Security Advisory:

Beware of Digital Arrest Frauds

In recent incidents, cybercriminals posing as police officials have been alleging unsuspecting individuals in fictitious money-laundering cases, manipulating and extorting money by threatening individuals with fake cases and interrogation !

Modus Operandi

⇨ Scammers posing as police officials, contact unsuspecting individuals alleging legal cases against them.

⇨ Using Aadhaar and SIM card details, scammers threaten individuals in the name of legal action and arrests by mentioning fake police cases.

⇨ Sometimes, scammers may conduct fabricated video call displaying a mock police station and present forged complaint documents along with Fake ID cards to deceive individuals.

⇨ Individuals are encouraged to communicate via private chats on messaging Apps like Skype, Telegram etc.

⇨ Under pressure, the individuals are coerced into transferring large sums of money to specified Bank Accounts or UPI IDs to evade supposed arrests.

⇨ Scammers may also persuade individuals to apply for personal loans online using their Aadhar, PAN etc., urging them to arrange money quickly. Once the loan amount is credited, the entire sum is siphoned off immediately by cybercriminals, leaving victim in a financial predicament.

Preventive Measures

✓ Be wary of unsolicited calls claiming legal issues or urgent threats, especially if they demand immediate action or money transfer.

✓ If threatened with legal action, verify with the relevant authorities before complying with any instructions or transferring funds.

✓ Always ask for the Official notice, other necessary details etc. & directly communicate with the local police station for verification / clarification.

✓ Refrain from sharing personal, financial, or Aadhar card details over the phone unless you can confirm the legitimacy of the call.

Always remember, real police authorities don't question individuals digitally. Official discussions happen through legitimate or formal channels, not through random online intimidation or coercion.

Report Cyber fraud Incident to **https://www.cybercrime.gov.in**

or call **1930** for assistance