BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Police Dismantle International SIM Cartel Providing Indian SIMs to Online Gangs

More than 20,000 SIM cards were falsely activated by the accused, who then sold them to hackers in South Asia and used them in extensive financial scams throughout India. The criminal enticed women with freebies under disguise of fake government initiatives or businesses. He obtained their Aadhaar cards and biometric information in return for a basic cup set; they were subsequently used to activate thousands of SIM cards under false pretences. These phony SIM cards were sold by the defendant to local cybercriminals. Through WhatsApp OTP groups controlled by hackers, he allegedly distributed the SIM cards, charging INR 3 to INR 50 for each OTP use. After activating WhatsApp and other apps on the SIM cards, these gangs utilized them to conduct cyberfraud operations against unsuspecting individuals. The SIM cards were destroyed after use to remove any evidence of his illicit activity.

The trail goes overseas; rented bank accounts are sold for commission to foreign–based cybercriminals.

Foreign–based cybercriminals have developed a new scheme to defraud individuals. Their local handlers approach the less fortunate and less literate people to ask about their bank rent accounts. After that, they transfer funds acquired by enters such accounts through cyberfraud. Subsequently, the handlers offer their clients the leased bank accounts for international kingpins. After the handlers effectively move the funds to their foreign kingpins, they give the bank back reports to their legitimate owners, providing offering them a commission of 15%–20% in return for same.

Hotel worker loses ₹81,000 after being tricked by cyber fraud

The victim went to the Wilson Garden ATM of Karnataka Bank to take out ₹25,000. He performed two transactions of ₹5,000 and ₹20,000 but the second transaction was unsuccessful, and he did not obtain the money even though it was debited from his account. Fearing for his life, the victim went to the bank and complained, and the bank promised to return the money to his account in 48 hours. The victim got a call from an unknown number a few hours later. The caller identified himself as a bank customer service representative and promised to assist him in getting his money back. The victim followed the directions and shared the OTP when the accused sent him a link to download the program. As soon as the OTP was shared, the accused transferred the entire amount online and switched off the phone.

Industrialist duped of Rs 7 crore by cyber criminals

The Industrialist Group owner was defrauded by scammers who took out Rs 7 crore from the industrialist's numerous bank accounts. One of them identified himself as a CBI agent, threatened to place the industrialist under virtual arrest, and produced a fictitious arrest warrant. The con artist demanded money from him in order to let him off free of charge.

Govt doctor falls victim to ₹39-lakh cyber fraud

The victim told police that the fraud began on June 24, when he, while on duty in the Medicine-1 OPD, received a call from an individual. The caller claimed that his Aadhaar-linked SIM card was involved in illegal activities and linked to terrorist operations. The victim alleged he was transferred to a purported police station over video call, where a man introduced himself as ADC of police and ED officer. The fake ED official claimed that he could face 5-7 years of imprisonment unless he cooperated by transferring funds, allegedly for RBI audits and investigations. The scammers used forged letters bearing the logos of Reserve Bank of India and Central Bureau of Investigation to demand various payments over several weeks. Under the threat of imprisonment, the doctor said he was coerced into transferring a total of ₹39.70 lakh across multiple transactions through SBI and HDFC bank accounts. The victim's father, an eye surgeon and HOD, was also targeted, with scammers falsely claiming that his son was in police custody and extracting around ₹12 lakh from him.

Woman doctor at Hospital duped of Rs 25 lakh by cyber fraudsters posing as police officers

The fraudsters threatened the 62-year-old doctor saying they are investigating a case of "human trafficking and money laundering" lodged against her. An FIR in the online defrauding case was lodged at the Cyber police station on September 22. An unidentified person claiming to be a telecommunication company staffer called her on WhatsApp on September 16, 2024, saying her mobile phone number would be deactivated in the next two hours. When she asked the reason for the purported move, her call was connected to another person posing as police officer. He shared a document on WhatsApp claiming that it was an 'arrest warrant' issued against her by a court in connection with a financial fraud complaint. Then, within some time, the victim received a WhatsApp call from a person claiming to be a CBI officer, who took details of the balance in her bank accounts for "investigation". The next day, the person posing as a CBI officer again called the victim and shared a bank account number. He asked the victim to transfer Rs 25 lakh to the bank account for investigation purposes. The police said the victim transferred Rs 25 lakh through the RTGS mode, as she was assured that the money would be returned after the investigation was over. But the fake CBI officer demanded more money from her. So, she felt suspicious and filed a complaint at the Cyber police station.

₹30 lakh was stolen from a woman by cybercriminals posing as telecom representatives.

As per the complainant, on September 2, she received a video call from an unknown number. The caller said he is from TRAI and was calling regarding a mobile number that was used for illegal activities and that SIM card was taken using my Aadhaar card. He told the victim that she needs to lodge a complaint, and for that he transferred the call to a person dressed in a police uniform. The person sent the victim, the documents on WhatsApp on letterheads of Central Bureau of Investigation (CBI) and TRAI addressed to the victim, alleging that the victim have been involved in money laundering.

A student fell victim to cybercrime and was defrauded of INR 18 lakhs.

A BCA student opened an account in SBI for scholarship. The victim told the police that on April 21, 2024, he received a call from an unknown number. The caller promised to earn a good amount of money by joining his business. When the student told this to his father, he refused. But the student remained adamant. On this, his father sent his hard-earned money as well as borrowed money from relatives and acquaintances to his son's account.