

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD



Delhi police bust sextortion, Crime Branch have uncovered a money trail exceeding ₹5 crore.

Incident

The Delhi Police have dismantled widespread sextortion and cyber fraud rackets operating across multiple states. A total of six individuals have been arrested, and investigative teams from the Crime Branch have uncovered a money trail exceeding ₹5 crore.

Modus Operandi

The cybercriminals operated through an illegal call centre in Mundka, which lured victims by offering fake bank loan schemes. Simultaneously, a sextortion racket was active, using synthetic bank account kits to facilitate fraudulent transactions and conceal identities. Victims were deceived through fake offers and manipulated via digital means, allowing the criminals to extract money or sensitive information under false pretences.

Action Taken

On May 24, following a tip-off about a suspicious consignment in the New Ashok Nagar area, the Crime Branch launched an operation and arrested three individuals in possession of synthetic bank account kits. Subsequent raids were conducted: one at the Mundka-based illegal call centre, leading to the arrest of seven people, and another at a New Ashok Nagar location, where four suspects linked to the sextortion racket were apprehended. The total number of arrests in connection with these operations stands at six, with ongoing investigations likely to uncover more links.

Key Concern

The case underscores the increasing sophistication and spreads of cybercrime operations, particularly the use of synthetic identities and fake financial services to exploit unsuspecting individuals. The involvement of call centres and cross-state coordination highlights the urgent need for enhanced cyber vigilance and preventive awareness across the country.

Man arrested for duping senior citizen of ₹6 crore in 'digital arrest' scam

Incident

The Pune City Cyber Police have arrested an individual from Raigad district for his involvement in a 'digital arrest' scam that led to a senior citizen being duped of ₹6.29 crore. The fraud occurred between November 9 and 19, 2024 and came to light when the victim lodged a complaint.

Modus Operandi

The victim received a video call from individuals posing as law enforcement and government officials. Using fear and intimidation, they falsely accused him of being involved in criminal activities and convinced him that he would face a 'digital arrest' unless he transferred money to settle the case. Under pressure, the victim transferred over ₹6 crore to the fraudsters.

Action Taken

During the investigation, cyber police discovered that the accused had made fixed deposits of ₹90 lakh and ₹20 lakh using the defrauded money. Through digital surveillance, IP tracking, and banking transaction trails, the suspect was in Panvel. A police team apprehended him and brought him to Pune for further investigation.

Key Concern

The case underscores the growing threat of impersonation-based cyber scams that exploit fear and trust in authority. The use of video calls by impostors adds a layer of realism, making such scams harder to detect. This incident highlights the urgent need for public awareness, especially among senior citizens, about the dangers of 'digital arrest' frauds.

Man arrested for duping senior citizen of ₹6 crore in 'digital arrest' scam

Incident

The Pune City Cyber Police have arrested an individual from Raigad district for his involvement in a 'digital arrest' scam that led to a senior citizen being duped of ₹6.29 crore. The fraud occurred between November 9 and 19, 2024 and came to light when the victim lodged a complaint.

Modus Operandi

The victim received a video call from individuals posing as law enforcement and government officials. Using fear and intimidation, they falsely accused him of being involved in criminal activities and convinced him that he would face a 'digital arrest' unless he transferred money to settle the case. Under pressure, the victim transferred over ₹6 crore to the fraudsters.

Action Taken

During the investigation, cyber police discovered that the accused had made fixed deposits of ₹90 lakh and ₹20 lakh using the defrauded money. Through digital surveillance, IP tracking, and banking transaction trails, the suspect was in Panvel. A police team apprehended him and brought him to Pune for further investigation.

Key Concern

The case underscores the growing threat of impersonation-based cyber scams that exploit fear and trust in authority. The use of video calls by impostors adds a layer of realism, making such scams harder to detect. This incident highlights the urgent need for public awareness, especially among senior citizens, about the dangers of 'digital arrest' frauds.

Retired School Principal Duped of Rs 1.02 Crore in a Digital Arrest

Incident

A retired school principal was duped of ₹1.02 crore in a sophisticated ‘digital arrest’ scam. The incident came to light when the victim attempted to liquidate a fixed deposit, prompting the bank to alert law enforcement officials.

Modus Operandi

The victim received a phone call on April 27 from individuals impersonating law enforcement and investigative agency officials. She was falsely told that her mobile number would be deactivated due to her alleged involvement in financial dealings and money laundering. The fraudsters further claimed there were 267 FIRs registered against her and kept her under psychological pressure through continuous video calls for two days. Convinced she was under threat of immediate legal action; she transferred over ₹1 crore to a fraudulent account in hopes of “closing” the case.

Action Taken

While attempting to break a fixed deposit of ₹50 lakhs to make another payment, the bank manager became suspicious and immediately notified the authorities. Thanks to timely intervention by the police, the transaction was halted, preventing further financial loss. The remaining amount was thus safeguarded.

Key Concern

This case highlights how cybercriminals exploit fear, authority, and digital communication to manipulate even well-informed individuals. The tactic of impersonating officials and exerting mental pressure through the concept of ‘digital arrest’ is becoming increasingly common. Vigilance by financial institutions and swift law enforcement action proved crucial in limiting the damage in this case.

Chandigarh Woman Loses ₹11 Lakh in Online Job Scam: Two Arrested

Incident

A woman residing in Chandigarh became a victim of an online job scam, resulting in a financial loss of ₹10.99 lakh. The scam was uncovered following her complaint, leading to the arrest of two individuals involved in the fraud.

Modus Operandi

The victim received a WhatsApp message offering easy money for performing simple online tasks, such as liking videos. She was then added to a Telegram group where she was promised high returns in exchange for advance payments. Initially, she transferred ₹1,000 and received ₹1,300 in return, which built her confidence in the scheme. Gradually, she was convinced to transfer increasingly larger amounts with the assurance of even higher profits, eventually sending over ₹10 lakh to the fraudsters.

Action Taken

Upon receiving the complaint on April 19, the cybercrime cell launched an investigation using digital and financial forensics. They traced ₹50,000 to a bank account belonging to one of the suspects. During interrogation, the individual admitted to opening the account for commission and revealed the involvement of a second person. Both individuals were subsequently arrested.

Key Concern

This incident highlights the growing threat of online job scams that prey on individuals seeking flexible work opportunities. Fraudsters exploit trust-building tactics and digital platforms like WhatsApp and Telegram to orchestrate financial fraud. The case underlines the importance of public awareness and early intervention in detecting and reporting suspicious online job offers.

City resident loses ₹1.44 crore to cyber fraud

Incident

A 52-year-old man lost ₹1.44 crore to a fake trading app scam that spanned from March 10 to May 10. The police registered a case against unknown individuals after the victim reported the fraud.

Modus Operandi

The victim was added to a WhatsApp group that claimed to offer stock trading tips for high returns. Shortly after, he was contacted by someone posing as a trading platform representative who convinced him to open an account on a fraudulent app. He initially invested ₹10,000 and saw fake profits displayed on the app, which prompted him to make further investments. Over 20 transactions, he transferred a total of ₹1.05 crore. The app showed a profit of ₹16.75 crore, but when he attempted to withdraw, he was told to first pay a 10% service charge. Even after paying this, he was asked to pay additional amounts under the pretext of fines and technical issues. Suspecting fraud after repeated demands, he refused to pay the final requested amount.

Action Taken

After the victim suspected foul play and filed a complaint, police registered a case against unidentified suspects. The matter is under investigation, with efforts underway to trace the app developers and associated digital footprints.

Key Concern

This case highlights the alarming rise in investment-related cyber frauds that exploit people's desire for quick profits. Fraudsters are using realistic-looking apps and professional communication channels to gain trust and manipulate victims into repeated payments. It underscores the urgent need for public caution while dealing with unsolicited financial schemes and emphasizes the importance of verifying trading platforms through official sources.