BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

GRAMAX
A GMR GROUP ENTERPRISE

CBI Raids Igatpuri Resort Call Centre, nabs 5 in ₹1 Crore Cyber Fraud Targeting US, Canada Victims

Incident
Authorities conducted a raid on an illegal international call centre operating from a resort in Maharashtra, leading to the arrest of multiple individuals. The operation resulted in the seizure of seven luxury cars, 44 laptops, ₹1.20 crore in cash, and 500 grams of gold.

Modus Operandi
The accused were allegedly running a fraudulent operation by impersonating customer support representatives of a well-known e-commerce platform. They made phishing and deceptive calls to victims based in the US and Canada, luring them into providing sensitive financial information. The scam involved transactions of approximately 5,000 USDT cryptocurrency (₹5 lakh) and gift vouchers worth 2,000 Canadian Dollars (₹1.26 lakh).

Action Taken
Following the registration of a cyber fraud case earlier this month, investigators raided the resort premises and apprehended several individuals linked to the scam. The operation also uncovered significant assets believed to be proceeds from the fraudulent activities.

Key Concern
The incident highlights the growing sophistication of cross-border cyber fraud operations and the use of impersonation techniques targeting overseas victims. It also underscores the involvement of cryptocurrency and digital gift cards as preferred mediums for transferring illicit funds.

From Gujarat to Tamil Nadu: Six Arrested, Lakhs Recovered in MultiState Cyber Fraud Linked to 10 States

Incident
Police have arrested multiple individuals involved in a multi-state online fraud network, recovering ₹20.81 lakh siphoned from victims' bank accounts. The operation exposed a network of fraudulent transactions spread across several states.

Modus Operandi
The accused allegedly opened multiple bank accounts or used existing mule accounts to receive funds from victims. These funds were quickly dispersed across numerous accounts in smaller amounts to evade detection. In this case, withdrawals were traced to over 10 different bank accounts linked to shell firms and individuals.

Action Taken
Within three days of receiving the complaint, investigators tracked the movement of funds through the national cybercrime reporting system. This led to the identification of suspects across multiple states, followed by arrests and the recovery of stolen funds.

Key Concern
The case underlines the growing prevalence of coordinated online fraud networks that leverage mule accounts and rapid fund dispersal techniques to obscure money trails, making detection and recovery more challenging.

Retired Woman in Mangaluru Loses ₹3.09 Crore in "Digital Arrest" Cyber Scam

Incident
A retired woman in Mangaluru lost over ₹3.09 crore in a highly organized "digital arrest" cyber scam. The victim received a call from someone posing as an official, claiming a parcel in her name had been seized for containing illegal substances.

Modus Operandi
The fraudsters alleged that the parcel was booked using the victim's identity documents and contained banned drugs. They threatened severe legal consequences, including decades of imprisonment, and convinced the victim that a "no-objection certificate" could clear her name — but only if she transferred a large portion of her pension. Under sustained fear and pressure over six months, she made multiple RTGS transfers to bank accounts provided by the scammers, totaling ₹3.09 crore.

Action Taken
A case has been registered, and police are investigating to identify and apprehend those behind the scam. Efforts are underway to trace the money trail and recover the stolen funds.

Key Concern
This case highlights the alarming rise of "digital arrest" scams, where victims are manipulated through fabricated legal threats and coercion into making large financial transfers. Public awareness and caution are essential to avoid falling prey to such schemes.

Two more arrested in ₹73L cyber fraud case

Incident
Police have arrested two more individuals in connection with a ₹73 lakh cyber fraud targeting a law firm. This brings the total number of arrests in the case to four. The fraud involved the unauthorized siphoning of funds from the firm's bank account.

Modus Operandi
The perpetrators allegedly used fake emails and counterfeit SIM cards obtained through forged documents to execute the fraud. These tools enabled them to gain access to sensitive financial information and carry out unauthorized transactions.

Action Taken
Following earlier arrests in the case, investigators apprehended two additional suspects from Rajasthan. The accused were presented in court and remanded to police custody for further questioning. The investigation aims to uncover the full extent of the network and recover the misappropriated funds.

Key Concern
This case underscores the increasing use of forged digital identities and fraudulent communication channels in corporate-targeted cybercrimes, emphasizing the need for strict verification protocols and timely incident reporting.