BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Cyber Cell uncovers financial fraud, over Rs 4 lakh recovered

According to a Cyber Cell officer, the victim discovered illegal transactions from their bank account, which prompted them to report the crime on November 10, 2024. He claims that on November 1, 2024, the victim got an APK file that was infected with malware and seemed to have come from an unreliable source. The victim unintentionally downloaded and opened the file, allowing their mobile device to be compromised. The hacker took Rs 4,45,999 out of the victim's account after gaining access to their bank information.

Cyber gang busted, 11 held for Rs 88 lakh fraud

The complainant informed the police that he might be held in connection with a money laundering case that was filed against him after receiving a call on October 19 from someone posing as a CBI investigator. The complaint claims that he was subjected to digital arrest, which forced him to move funds into unidentified accounts to dodge prosecution and avoid legal action.

Cyber Criminals Pose as CBI Officers, Target Retired Professor

A retired professor was involved in a significant cybercrime case after over Rs 3 crore was fraudulently transferred from her accounts in a matter of 48 hours. Police sources claim that the plot started when a group of people showed up at the woman's house with a fake warrant to trick her into thinking she was connected to a court case. Shortly after the cybercriminals called the woman and pretended to be CBI officers. The scammers coerced the elderly woman into sending Rs 3.07 crore to their accounts by claiming that she was being investigated for money laundering and threatening to arrest her right away. The victim obeyed their requests out of concern for her safety and ignorance of the fraud.

Cyber criminals dupe man of Rs 85K

According to the victim, on November 7, his Telegram ID was added to a group. He claimed that the group administrators had given him the opportunity to get paid by doing specific duties. He claimed that he was charged with sending screenshots of the products in the group and that they used to send him messages with links to Amazon purchases. He claimed that he also got paid for completing these tasks. He was thereafter joined to another Telegram group by the admins, who also instructed him to use UPI to transfer funds to a certain account. The man received Rs 3,900 after transferring Rs 3,000. In subsequent transactions, the sum rose to Rs 5,000, Rs 20,000, and then Rs 60,000. According to the victim, the administrators continued demanding more money but failed to transfer any back to him.

Hyderabad retried lecturer loses Rs 45.5L in CBI impersonation scam

On November 12, the victim received a call informing them that someone had reported the police had confiscated a package containing illegal substances. By claiming that his Aadhaar number was connected to the package, the caller falsely accused the victim and threatened to incriminate him in a money laundering case. The caller gave the victim the number of a fictitious CBI officer and told them to comply to avoid arrest. The impostor, who was wearing a police uniform, threatened to take swift legal action against the victim if he did not comply during a WhatsApp video conversation. After being intimidated, the retired lecturer gave the scammers his bank account information and, at their request, transferred money to several accounts via Google Pay, Paytm, Net Banking, and RTGS. To further trick him, the scammers produced fictitious Supreme Court receipts that verified the payments and had a registrar's signature.

Five held for duping minister’s accountant of ₹2 crore in cyber scam

Using the minister's son's display photo, the scammers reached out to the victim via WhatsApp. The cyber police also succeeded in freezing around ₹12 lakh that the offenders had moved to different bank accounts. Police officials said efforts were on to track down the other scammers involved. A WhatsApp message with the profile photo of the minister's son and company director was sent to the minister's accountant on November 13. The cybercriminals, posing as the minister's son, told the accountant to deposit ₹2.08 crore into three separate bank accounts, saying it was to complete certain business transactions.

Woman cyber fraudster extorts Rs 20k from Engineering Student

A cyber extortion group defrauded a 22-year-old engineering student of Rs 20,000 after trapping him on social media and blackmailing him. The victim claimed in his complaint that a few months ago, he became acquainted with a girl on Instagram. Late at night on November 21, he got texts from a woman who triggered him with a video call on WhatsApp that showed him a girl's disrobed footage. Using a different phone, the scammers took the victim's obscene videos, threatened to broadcast them on Instagram, and demanded Rs 20,000, which the victim promptly paid. The victim went to the police when the group wanted additional money and threatened to show his parents and other family members the photos.

Retired Officer Duped of ₹1 Crore in Elaborate Cyber Fraud

A retired government official lost ₹1 crore to scammers after falling prey to a sophisticated cyber scam. At first, the thugs pretended to be customs officers and demanded money to release gifts that were purportedly given by a foreign acquaintance, defrauding him of Rs.20 lakh. The scammers later deceived him into paying an additional ₹80 lakh by posing as embassy employees and offering to reimburse the initial sum. The victim was tricked into thinking a foreign woman he had interacted with on social media had brought him presents. Using this relationship, the scammers demanded large sums of money for fictitious customs taxes. The con artists purported to be embassy representatives and took ₹80 lakh under the pretence of legal and recovery procedures when he asked for assistance in recovering the ₹20 lakh.