BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Haryana Man Loses ₹10 Lakh in Fake Work-From-Home Job Scam

- **Victim's Mistake:** Trusting an online job offer

A man in Haryana fell for an online "work-from-home" job offer that promised easy earnings. The fraudsters asked him to invest small amounts, showing fake profits initially. When he tried to withdraw his earnings, they demanded more money in the name of "processing fees." He ended up losing ₹10 lakh.

- **Lesson:** Never pay upfront fees for jobs. Legitimate employers never ask for money.

Hyderabad Woman Duped of ₹15 Lakh in 'Digital Arrest' Scam

- **Victim's Mistake:** Panicking when threatened.

A 35-year-old Hyderabad woman received a call from someone claiming to be a TRAI official, saying her phone number was linked to illegal activities. The scammer transferred her to a "CBI officer," who threatened her with arrest unless she transferred money into a "verification account." Out of fear, she wired ₹15 lakh before realizing it was a scam.

- **Lesson:** No government official will ever demand money over a phone call. If in doubt, hang up and verify with local authorities.

Businessman in Vadodara Loses ₹87 Lakh in Fake Stock Trading Scheme

- **Victim's Mistake:** Trusting a fake investment group

A businessman was lured into a WhatsApp stock trading group that promised high returns. He was told to start with small investments and saw fake profits in his trading account. Encouraged, he invested ₹87 lakh—only to realize he could not withdraw his money.

- **Lesson:** Be cautious of unverified online investment schemes. Always check if a financial firm is registered with SEBI (Securities and Exchange Board of India).

Retired Government Officer in Indore Tricked by 'Part-Time Online Task' Scam

- **Victim's Mistake:** Sending money to "unlock" higher earnings.

A 60-year-old retired officer received a Telegram message offering a simple online job—liking YouTube videos for money. Initially, he received small payments, which built trust. Later, he was asked to "invest" for bigger earnings. He ended up transferring ₹12.5 lakh, only to be blocked by the fraudsters.

- **Lesson:** : If a job pays you to do nothing meaningful, it's a scam. Don't invest in schemes that require money upfront.

Chennai Student's Instagram Hacked, Used for Sextortion Scam

- **Victim's Mistake:** Clicking on a fake link.

A 19-year-old college student received a message from a "verified" Instagram account, claiming she had won a prize. The message contained a link that stole her login details. The hacker then locked her out, contacted her followers, and demanded money from them by threatening to release edited explicit photos.

- **Lesson:** Never click on unverified links. Enable two-factor authentication (2FA) to protect your accounts.

Quick Tips to Stay Safe

- **Verify Calls:** If someone claims to be a government official, bank executive, or police officer, hang up and verify independently.
- **Don't Rush:** Scammers create urgency to make you act without thinking. Take a moment to check.
- **Avoid Quick Profits:** If a scheme promises "easy money," it's a scam.
- **Secure Your Accounts:** Use strong passwords and two-factor authentication (2FA).
- **Report Cyber Fraud:** If you suspect a scam, report it at cybercrime.gov.in or call 1930.

Cyber scams are increasing in India, but awareness is your best defense! Share this with friends & family to keep them safe.

Powered by GRAMAX A GMR GROUP ENTERPRISE