BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Cyber Fraud Racket Busted; 6 Arrested For ₹1.93 Crore Corporate Scam, Chinese Links & Illegal Arms Seized

Incident
An inter-state cyber fraud racket was uncovered involving the impersonation of a company director via WhatsApp, leading to the fraudulent transfer of ₹1.93 crore from a reputed company.

Modus Operandi
The fraudster contacted a senior employee through WhatsApp, pretending to be the company's director. Using social engineering tactics, they manipulated the employee into transferring a large sum of money to a bank account that was later found to be linked to multiple cyber fraud complaints.

Action Taken
The cyber police conducted a technical investigation and arrested six individuals from multiple states, including Maharashtra, Goa, and Uttar Pradesh.

Key Concern
The ease with which the attacker impersonated a high-level executive and convinced an employee to make a significant financial transaction highlights vulnerabilities in internal verification protocols and the growing threat of social engineering-based cyber-attacks.

25 Linked To 453 Cyber Fraud Cases Arrested in Hyderabad, Crores Recovered

Incident
Twenty-five cyber fraudsters operating across seven states were arrested, with links to 453 cybercrime cases nationwide—66 of which affected victims in a particular region. Among the reported cases was a stock trading scam causing a loss of ₹2.59 crore.

Modus Operandi
Fraudsters used social media platforms like Facebook and WhatsApp to lure victims into investing in a fake stock trading platform. The scale of the operations was vast, as indicated by the seizure of multiple digital and banking instruments including phones, debit cards, cheque books, and SIM cards.

Action Taken
The Cyber Crime Police arrested 25 individuals and seized key evidence. In June alone, ₹72.85 lakh was refunded to victims, and an additional ₹3.67 crore was returned during the National Lok Adalat. Two individuals from a northern state were arrested specifically for the high-value trading scam.

Key Concern
The involvement of fraudsters from multiple states and the high number of cases point to a well-organized, large-scale cybercrime network. The use of trusted platforms like social media to bait victims underscores the urgent need for digital literacy and stringent online investment awareness.

Pune Engineering Firm Duped of ₹2.3 Crore in Email Fraud Involving Foreign Supplier

Incident
An engineering company lost over ₹2.3 crore in a man-in-the-middle (MITM) email scam during an international transaction with a foreign supplier. The incident occurred during the payment process for a machinery purchase.

Modus Operandi
The attackers intercepted email communication between the company and its overseas supplier. On the day of the transaction, the fraudster sent a spoofed email—appearing to be from the supplier—with updated bank account details. The company, unaware of the deception, transferred the funds without verifying the changes through an alternative communication channel.

Action Taken
The case was reported to the Cyber Police Station, and an investigation has been initiated.

Key Concern
The case highlights serious vulnerabilities in email security and the lack of verification protocols in high-value international transactions. It underscores the growing threat of MITM attacks in business-to-business dealings, especially when due diligence is bypassed.

Case against two unidentified cyber fraudsters for attempting to extort Upalokayukta

Incident
A case was registered against two unidentified cyber fraudsters who attempted to intimidate a senior official by impersonating legal consultants from a government data protection authority, possibly as part of an extortion attempt.

Modus Operandi
The fraudsters made a phone call posing as senior and junior legal consultants from a regulatory board. They tried to intimidate the victim with a fake legal case and offered to "resolve" the matter, likely in exchange for money or favors, which is indicative of an extortion strategy using impersonation and legal threats.

Action Taken
A formal complaint was lodged, and a case has been registered under relevant sections of the Information Technology Act. An investigation has been initiated to identify and trace the culprits.

Key Concern
This incident underscores the rising trend of fraudsters impersonating officials from regulatory or legal bodies to target and extort individuals. It also highlights the need for increased public awareness and robust caller verification processes to prevent impersonation-related scams.