

BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead



13-member gang arrested for cyber fraud and Hawala transactions

A woman impersonating a TRAI officer called a victim, claiming their SIM and Aadhaar were being used fraudulently for dark web activities. A caller posing as an officer also contacted the victim, threatening arrest for drug and firearm possession. The victim was convinced to cooperate and transferred Rs 27 lakh to a fake RBI safe account.

Sanyasi loses Rs 27 lakh after cyber criminals posing as policemen threatened to arrest him

An IVR phone call informed a retired engineer that her call would be disconnected in two hours and that she should press 09 for further details. She dialled 09 as she did not want her number to get disconnected since her cell phone number was linked to Aadhaar, bank accounts and others. According to the scammer, the victim was facing a criminal case filed by the police since numerous accounts were registered using her phone number and Aadhaar number, and money laundering was also carried out. The caller transferred the phone to a different individual posing as a police officer, who threatened to arrest her unless she appeared at the cybercrime police station for an investigation within two hours. Later, the scammer persuaded her to make a digital arrest. She was forced to send ₹4.67 crore, that would be returned to her accounts after verification.

Cybercriminals Scam Executive of Rs 59 Lakh Through Fake Online Trial

Cybercriminals accused a 59-year-old executive of money laundering, staged a fake online courtroom, conducted a phony trial, denied him bail, issued a fraudulent court order, and ultimately swindled him out of Rs 59 lakh. A senior officer stated that the stolen funds had been transferred to various bank accounts and UPI IDs. Interestingly, the scammers communicated exclusively in English, unlike typical cyber fraud cases where Hindi is more commonly used. The scam began when victim received an automated call at work from an unknown number, claiming that all of his mobile number would be blocked. He was then transferred to a man who identified himself as a member of the crime branch, and accused victim of being involved in money laundering. The scammer claimed that an account linked to his Aadhaar card had been opened in Canara Bank, even though the victim had no association with the bank.

72-Year-Old Retired Engineer Loses Rs 4.67 Crore

The woman received an automated call claiming her mobile connection would soon be disconnected. Concerned that her phone number was linked to crucial services like Aadhaar and bank accounts, she followed the instructions and pressed the number for further details. They falsely claimed that a parcel containing illegal items like drugs, fake passports, tiger skins, and ATM cards had been seized in her name by customs. The scammers then warned her of an impending "digital arrest" and convinced her to transfer her savings to a supposed Reserve Bank of India (RBI) account for verification, promising that her funds would be returned within 30 minutes. The victim was tricked into transferring Rs 4.67 crore to a fake RBI account, believing it would be returned.

Cyber criminals dupe man of Rs 36.5 lakh

The victim received a call from an unknown number, claiming that his mobile was linked to illegal activities, and 17 FIRs had been filed against him. The scammers sent fraudulent documents, alleging suspicious bank accounts and fake ATM cards under the victim's name. They also provided fake court orders. Posing as an IPS officer, the scammers pressed him to surrender funds, promising to return the money in three days.

Man Loses Rs 4 Lakh to Cyber Fraud

'Cyber Law Consulting' was the website that the victim visited via Facebook. It says it offers investment possibilities and financial advice. He was instructed to join a WhatsApp group from that webpage. Then a number associated with 'Cyber Law Consulting' sent him texts. He was offered high-profit share investing plans by this number. The victim opened an account on the website and began investing after being enticed by the substantial rewards. "They instructed me to pay a thirty percent profit share when I went to them to withdraw money. They demanded payment of a penalty when I requested a withdrawal of monies once more. Their goal was to take as much money out of me as they could each time I wanted to withdraw," the victim said.

Two held for duping elderly couple of Rs. 10.61 Cr in cyber fraud

According to the police, the victim, was contacted by a man posing as a police official, who told him that they were looking into him in relation to a money laundering case. The scammers made up the story that the victim's Aadhaar card and PAN had been used to open a bank account. The victim was then threatened by the scammers using fictitious letters from the Income Tax Department and Enforcement Directorate. The scammers made video conversations and engaged in online communication with the victim while posing as investigators and threatening legal action. The victim was tricked into moving Rs. 10.61 crores into various accounts. During their investigation, the police discovered that the fraudsters had used a current account that had been formed under the name "XYZ Private Limited." The victim transferred a total of Rs. 4.62 crores into the account.