GRAMAX
A GMR GROUP ENTERPRISE

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

A 61 year old man duped of Rs 3.40 lakh in gas connection fraud

Victims are being asked to update their MGL gas connection invoices through texts. He received a message from an anonymous sender at approximately 10 a.m. on Sunday, telling him to update his MGL gas connection bill in order to keep utilizing the service. The same person called him shortly after, informing him that if the bill wasn't adjusted, his gas connection would be cut off. After that, the caller gave him instructions on how to download the "MGL Bill Update" app from the Play Store.

Even though the victim had trouble at first downloading the program, the con artist assisted him in adjusting his phone's settings so that the download could proceed. After installing the app, the con artist requested that he input the credentials of his bank account. His credit card was used to deduct ₹3.40 lakh, and multiple transactions were conducted from his account even though he did not receive any OTPs from his bank.

A Railway official lost 9 lakhs online to scammers posing as 'CBI' officers

Cybercriminals posing as CBI investigators stole ₹9 lakh from a railway official, claiming that the official was connected to a bank account that was being used to launder enormous sums of money. The victim went to work and continued to be on video calls, but he was told to go back home by scammers who said that 'CBI officers' wanted to look into him. According to news agency PTI, the official was brought before a con artist posing as a "judge" who demanded that he transfer money into a particular bank account as "penalty" for the offense.

A 26-year-old engineer engages in sextortion scheme targeting foreign victim

According to police, the accused, a Bengaluru-based engineer, targets foreign victims by befriending them on social networking sites and getting them to share their private pictures. Later, he would use these pictures to blackmail and extort money from them. Police said he also used online payment platforms like Zelle, which is widely used in the US, to collect money from his victims and later transfer it to his Indian accounts for further use.

A 59-year-old Bengaluru executive was duped ₹59 lakhs in elaborate fake online courtroom scam

In a shocking case of cyber fraud, a 59-year old Bengaluru man, was scammed out of as much as ₹59 lakh by criminals who staged an elaborate fake online courtroom trial. The victim, became a victim of the fraud between September 12 and 13, The Times of India reported. The ordeal began when the victim received an automated call while at work, warning him that his phone numbers would be blocked. The call was then transferred to someone claiming to be from the crime branch, accusing him of being involved in money laundering, the report noted. Despite the victim knowing he had no connection to the accusations, the scammers intensified their act by making a WhatsApp video call. A man, dressed in a police uniform, appeared to be in a police station, adding to the deception, the publication stated.

A doctor has fallen victim to a Rs 3 crore online fraud, involving scammers impersonating officials from Police

The fraud took place between Aug and Sept this year, involved three accused who tricked the doctor into transferring the sum in various instalments. A police officer said that the accused made a call to her on Aug 14, alleging that a parcel containing contraband, including MDMA and a passport, with credit cards and clothes, had been intercepted under her name. They transferred her call to an official who claimed to be from the crime branch. Posing as officials, they convinced her that her bank accounts were under investigation for money laundering and human trafficking. "They took her statement on a WhatsApp video call and scared her saying her arrest warrant had been released and she had been made an accused in the cases," said the officer

Victim duped by pseudo officers, loses 13 lakh

The woman had received a phone call claiming to be from the Police Station. The caller alleged that her mobile SIM card and Aadhaar card were used in illegal activities, and one of her associates had already been arrested. The caller threatened her unless she paid to avoid being arrested. Consequently, the woman transferred ₹13 lakhs.

Two have conned of ₹2.83 lakh in cyber fraud cases

In the first such case, a 53-year-old woman lost ₹1.70 lakh in an impersonation fraud following a 'digital arrest'. The complainant received a call from fraudsters posing as officials from cybercrime unit and informed that her Aadhaar card, PAN card number, and phone number were used to open a bank account with ₹1 crore. As the victim denied ownership, the fraudsters further said that she was among the 24 individuals booked for engaging in illegal sexual harassment on social media. The fraudsters issued an arrest warrant and promised to cancel the warrant after a 7-day verification, prompting the victim to deposit ₹1.70 lakh into fraudulent accounts," the police said.

Meanwhile, a 51-year-old private employee received a phone call regarding credit card insurance. According to the police, the scamster explained the benefits and convinced the victim to share credit card details, including the CVV number. The fraudster then sent a WhatsApp link to hack the victim's phone and receive OTP. As soon as the victim clicked on the link, a total of ₹1.13 lakh was debited from the victim's SBI credit card in two transactions," said the officials.

Cyber frauds dupe retired cop of ₹10.60L

The victim, was looking for a work-from-home job opportunity after retirement and the cyber frauds lured him with prospects of earning well. According to his complaint to the police, on September 13, he got a WhatsApp message from an unknown woman, offering him a part-time job opportunity. When he showed interest in the offer, he was asked to download the Telegram app, a free, cross platform messaging app, and told that the money would be credited to his account, if he completed the tasks entrusted to him. He, accordingly, completed three tasks of "liking" and "reviewing" some products whose advertisements were displayed on social media and received ₹38,000 in instalments," said a police officer. Later, he was asked to deposit money before new tasks were entrusted to him. He followed the instructions and successfully completed all the tasks and simultaneously deposited the requisite amounts for each of the tasks. However, despite completing the work, his returns were not reflected in his virtual account and when he inquired about it, he was asked to deposit ₹3 lakh more to get the complete amount back.