Beware of “Digital Arrest” scams

The “Digital Arrest” scam involves fraudsters who pose as officials from various organisations, including government agencies and law enforcement, to intimidate and defraud individuals. The scam typically begins with a video call where the scammers falsely accuse the victim of involvement in illegal activities. These accusations are designed to create panic and compel the victim to comply with financial demands.

Common tactics used by scammers:

- **False accusations**: Scammers claim that the victim is implicated in criminal activities such as drug trafficking or possession of illegal items.
- **Fabricated emergencies**: Victims may be told that a loved one is in trouble, such as being in custody or involved in an accident.
- **Demand for money**: To resolve the fabricated issues, victims are asked to transfer money immediately.

Recent high-profile cases

In a recent incident, a prominent doctor based in Noida, was targeted by scammers posing as officials from the Telecom Regulatory Authority of India (TRAI), as per reports. The fraudsters accused her of using her phone number to distribute illegal content. Under duress, doctor transferred Rs 60 lakh before realising the scam.

In a similar case involved a 72-year-old woman from South Delhi, who was deceived by scammers impersonating police personnel. The fraudsters extorted Rs 83 lakh from her by fabricating a legal issue requiring immediate payment.

In a rare cyberfraud case, a 59-year-old executive in Bengaluru was duped of Rs 59 lakh by scammers who conducted a fake online trial, complete with a simulated courtroom and judge.

Scammers often use sophisticated setups to enhance their credibility:

- **Fake offices**: Studios are designed to mimic police stations or government offices.
- **Uniforms**: Scammers wear official-looking uniforms to appear legitimate.

- **Video conferencing tools**: Platforms like Skype are used to create a convincing and interactive experience.

To avoid falling victim to the “Digital Arrest” scam:

- **Verify caller identity**: Always confirm the identity of individuals claiming to be from official agencies.
- **Avoid immediate payments**: Do not transfer money based on unsolicited calls or video requests.
- **Seek help**: Contact local authorities or trusted individuals if you receive suspicious communications.

Prompt reporting to cybercrime authorities is essential to prevent further victimisation and assist in law enforcement efforts

Report suspicious calls to the cybercrime **helpline number 1930 or through the website www.cybercrime.gov.in.**