GRAMAX
A G&R GROUP ENTERPRISE

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

PRIVATE FIRM EMPLOYEE IN BENGALURU LOST ₹1.9 CRORE IN COURIER SCAM

The victim received a call on his mobile from an unknown person claiming to be from the Mumbai Customs office and the caller said a parcel in his name sent to a foreign country was withheld for having five passports, 200 grams of MDMA, laptops, and cash. The caller informed him that as per the protocol, the Mumbai cybercrime police had been alerted and they were probing the case. Soon, he started receiving calls from different people who claimed to be Customs officials and Mumbai cybercrime police and threatened him that they were probing his possible link with a money-laundering case and sought his bank account details for verification. The victim shared his bank account details from which the accused accessed his bank accounts and withdrew his savings of ₹1.95 crore from two different accounts for two days.

GANG INVOLVED IN HOUSE ARREST, BUSTED!

Digital house arrest is a tactic where cybercriminals confine victims to their homes in order to scam them. Offenders generate fear by making audio or video calls, frequently posing as law enforcement officers using AI-generated voices or videos. the gang duped a complainant of Rs 52.50 lakh by convincing him that his identity was being used to send a parcel abroad containing illegal drugs, passports, and credit cards. The gang posed as officials from the Mumbai crime branch and other agencies, claiming to investigate money laundering, police said. Their modus operandi included using third party bank accounts, making phone and WhatsApp calls, and sending fake IDs to convince victims of their authority. "The suspects would tell the account holders that their parcels containing illegal items were caught by customs in Mumbai, and the investigation was confidential, deterring them from discussing it with anyone.

DELHI MAN DUPED OF OVER RS 20 LAKH IN DWARKA, FRAUDSTER ARRESTED

A fraudster lured victims into participating in simple online tasks with the promise of earning a huge amount of money. The victim received a message on his telegram account regarding a part-time job. The accused person had asked to make an account on the alleged website to buy and sell crypto currency. Additionally, some prepaid tasks were assigned to the complainant and as per the instructions of the accused, the complainant invested Rs 20,16,640 in prepaid tasks from November 23 to November 24. The accused people, however, did not turn up and cheated the amount from the complainant.

GANG RUNNIG NATIONWIDE LOAN FRAUD SCHEME, BUSTED!

The victim had received a phone call offering a Rs 2 lakh loan from a reputed bank at a discounted rate. When he opted to take it, the gang asked him for his PAN and Aadhaar cards, and began levying various charges. One after another the victim kept on paying the charges in greed of loan. The accussed kept on asking for the money in name of different fees. After he paid out Rs 1,20,340, the victim realised he had been cheated and went to the police.

RETIRED MECHANICAL ENGINEER IN PUNE LOSES LIFE SAVINGS OF ₹4 CRORE

A 59-yearold retired mechanical engineer in Pune duped of nearly ₹4 crore in an online share trading scam. The fraudsters contacted the victim in October 2023 over the phone with an online share trading offer. They allegedly assured him of huge returns on investments in online share trading.

The fraudsters gained his trust by interacting with him multiple times. As per their instructions, the victim transferred ₹3,95,85,204 from his bank account to various other bank accounts till December 9, 2023

But when he did not get the assured returns, he realized he had been cheated and approached the police

SENIOR CITIZEN FROM BENGALURU LOSES RS 1.2 CRORE AFTER GETTING CALL FROM FAKE TELECOM DEPARTMENT OFFICER.

A 77-year old woman from Bengaluru was swindled out of Rs 1.2 crore by cyber criminals posing as officials from the telecom department and the Mumbai Crime Branch. The scam unfolded over nearly 20 days, impacting the elderly woman mentally and financially, leaving her and her family in distress. The victim received a call from an unidentified person claiming to be a representative of the Telecom Department. The caller alleged that a SIM card had been purchased in her name in Mumbai and was being used for illegal activities. The caller further informed her that, as per protocol, the Telecom Department had filed a complaint with the Mumbai Crime Branch for further investigation.

VIETNAMESE HACKERS TARGET INDIANS WITH FAKE WHATSAPP E-CHALLAN SCAM, STEALING PERSONAL DATA AND FUNDS.

A leading cybersecurity firm, has uncovered a concerning scam involving fake e-challan messages sent via WhatsApp by a Vietnamese hacker group. These scammers target Indian users, attempting to steal personal data and commit financial fraud by tricking recipients into downloading a malicious app. The scammers send messages posing as authorities from Parivahan Sewa or Karnataka Police, issuing fake traffic violation fines. The message includes a link that, when clicked, prompts the download of a malicious APK (Android application package). Once installed, this app requests extensive permissions, such as access to contacts, phone calls, SMS messages, and even the ability to become the default messaging app.

WOMAN FALLS PREY TO CARD ACTIVATION FRAUD, LOSES ₹3.7 LAKH

A 43 year-old victim received a new SBI credit card. On the same day, she was contacted by a person claiming to be a bank official. He offered to help her activate her credit card. “Unaware of such cheating, she revealed the credit card and bank account details to the person over the phone. The accused later said that for completion of credit card activation and its usage, an application named QS Support has to be installed on the mobile phone. As directed, the victim too installed the app and she received messages that ₹3.21 lakhs were debited from her bank account on seven transactions and ₹48,000 taken from her credit card. The app which the complainant installed on her mobile phone was a remote access application. This allowed the fraudster to access the victim’s mobile phone. He obtained all the required passwords and OTPs to complete the transactions.