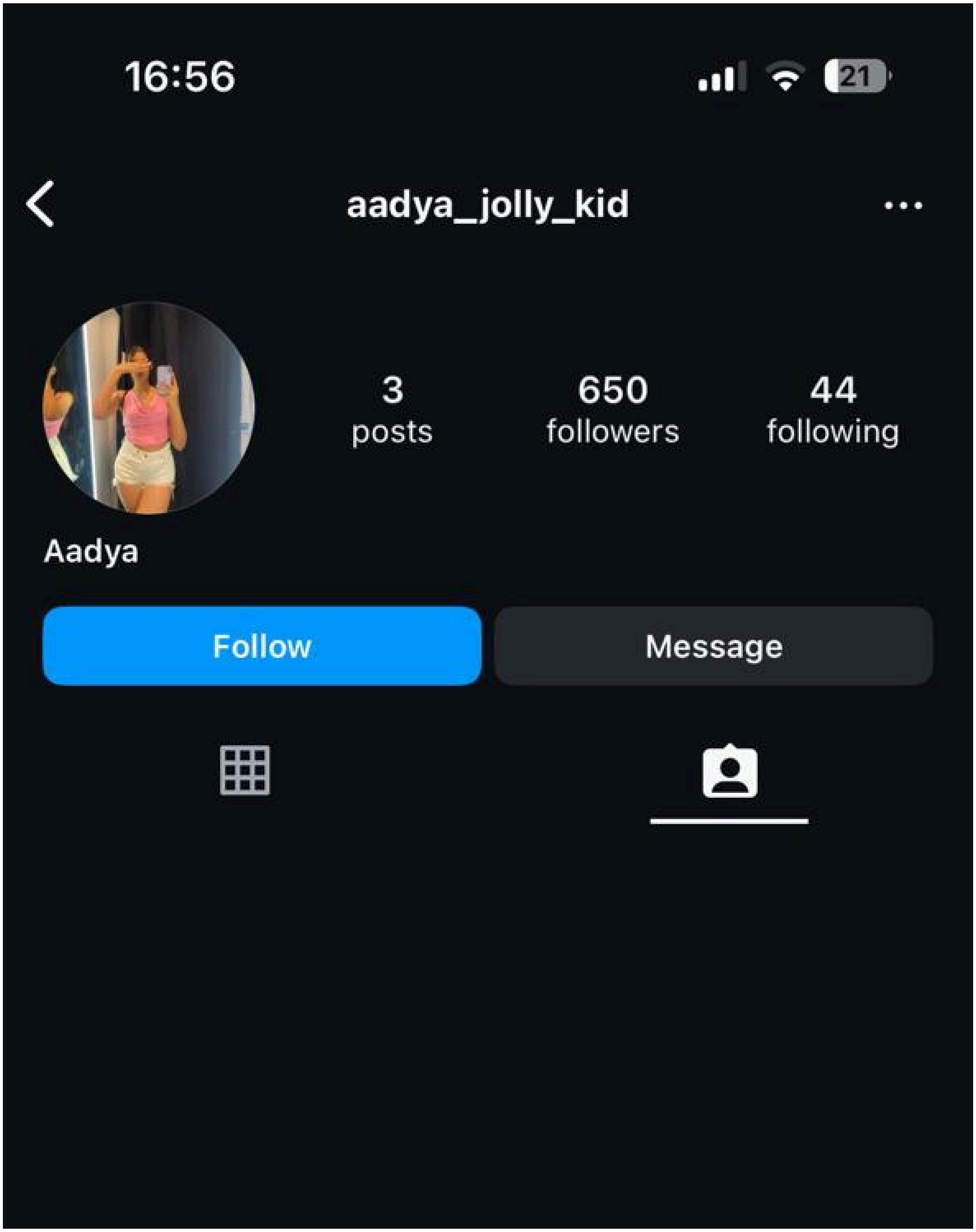


3 posts

650 followers

44 following

Aadya



aadya_jolly_kid

3 posts

650 followers

44 following

Aadya

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

Interpol's International Child Sexual Exploitation (ICSE) Database is a crucial tool in combating child sexual exploitation globally. Its primary objectives and target demographics can be outlined as follows:

**Objectives**

1. Identification of Victims: The primary goal of the ICSE Database is to identify victims of child sexual exploitation and provide them with the necessary support and protection.
2. Identification of Offenders: By analyzing images and videos, the database aims to identify perpetrators and bring them to justice.
3. Facilitation of International Collaboration: The database promotes collaboration among law enforcement agencies worldwide by providing a centralized repository of data that can be accessed and analyzed globally.
4. Reduction of Duplication of Efforts: By providing a shared platform, the ICSE Database helps avoid duplication of efforts among different agencies, making the investigative process more efficient.
5. Enhancement of Investigative Capabilities: The database uses advanced technologies to enhance the capabilities of investigators, including image and video analysis tools that help in identifying and locating victims and offenders.
6. Capacity Building and Training: It aims to support member countries in building their capacities to combat child sexual exploitation by providing training and resources.

**Demographics**

1. Law Enforcement Agencies: The primary users of the ICSE Database are law enforcement agencies across Interpol's member countries. These agencies use the database to share information and collaborate on cases involving child sexual exploitation.
2. Victims of Child Sexual Exploitation: While not direct users of the database, the primary beneficiaries are the children who are victims of sexual exploitation. The database aims to rescue these children and provide them with the necessary support.
3. Investigators and Analysts: Specialists who work on child exploitation cases, including digital forensic analysts and investigators, use the database to aid their work in identifying victims and offenders.

4. Policy Makers and Child Protection Organizations: Although not direct users, these groups benefit from the data and insights generated by the database to inform policies and strategies to combat child sexual exploitation.

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

The CIS Google Android Benchmark provides a comprehensive set of recommendations for hardening your Android device's security and privacy. Here's a quick overview of the settings it suggests for privacy and browsers:

**Privacy Settings:**

- Lock Screen: The benchmark recommends strong lock screen options like PIN, password, or fingerprint to prevent unauthorized access. It also suggests disabling notifications on the lock screen to avoid sensitive information being exposed.
- App Permissions: It emphasizes reviewing and granting app permissions cautiously. Only allow apps the minimum permissions they need to function.
- Location Services: The benchmark advises on managing location services for apps. Enable them only when needed and disable them otherwise.
- Advertising: Consider disabling personalized advertising to limit data collection for ad targeting.
- Find My Device: Enabling "Find My Device" helps locate a lost or stolen phone.

**Browser Configuration (Likely Chrome):**

- Pop-ups and Redirects: Blocking pop-ups and redirects helps prevent exposure to malicious websites.
- JavaScript: Disabling JavaScript can enhance security but may break some website functionalities. The recommendation might be to enable it with caution.
- Third-party Cookies: Blocking third-party cookies limits tracking across different websites.
- Incognito Mode: The benchmark might suggest using incognito mode for browsing sessions where you don't want your activity tracked.
- Safe Browsing: Keeping Google Safe Browsing enabled helps protect against malware and phishing sites.

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

The ISEA (Information Security Education and Awareness) portal, hosted at www.infosecawareness.in, provides guidelines for children to follow while accessing public systems.

1. User Authentication: Children should use strong, unique passwords for their accounts on public systems and avoid sharing these passwords with others.
2. Personal Information: They should be cautious about sharing personal information such as full name, address, phone number, school name, or photos with strangers or on public forums.
3. Safe Browsing Practices: Encouragement to visit only trusted websites and avoid clicking on suspicious links or pop-ups that may lead to malicious websites.
4. Awareness of Cyberbullying: Children should understand the concept of cyberbullying and know how to respond if they experience or witness it online. This includes reporting such incidents to trusted adults.
5. Privacy Settings: Understanding and utilizing privacy settings on social media platforms and other online services to control who can view their information and posts.
6. Downloading and Sharing: Being cautious about downloading files or software from unknown sources and avoiding sharing files that may contain viruses or malware.
7. Reporting Concerns: Knowing how and where to report any suspicious or inappropriate behavior encountered online to parents, teachers, or trusted adults.