BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Palwal Police Busts Delhi-Based Cyber Fraud Call Centre; 11 Arrested in ₹40 Lakh Scam

Incident
A fake call centre operating out of Delhi was busted by the police, leading to the arrest of 11 individuals (including three women) involved in a nationwide credit card fraud exceeding ₹40 lakh. The case came to light after a resident reported unauthorized transactions on his credit card amounting to ₹33,000.

Modus Operandi
The fraudsters ran a bogus customer care centre, pretending to be bank representatives. They contacted credit card holders and convinced them to share their one-time passwords (OTPs) by falsely promising an increase in their credit limits. Once the victims provided OTPs, the fraudsters used them to transfer money through digital wallets and withdrew the funds via Common Service Centres (CSCs).

Action Taken
Acting on the complaint, the cybercrime unit conducted a targeted operation, raided the fake call centre, and arrested 11 people connected with the fraud.

Key Concern
The incident highlights the continuing threat of social engineering scams, where fraudsters exploit victims' trust by posing as legitimate service providers. People should remain cautious about sharing OTPs or sensitive information over the phone, especially when contacted unexpectedly.

4 held from Gujarat for cyber fraud cases worth ₹1.38cr

Incident
The cybercrime cell of the police arrested four individuals from Gujarat in connection with three separate cases of financial fraud targeting residents earlier this year. One major case involved a victim who was defrauded of over ₹1 crore after being lured into investing through a fake demat trading app.

Modus Operandi
The fraudsters added victims to a WhatsApp group posing as an investment institute, where they initially offered small returns to gain their trust. Once victims invested significant amounts, the fraudsters prevented withdrawals and demanded additional payments under the pretext of taxes, using intimidation and threats to coerce more money.

Action Taken
During the investigation, authorities obtained call data records, customer application forms, and KYCs linked to the fraudulent bank accounts. Funds were tracked to multiple bank accounts in Gujarat, leading to the arrest of four individuals involved in the scam.

Key Concern
The case underscores the dangers of online investment scams, where fraudsters exploit victims through seemingly legitimate trading platforms and social media groups. People should verify investment opportunities independently and avoid making payments based solely on online promises or pressure tactics.

Cyber Police recovers Rs 11,06,555.82 in Online Financial Fraud Cases in Kupwara

Incident
The cyber cell of the district police successfully solved multiple cases of online financial fraud, recovering a total of over ₹11 lakh. The cases involved complaints from various victims, including civilians, government employees, and defence personnel, who were targeted through different digital scams.

Modus Operandi
Fraudsters used a variety of deceptive methods such as fake job offers, fraudulent investment schemes, bogus KYC update requests, misleading credit SMS alerts, and impersonation scams. Victims were manipulated into voluntarily or unknowingly transferring money to fraudulent accounts.

Action Taken
The cyber cell acted promptly by gathering digital evidence and coordinating with financial institutions and service providers. Through a combination of court interventions and advanced cyber techniques, investigators traced the fraudulent transactions and successfully recovered funds in multiple cases.

Key Concern
The rise in diverse online scams highlights the need for constant vigilance against digital threats, including digital arrest scams, fake online trading platforms, fraudulent credit SMS messages, and malicious mobile applications. The public should exercise caution when responding to unexpected messages or requests for personal or financial information online.

Vizag Cyber Crime Police Bust Betting Call Centre in Bengaluru, Arrest 13 Andhra Pradesh

Incident
The city cybercrime police dismantled an interstate online betting network by raiding a call centre in Bengaluru, leading to the arrest of 13 individuals. The case was initiated after a victim reported suspicious transactions linked to online gambling platforms.

Modus Operandi
The accused were allegedly operating online betting services connected to various gambling apps. Victims were introduced to online gambling by acquaintances who encouraged them to open multiple bank accounts. These accounts were then used for suspicious transactions involving large sums of money, including transactions exceeding ₹14 lakh.

Action Taken
Based on technical evidence and intelligence, the police conducted a targeted operation, raiding the call centre and seizing 60 mobile phones, 13 laptops, 132 ATM cards, 137 bank passbooks, cheque books, webcams, routers, a money-counting machine, and financial ledgers. The arrested individuals came from multiple states. Legal proceedings have been initiated under relevant sections of criminal, IT, and gaming laws, and efforts are ongoing to apprehend the primary suspect who remains at large.

Key Concern
The case highlights the growing threat of online gambling networks exploiting unsuspecting individuals to facilitate large-scale financial fraud. People should exercise caution when approached to open bank accounts or participate in online betting, as these activities can lead to involvement in illegal transactions and severe legal consequences.

61-Year-Old Seawoods Senior Citizen Duped Of ₹1.36 Crore in Fake Stock Market App Scam; Case Registered

Incident
A senior citizen was defrauded of ₹1.36 crore by a cybercrime gang that lured him into investing in fake stock market schemes through a fraudulent mobile application. The case was registered by the cyber police after the victim reported the incident.

Modus Operandi
The victim encountered an online advertisement about stock market investments on social media. After clicking the link and providing personal details, he was added to a messaging group where members appeared to share high returns on share investments, creating a false sense of legitimacy. Convinced by these fabricated success stories, the victim invested significant amounts of money.

Action Taken
A case has been registered under relevant provisions of fraud and IT laws, and an investigation is underway to identify and apprehend those responsible for the scam.

Key Concern
The case underscores the dangers of investment scams promoted through social media platforms, which often exploit fabricated testimonials to create a false impression of credibility. Individuals should be cautious of unsolicited investment offers online and verify the authenticity of platforms before sharing personal details or investing funds.