

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD



CB Anti-Corruption Officer Scam – ₹35 Lakh Fraud Across UP & Gujarat

Incident

A gang posing as officers from the Central Bureau's Anti-Corruption Wing duped several people across Uttar Pradesh and Gujarat. Victims were falsely informed that they were involved in money laundering or financial crimes and coerced into transferring money under the pretext of clearing their names. The total fraud amount exceeded ₹35 lakh.

Modus Operandi

The fraudsters called victims pretending to be senior CB officials, claiming investigations into suspicious financial activities. They threatened arrests and legal action if immediate payments were not made. The victims, fearing prosecution, transferred amounts into mule bank accounts provided by the scammers.

Action Taken

Police teams from UP and Gujarat collaborated and arrested multiple accused from different cities. Authorities also identified and froze several bank accounts used to siphon off funds. Investigations are ongoing to trace other members of the network and recover the defrauded money.

Key Concern

The scam highlights how impersonation of government officials can be used to exploit fear among citizens. It underlines the need for better awareness about official communication protocols and stronger checks on opening fraudulent bank accounts.

Nashik Stock Market Cyber Fraud – ₹55 Lakh Lost

Incident

A Nashik-based businessman was tricked into investing in a fake stock market scheme promoted through social media platforms, leading to a loss of over ₹55 lakh.

Modus Operandi

Fraudsters created a fake online trading portal and lured the victim through attractive promises of high returns. They provided login credentials to the platform where fabricated profits were displayed, enticing the victim to keep investing. When the victim tried to withdraw money, the portal became unresponsive.

Action Taken

The victim filed a complaint with Nashik cyber police, who have registered an FIR and started tracing the digital footprints of the scammers. Authorities have also issued alerts warning others against such investment scams.

Key Concern

This case exposes vulnerabilities in online investment awareness, emphasizing the need for verifying financial platforms and regulatory registrations before investing.

Rath Yatra 2025 Hotel Booking Fraud

Incident

Several devotees planning to attend Rath Yatra 2025 in Odisha fell victim to a hotel booking scam, collectively losing lakhs of rupees after making advance payments for non-existent hotel rooms.

Modus Operandi

Scammers created fake websites and social media pages impersonating popular hotels in Puri, advertising attractive rates and asking devotees to pay in advance. Victims realized they were duped only upon contacting the hotels directly or arriving in Puri.

Action Taken

Multiple complaints were filed with Odisha Police, which have launched a probe to identify the fraudsters. Cybercrime units are tracking phone numbers and payment gateways used in the scam.

Key Concern

The case underscores the risk of online travel booking frauds, especially around major events. It highlights the importance of booking through official hotel websites or verified aggregators.

Hyderabad Cybercrime – Betting Scam Using Influencers

Incident

Hyderabad Police busted a syndicate involving social media influencers who promoted illegal betting apps, leading to widespread financial losses among users.

Modus Operandi

Influencers were paid to endorse betting platforms on Instagram and YouTube, attracting followers to register and deposit money. These apps manipulated results to ensure players kept losing, and their deposits were siphoned off.

Action Taken

Police arrested several influencers along with the main operators behind the betting platforms. Authorities seized digital devices, bank accounts, and marketing materials. Further investigation is ongoing to identify other accomplices.

Key Concern

This case shows how influencers can be misused to legitimize illegal activities, calling for stricter guidelines around endorsements and better digital literacy among social media users.

Chips Seller Lured with Chandigarh Trip, Used as Bank Mule in ₹1.93 Crore Cyber Fraud

Incident

A chips seller from Uttarakhand was duped with the promise of a free Chandigarh tour but was instead used as a bank mule in a massive cyber fraud worth ₹1.93 crore. The victim unknowingly helped the fraudsters launder stolen money through his bank account.

Modus Operandi

Fraudsters befriended the chips seller, offering an all-expenses-paid trip to Chandigarh. During the trip, they convinced him to open new bank accounts, citing the need for formalities like hotel bookings and travel expenses. These accounts were later used to channel proceeds from multiple cyber frauds across the country.

Action Taken

Cybercrime police identified unusual large transactions in the victim's accounts and questioned him, uncovering the mule network. An FIR was registered, and efforts are underway to trace and arrest the main fraudsters behind the syndicate.

Key Concern

This case highlights how vulnerable individuals can be exploited as money mules, emphasizing the importance of public awareness around safeguarding personal financial credentials and recognizing signs of fraudulent schemes.