BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

FRAUDSTER IMPERSONATE AS CUSTOMER CARE GUY, USED REMOTE DESKTOP APPS TO LOOT PEOPLE.

The accused used remote desktop apps to take control of his victims' computers. Police found that the accused had siphoned over Rs 1 crore. The accused started putting up fake advertisements on search engine websites in such a way that if a user searched for the official customer care helpline of a particular service provider, web links would redirect to his website. In this way, an unsuspecting airline ticket holder, a professor searched the name of the carrier to avail himself of a cancellation refund.

The user dialled a number given on the website, and the accused represented himself as a customer care representative of the airline. The victim was then asked to download a remote desktop control application to lodge a complaint, but a phishing link was provided to him. The link resembled a bank account details form, similar to those used by banks. Once the victim entered his bank details, the fraudster logged into his netbanking and siphoned off more than Rs 7 lakh.

IN GREED OF MONEY MAN AGREED TO CONVERT TO ANOTHER RELIGION, END UP LOOSING LAKHS.

Investigation revealed that a caller with a fake identity lured the complainant into giving a huge sum money running to about ₹10 crore. For this, he wanted the complainant to convert from Hinduism to another religion. Agreeing to the deal, the caller directed to open an online bank account with an overseas bank. He also claimed that the complainant had to pay certain taxes before receiving the gift money. In the process, the complainant sent sums on various dates totalling to ₹4,88,159 by Gpay to the accused. When there was no response later, he realised that he was being tricked and submitted a petition.

EMPLOYEE SCAMMED OF ₹2.73 LAKH IN CYBER FRAUD SCHEME

The woman, who works as an administrative officer in a company located at Nariman Point, received a call around 10 AM. The caller introduced himself as Pradeep Sawant from the Mumbai Cyber Branch. The scammer further stated that it was found in his investigation that on January 15, an account was opened at Andheri East ICICI Bank with the victim's Aadhaar card number. Similarly, the Aadhaar card has been used to open several accounts across the country. Afterwards, the scammer gave the woman an account number and asked her to transfer money into it. The scammer mentioned the name Mohammad Ismail Malik and sent his photo to the victim's WhatsApp, asking if she recognized him, to which the woman denied.

A police officer revealed that the accused informed the victim woman that this man is trapped in a drugs case and has used your Aadhaar card in the bank account, so your bank account needs to be investigated. The accused told the victim to transfer her money into an account, assuring her that after a thorough investigation, her money would be returned. In this way, the woman transferred Rs. 2.73 lakh. Afterward, she was informed that even after returning home, the Skype account should not be closed. On the second day, the woman tried to contact the same Skype ID again, but the number was switched off.

THUGS IMPERSONATED AS RTO OFFICIALS, DUPED PEOPLE ON THE PRETEXT OF PROVIDING DUPLICATE NOC

A victim had sent a request to the RTO requesting to issue duplicate NOC of his vehicle.

Subsequently, he received a call from an unknown person who impersonated as a working clerk in RTO, he told him that he can help him. The accused duped ₹ 7,500 from him as NOC cancellation fees. After some time, the complainant received another call from another person who impersonated as RTO inspector and defrauded the complainant of ₹ 43,300 on the pretext of issuing a duplicate NOC.

After taking the money none of them answered the calls of the complainant. The scammers planned to dupe innocent people by impersonating themselves as RTO agents, they created a profile on a website in the name of the RTO office to cheat people.

CYBER FRAUDSTERS, POSING AS POLICE AND CBI OFFICIALS, SCAM RETIRED DIRECTOR OF MNC WITH RS 25 CRORE

The victim, received a WhatsApp call with the caller posing as an official of the telecom department, who told her that her three mobile numbers will be deactivated. When the victim, who is a senior citizen, sought to know the reason, the caller told her that he was connecting the call to a police officer . Following this, another man posing as a police officer talked to her and said that they had received a money laundering complaint against her and her mobile numbers and Aadhaar card were found linked to the case. The caller then transferred the call to another person, who posed as a CBI officer and threatened her with the money laundering case.

The caller told her that if she wanted to get out of the case, she should deposit money into the bank accounts provided by him and assured that she will get her money back. The fraudsters opened a current account in her name and asked her to deposit the demanded amount, assuring her that the money would be sent to the Reserve Bank of India (RBI). The caller also asked her to collect the receipt of the payment from the local police station. Falling into the trap, the victim transferred around Rs 25 crore to the account and got scammed.

A MAN DUPED OF 46L BY GANG OF 4 WHO POSED AS CYBER POLICE

A Nerul resident has been defrauded of Rs 46 lakh by a four-member gang of cyber fraudsters. The accused posed as Mumbai cyber crime officials and contacted him over. They claimed that there was a case of money laundering and drugs registered against him. They threatened him stating that legal action would be taken against him and was asked to furnish details about his bank account. They made him transfer Rs 46 lakh between April 10 and 15 to different bank accounts. After the victim realized that he was cheated by cyber fraudsters, he registered an FIR with Navi Mumbai.