BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Teacher loses around ₹5 lakhs as he tries to activate bank credit card

A 50-year-old man has allegedly lost close to ₹ 5 lakh to fraudsters who claimed to be credit card customer care executives. The victim downloaded a dubious app – 'Quick Support' – after which he received over 25 messages alerting him that large sums of money were debited against his SBI credit card. browsed for an SBI credit card customer care number and called the first number he found online. The person at the other end introduced himself as an SBI staff member, and told victim that he must download 'Quick Support' app and fill up the details in a form after which his credit card would be activated. He acted on the instructions of the 'SBI staff' and deleted the messages he received from the bank after downloading the app. The fraudsters managed to siphon off the money in a few transactions.

Tracking Blue Dart package, retired bank employee in loses ₹30,000 to cyber fraud

A retired bank employee was duped of ₹30,000 while trying to get an update on the delivery of her Blue Dart package. The victim searched for the Blue Dart customer care number online and called the first number she came across. The person who answered her call told her that the delivery address she had listed was incorrect and asked her to pay ₹2 to fix it. She argued that she would pay the nominal charge once the delivery executive made the delivery. However, the accused demanded that she pay with her debit card. The victim who is a retired Union Bank employee. However, she was tricked into sharing her debit card number and an OTP she had received on her mobile number. In a few minutes, ₹30,000 was withdrawn from her bank account

A man was duped over ₹9 lakhs with 'elite credit card' promise

Initially the group of fraudsters would illegally seek details of the victims from retail stores of high-end cars. One of them would then reach out to the complainant posing as a relationship manager of CitiBank Diners club and offer them a "premium elite credit card". The accused would then promise to facilitate a free-membership of South Mumbai's Wellington Club for their targets in lieu of taking the card. After luring the victims, the frauds would send a link to a form and ask them to fill it. With this, they would obtain their personal details like names, addresses, Aadhaar card and Pan card numbers.

Subsequently, during the conversation, they would gauge whether their prospective victim owned an Android or an iPhone and accordingly, send over a phone under the pretext of completing the authentication process. The victims were further encouraged to insert their SIM cards into the new phone that had been couriered to their house and click on some applications after which the accused would allegedly access all the details, including their bank accounts, through the installed applications such as DOT Secure and SecurEnvoy Authenticator. The accused would then use that money to buy gold coins and iPhones on the victim's name and subsequently, sell them at a cheaper value.

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.

SMS came in the name of SBI and a blow of 8 lakhs

The victim who had his phone number linked with his father's bank account got an SMS with KYC update, which also had a link. When he clicked on that link, an app named SBI YONO was downloaded in his phone. The user already had the SBI YONO app on his phone, but he thought it was a new app. After this he entered his details for KYC update. The user also entered his login credentials in the fake YONO app. Within just 7 minutes, back transactions were done from the user's account. In continuous transactions, an amount of more than Rs 8 lakh was deducted from the user's account .

Cyber fraudster dupes RDO of ₹50k

A cybercrook duped the revenue divisional officer of Anakapalli district to the tune of ₹ 50,000. Police said RDO Chinni Krishnudu received a gift coupon on WhatsApp from an account with the display picture of district collector. The sender also sent a message in the name of collector asking for mone he fell short of funds for purchase of a gift coupon from Amazon. He sent five links each for ₹10,000. Later, the RDO realised that he was cheated.

40-Yr-old man duped of ₹ 1.95 lakh by cyber fraudster while trying courier parcel

A 40-year-old victim was cheated by the cyber crook when he was trying to send a parcel. The victim searched for courier service on the internet and called on the first number he found, reported The Indian Express. The person who received the victim's call sent a link on his mobile phone and asked him to fill in his details. the accused asked Oriya to make a payment of ₹ 5 for confirmation. The fraudster told the victim that he did not receive the payment and asked him to pay ₹5 to the delivery agent who would come to pick up the parcel. However, between two days, Rs 1.95 got deducted from Oriya's account in multiple transactions. The victim got the message that ₹95,000 got debited from his account on on first day and on the next day ₹45,000, ₹50,000 and ₹5,000 were deducted from his account.

Fraud of 6 lakhs on the pretext of car dealership

A victim was cheated ₹5.91 lakh on the pretext of giving a car dealership. The victim has a transport company. He searched the company's website to get the dealership of the car. He got a call after 3 days. Vicious should upload the application on the email id to get the dealership. He uploaded all the information. Again after 3 days, he got a call. Interview was taken on the phone itself to make Karan Singh a dealer. After this he transferred ₹125400 as registration fee and ₹465900 for NOC to his account. When for the third time, he got a message to transfer ₹10.85 lakh more he sensed something fishy and went to the police.