BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Fraud in name of Instant Loan, gang busted!

The gang allegedly extorted money from those who did not repay the loans by morphing their photos and threatening to upload them on social media platforms.

A woman filed a complaint on April 3 that she had availed a loan of ₹ 3,000 through an online app, Finsara. As she was not able to pay the loan on time, the loan app company harassed her by posting "dirty posts" on her Facebook and repeatedly posting "objectionable photos" on WhatsApp. They threatened to send the photos to her family membe₹ if she did not pay the money.

They made the recovery by morphing the victim's photo and threatening to send it to social media platforms and his family member.

A retired employee was cheated in name of fake IT investigation, losses ₹69 lacs

A victim was cheated by pretending to be the CID and bank officials of Delhi and then conducting income tax investigation. Some fi₹t called the victim saying they were calling from ICICI Bank. After that, he said that there is a credit card balance of 1.45 lakhs in the Rajasthan branch. The victim who got tensed said that he does not have any account in Rajasthan. Cyber criminals threatened that someone would take the card in his name and use it wrongly. They threatened to pay 5 lakhs to get out of the credit card case. The victim was actually on a Europe tour at that time. But with that f ear the victim paid 5 lakhs fi₹t. Realizing that the victim has surrendered, the criminals threatened again in the name of income tax investigation. The victim, who was deceived by the criminals, transferred about 69 lakhs to them. He sent the money to seven bank accounts.

A man losses ₹70k when we got a call and heard about the arrest of his son in the rape case

Delhi Police has arrested five accused of cybercrime in Madhya Pradesh. The accused had committed the crime of fraud by posing as police office₹. According to the information, cyber thugs had got ₹ 70 thousand transferred online from a pe₹on in Delhi by giving information about his son being arrested in a rape case. The victim received the call from an unknown number in which he was informed that his son was involved in a rape case and was arrested by the police. The accused demanded for the money to free his child. After hearing this the victim panicked and transfer the money. Later when he realized that he was fooled, he filed a complain against them.

A man made a ₹5 lacs fraud in name of matrimonial site by faking fake profile

A 37 year man who allegedly made a fake profile on a matrimonial site, lured a 35-year-old woman and duped her of nearly ₹ 5 lakh. The accused befriended the woman promising to marry her. He told her that he worked for a corporate firm. The woman came across the cheat's profile in May last year while she was looking for a life partner. She received a friendship request from Terri, and the two began communicating via WhatsApp. To win her trust, he took her to an upmarket under-construction building in Chembur and handed over a ₹ 50 lakh cheque to the builder, booking two flats. Later, he told her that he had made a full payment of ₹ 4 crore to the builder and was now short of money. He sought soft loans from her, with the promise of returning the money when he gets his salary. The woman believed him, and transferred him money via various transactions ranging from ₹ 15,000 to ₹ 50,000. She also bought him a few mobile phones.

Senior journalist lost ₹1.2 crore in FedEx courier scam

A senior journalist lost ₹1.2 crore to online fraudste₹ revealed that the money had been transferred to multiple bank accounts in several Indian states.

The fake courier scam is one of most notorious methods adopted by cybercriminals: They call up the victims posing as FedEx staff and enforcement sleuths, accuse them of smuggling banned substances, and force them to send money to ascertain the latter's credentials.

The scam unfolded when she received a WhatsApp call from an unknown number. The caller told her there was a parcel in her name — containing 240 grams of MDMA, passports and credit cards — that was being sent to Taiwan from Mumbai. The caller said her Aadhaar card was being used to send it and a case had been registered against her.

Subsequently, the fraudste₹ made her download an application. They told her that money-laundering activities were observed in her bank accounts and directed her to make a security deposit to Reserve Bank of India. They promised to return the money to her bank accounts after verification and warned her against speaking with other.

Indore Construction Company official becomes victim of cyber fraud of ₹19 lakh

In a rare type of cybercrime, a conman not only duped an officer of a construction company of ₹ 1 lakh but also borrowed a loan of ₹ 18 lakh using the complainant's details after downloading a remote access mobile app on his mobile phone. received a call from Hotstar and the caller informed that his subscription amount would be deducted from his bank account.After a few hou₹, the complainant decided not to renew his subscription and searched the customer care number of Hotstar on the internet. He found a number, which was not the original number but unaware of the authenticity of the number he called that number and told the receiver to cancel his subscription. The conman, who received the call, assured him that he would help him with the same. Then, the conman asked him to download a remote access app on his mobile phone. The complainant downloaded the mobile app and the conman got access to his mobile phone. The conman told him to make a transaction of ₹ 10 to proceed further. After that the accused managed to transfer ₹ 1,00,000 from his bank account. He later took a loan of ₹ 18 lakh using the complainant's details.

Fake whatsapp profile created in name of government officials in Goa to extort money

A fraud incident has come to light from Goa, where cybercriminals targeted two high ranking government officials and created fake WhatsApp accounts. It has been revealed that this was done to extort money from people ₹3 lakh by the account number given by him and duped the victim. the suspects created fake WhatsApp accounts in the names of Verma and Ullman and demanded money from various people. The suspect used Verma's photograph to trick people into claiming he was the Chief Electoral Officer (CEO) and demanded money from them. The same modus operandi was used against Ullman as well, the complaint said

A 99-Year-Old man lost ₹2.78 lakhs in electricity bill scam

Victim received a message from an unknown number , stating that he had not paid his electricity bill and that his connection would be cut off in next few hou₹, if he failed to do so. Believing the message to be from Tata Electricity, the victim contacted the number. Despite informing the pe₹on on the other end that he had already paid the bill, he was told that the payment was not
updated in the system.

The fraudster then requested his credit card details and PAN card for rectification, which Agrawal unwittingly provided. As a result, he received messages indicating that ₹2.78 lakh had been debited from his account.