GRAMAX
A GAR GROUP ENTERPRISE

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

BISHOP DUPED OF ₹15 LAKH BY CYBER FRAUDSTERS

A Christian bishop that he was cheated of ₹15 lakh by cyber frauds who claimed that his Mumbai bank account was linked to a money laundering case related to Jet Airways founder Naresh Goyal. The victim received a call and told, that his account is linked to money laundering case of Naresh Goyal. He was asked to cooperate with the probe. The victim denied the bank account and his connection with Naresh Goyal, to which he was informed his bank account was likely to be misused by the accused and CBI has taken over. After an hour, he got a video call in which the CBI emblem and voices of the officers were seen and heard. During the call, he was asked questions related to his bank accounts he owns and the deposits in them.

He was informed that he was being put in 'digital custody' and he would be presented in court digitally. The next day, the victim was present digitally in the fake court and heard the voice of a 'judge' who asked him about his involvement in the case. He denied the allegations, to which the judge scared the victim that his accounts would be frozen. The victim was asked to declare the accounts and transfer 13 lakh money into a secret service monitored by Supreme Court. He was assured that the money would be returned if he was innocent. He was tricked again and send 1.2 lakh as recently 'withdrawn' amount from the account. The victim said he received documents with the seal of the judge as well as receipts for the money transferred.

DOCTOR, LOST RS 74.38 LAKH TO CYBER CROOKS

A doctor of lost Rs 74.38 lakh to cyber criminals. He got an message on Instagram and he opened the link and invested Rs 24 lakh on the promise that it would grow to Rs 1.27 crore in a few months. A few days, he received a WhatsApp call from cyber criminals who told him to deposit Rs 50 lakh to claim the promised amount. In greed of money without having second thought, the doctor deposited the money.
Later, he received another call asking him to pay 30 per cent of the promised Rs 1.27 crore towards service tax. When he refused, the fraudsters stopped sending messages to him. The doctor then lodged a complaint.

CYBERCROOK CHEATED FOOD STALL OWNER OF 7 LAKH

A 32-year-old food stall owner was cheated of Rs7.1 lakh under the garb of updating his Aadhaar card by a cybercrook, who posed as a bank officer. A call was made through a social media account on July 20, informing the victim that his Aadhaar card, linked to his two bank accounts, required an update.
He was further warned that without this step, he would not be able to conduct further transactions. The accused offered him help and asked him to download a mobile app, using which the update could be carried out easily. The victim followed the instructions as he believed the caller was from a bank. Soon after the apparent completion of the process, the accused withdrew Rs3.9 lakh and Rs3.2 lakh, totalling Rs 7.1 lakh, from both of the victim's accounts. On realising that he had been cheated, the victim followed up with the bank, sharing all details about the fraudster.

POWERED BY
GRAMAX
A GAR GROUP ENTERPRISE

RETIRED BANK MANAGER LOST ₹10 LAKH TO CYBER FRAUD

While scrolling Facebook, the victim came across a link that help him create a credit card. Upon clicking the link, he receive a WhatsApp call. The caller claim to be an executive of a bank and asked him to change phone settings. As the victim clicked on the link, his screen was shared with fraudster.
The caller engaged the victim on call, but soon he realised he was being scammed. He quickly transferred 1 lakh from one of his accounts to another to safeguard his money. Meanwhile, he tried to freeze his accounts but was unable to do so as the option was disable. The fraudster transferred 10 lakh from the victim's account, in 45 minutes, as he had already altered the setting via the shared screen.
The fraudster transferred 2 lakh via the victim's banking app and later the victim discovered the fraudster has also checked his credit score with Punjab national bank and applied for 8 lakh loan. The bank approved the loan within 5 minutes and deposited the amount into his account, to which they transferred this money into their own accounts. The victim noted that no call or OTP was received for loan approval, raising the bank's verification process.

WOMAN WAS CHEATED OF RS 25 LAKH: 'DRUGS IN PARCEL' SCAM, ACCUSED BUSTED.

A woman was cheated of Rs 25 lakh by cyber criminals posing as executives of an international courier company and officials from narcotics department. She was told that a parcel sent in her name to Iran had been intercepted in which drugs, fake credit cards and expired Iranian passports had been recovered. On the pretext of verification of her accounts, the complainant was manipulated into transferring Rs 25 lakh to various fraudulent accounts. In 'drugs in parcel' scams, the victims are contacted by fake international courier service executives claiming drugs have been found in parcels addressed to them. They are told they are under police investigation and are told to communicate via Skype with fake profiles posing as law enforcement officials. Fraudsters impersonate IPS officers to further deceive victims. They coerce victims into transferring money for various reasons, including customs fees or legal charges, and by also claiming that their bank accounts are at risk from hackers. Callers often intimidate victims, claiming they're under surveillance.

IN 5-DAY TRAUMA OF CYBER BLACKMAIL, 74-YR-OLD FORCED TO PART WITH RS 97 LAKHS.

A 74-year-old man was blackmailed over 5 days in which he was coerced to remain on a call and go to the bank multiple times to make large online transfers totalling 97 lakh. The fraudsters posed as police officers threatened to arrest the victim for 'sending obscene messages', 'money laundering' and in matter of 'national security'.

The fraudster identified himself as an officer from the Telecom Regulatory Authority of India. The caller scared the victim that the number would be blocked in 2 hours because obscene messages were being sent from his number to many people in Mumbai. The complainant urged the caller not to disconnect and was given a number to call. The fake police officer told the victim that his bank was being misused for money laundering and an arrest warrant has been issued in his name. The victim was asked to appear before the Mumbai crime branch or he would be arrested. The victim pleaded that he was a senior citizen and he should be spared. He was offered a 'priority investigation' and was directed to furnish all details of his bank accounts, deposits, investments, etc.
The fake IPS officer ask the victim to undergo a thorough verification after 3 days. He was asked to transfer 55 lakh from his savings. He was asked not to disclose the matter and go to bank for while being on call 'surveillance purposes'. He was asked to transfer 20 lakh and 22 lakh while his investigation is done in matter of 'national security'. He was promised to get his money back after the verification process. A while later, the victim tried calling the numbers but there was no response. After realising that he had been cheated, he approached the Cyber crime police station.

A 42-YEAR-OLD RESIDENT WAS DECEIVED INTO LOSING MORE THAN RS 35 LAKHS BY SUBSCRIBING TO A YOUTUBE CHANNEL

A 42-year-old resident was deceived into losing more than Rs 35 lakhs by subscribing to a YouTube channel. The accused contacted the complainant via mobile at 92854 19XXX. The complainant was lured into subscribing to YouTube exclusively through WhatsApp, with no upfront investment. The accused methodically kept looting the complainant, taking advantage of the complainant's initial perception of benefits, to extract a total of ₹35,25,364 through multiple bank accounts.
international transaction fees. The men deposited the fee later he got a phone call and was asked to share the OTP. Without thinking, he shared the OTP in hurry. After few seconds, he got a message from bank stating that his account is debited with a sum of 45k.