BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Investors Defrauded Of ₹5.39 Crore through Fake Online Trading Platform

Incident:
Investors lost a staggering ₹5.39 crore after falling prey to a fake online trading app scam run by a 29-year-old individual from Mumbai.

Modus Operandi:
The fraudster, linked with multiple cybercrime cases nationwide, operated a fake trading platform posing as a legitimate investment company. Victims were approached via social media and dating platforms, offered high returns, and lured into transferring large sums. Layered banking networks were used to launder the funds and hide digital footprints.

Action Taken:
Authorities identified bank accounts linked to over 50 cybercrime cases connected to the scam. An investigation into recovering the siphoned funds is ongoing.

Key Concern:
The rise of fake financial platforms exploiting online trust and relationship-building tactics is leading to multimillion-rupee scams targeting individuals across India.

Entrepreneur Falls Victim To ₹53 Lakh Stock Market Investment Fraud

Incident:
A woman entrepreneur from Malad was conned out of ₹53 lakh by fraudsters promising high returns in stock market trading.

Modus Operandi:
The scammer posed as a mutual acquaintance, won her trust, and added her to a fake WhatsApp group where members (likely fake profiles) shared positive testimonials about profitable investments. After observing for a few days, the victim invested significant sums through links shared by the fraudster.

Action Taken:
The cyber cell is tracing multiple bank accounts opened by the fraudster to launder the defrauded money.

Key Concern:
Social engineering tactics and fake community endorsements are being increasingly used to lure educated professionals into high-value cyber investment scams.

Bank Defrauded Of ₹10 Crore Through Forged Letters Of Credit

Incident:
A public sector bank suffered a ₹10 crore loss after a senior bank manager and two associates created and used fake Letters of Credit (LCs).

Modus Operandi:
The bank official exploited his access to issue fake LCs to a businessman, facilitating massive unauthorized fund withdrawals. The fraud was discovered during internal verifications ahead of issuing a fresh LC.

Action Taken:
An internal inquiry led to the exposure of the fraud, following which court proceedings convicted the accused.

Key Concern:
Internal banking controls are vulnerable to insider threats, leading to massive financial exposure if not promptly audited.

Job Seekers Defrauded Of ₹3.42 Crore through Fake Employment Scheme

Incident:
Unsuspecting job seekers were conned out of ₹3.42 crore through fake employment offers and misuse of their personal documents.

Modus Operandi:
Fraudsters gathered identity proofs such as Aadhaar cards and PAN cards under the guise of job recruitment and used them to open bank accounts. These accounts were later used to route illegal funds linked to various online scams.

Action Taken:
The police launched an investigation after a complainant received a GST department notice regarding suspicious transactions.

Key Concern:
Cybercriminals are exploiting the employment crisis by harvesting personal documents and using them to facilitate large-scale money laundering operations.

Student Loses ₹4.30 Lakh in Online Work-From-Home Task Scam

Incident:
A 20-year-old engineering student from Jammu and Kashmir, currently studying in Mumbai, was defrauded of ₹4.30 lakh through an online task fraud.

Modus Operandi:
The victim was offered simple part-time jobs with high returns via WhatsApp and Telegram. After initial small payments to build trust, he was asked to deposit larger sums for “security fees” but received no further payments.

Action Taken:
The student filed a police complaint; authorities are investigating digital leads and transaction channels.

Key Concern:
Students seeking part-time income are becoming primary targets for cybercriminals using fake task scams on social media platforms.

Powered by GRAMAX
A GMR GROUP ENTERPRISE