BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Retired Naval Officer Loses ₹2.47 Crore to Fake Investment App

Incident: A 65-year-old retired Navy officer was scammed out of ₹2.47 crore after being misled into downloading a fake investment app.

Modus Operandi: The victim was added to a WhatsApp group that mimicked an authentic investment community. Group members, likely scammers, boasted of high returns. Trusting their advice, the officer downloaded the fraudulent app and followed stock tips that prompted him to invest large sums across several bank accounts. The app displayed fake profits, showing a portfolio worth ₹39.43 crore to build credibility and push further investments.

Action Taken: A case has been registered by Navi Mumbai Cyber Police under relevant sections of the IT Act. The scammers are currently under investigation.

Key Concern: Fraudsters are using sophisticated fake platforms and social proof to manipulate and defraud individuals—especially the retired and elderly.

₹11.19 Crore Corporate Fraud Averted Just in Time

Incident: A massive scam targeting a private business in Mumbai was intercepted before a ₹11.34 crore transfer could go through.

Modus Operandi: Cybercriminals hacked into the company's email account and sent a fraudulent request to the bank, instructing transfers of large amounts to two different accounts under the guise of business transactions.

Action Taken: The alert complainant contacted the 1930 Cyber Helpline. Swift coordination between Mumbai Police and the bank helped stop the transaction in time.

Key Concern: Business Email Compromise (BEC) attacks can result in devastating losses. Immediate reporting is crucial for damage control.

Retired Judge Defrauded of ₹90 Lakh in Investment Scam

Incident: A retired Kerala High Court judge was duped into investing ₹90 lakh into a fake scheme.

Modus Operandi: Fraudsters posed as representatives of an investment firm offering high returns. The judge transferred funds over a period, expecting returns that never came. The money was then funnelled through mule accounts and converted into cryptocurrency.

Action Taken: Three suspects have been arrested. Police traced the money trail to ATMs and crypto wallets used by the fraudsters.

Key Concern: Cybercriminals are leveraging fake investment schemes and using crypto to launder stolen funds quickly and discreetly.

87-Year-Old Retired Doctor Scammed of ₹16.14 Lakh Over Fake Pest Control Call

Incident: An elderly woman looking for pest control services became the victim of a cyber scam.

Modus Operandi: While searching for civic service numbers online, she dialled a fake contact. The scammer asked for a ₹50 registration fee and sent her a malicious link. After she entered her details, her phone was compromised, and over ₹16 lakh was drained from her account through a series of unauthorized transactions—all while she was still on the call.

Action Taken: An FIR has been registered. The scam highlights how even the smallest online actions can open doors to major financial loss.

Key Concern: Search engine manipulation and impersonation of government service contacts are becoming common entry points for scams.

Delhi Woman Loses ₹1.10 Lakh After Clicking Suspicious Link on WhatsApp

Incident: A new mother from Delhi shared a viral video revealing how she lost ₹1.10 lakh through a phone scam.

Modus Operandi: She received a suspicious call, followed by a spoofed message and malicious link. Upon entering her bank details, her money was instantly siphoned off. She also received alerts from UPI apps she hadn't even registered with. When she approached the police, they dismissed her, claiming this type of fraud happens "every day."

Action Taken: A police complaint has been filed. The number was traced back to a 70-year-old man in Bihar, indicating possible misuse of identity.

Key Concern: Phishing links, message spoofing, and poor institutional response continue to enable scammers.