BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

J&K terror link used as pretext in to scam ₹ 13 lakh

YOUR BANK account is linked to terror activities in Jammu and Kashmir," was a message a 47-year-old resident received by a man posing to be an IPS officer. The victim received an Interactive Voice Response (Automated call) call. After she responded to it, she was told by a person posing as an executive of a courier company that in a parcel sent by her to Taiwan, MDMA drugs had been seized and that an FIR had been registered at 'Narcotics Department' in Mumbai.

She was told that she will have to come to Mumbai for an investigation. When she said that she had not sent any parcel, she was told to complete a procedure over a video call. She was made to download a video calling application and received a call from a profile with a display picture reading 'Mumbai Narcotics Department.' A person identified himself with the name of a serving IPS officer from Maharashtra and even showed his identity card. She was asked to send a copy of her Aadhar card and bank details.

The man told her that her account was showing links to some suspects in Jammu and Kashmir and was told that it was being used for terror activities there. Over next five days she was made to make four large transfers totaling ₹13.7 lakh on the pretext of completing false legal formalities and financial obligations in connection to the FIR.

Cyber criminal posed as CBI officials and cheated 50 lakhs

The victim alleged an unidentified person called him over the phone and claimed that he was a CBI officer from Delhi. The caller told victim that he had frequently shared whatsapp messages abusing women on his mobile phone and also had nexus with those who were arrested in money laundering cases. He told him that he would have to face enquiry and invited him to connect through Skype under the pretext of enquiry. The caller asked him to transfer ₹50 lakh to a bank account to get exonerated from the case. Panic- stricken victim had transferred the money as demanded by the caller. Later he realized that he was duped by the caller.

IT Engineer falls victim to cybercrime, lost 13 lakhs

The victim was currently without a job back then and was looking for a job. He therefore applied for a job-based in New Zealand on an online website. The fraudster then asked for money from the victim from time to time. The fraudster took money saying that the money was needed for several formalities for the victim to come to New Zealand such as visa, passport, character certificate verification, etc. The fraudster took money from the victim for straight 25 days and took a total of 13 Lakhs

‘Beware of juice-jacking’: USB charger scam

USB charging ports at public places are being misused by cyber criminals for malicious activities. “Cyber-criminals may use USB charging ports installed at public places like airports, cafés, hotels and bus stands for malicious activities. Charging your electronic device at such infected USB charging stations may make you a victim of juice-jacking cyber attack.

Cyber criminals through juice jacking, can install malicious apps; encrypt devices and demand ransom to restore data and they could even steal data from devices. The agency advised the public to be cautious while using public charging stations or portable wall chargers. It also advised the public to use electrical wall outlets for charging mobile devices and carrying personal cable and power bank. Lock your mobile device and disable pairing with a connected device. Try to charge your phone when it is in switched off state.

Cyber thugs create fake websites of Manali hotels to dupe tourists

Cyber fraudsters are doing fraudulent online booking of hotels in Kullu and Manali and they are defrauding tourists by creating fake websites. On reaching hotels, tourists come to know that there is no booking in their name. The police have appealed to tourists to remain alert regarding the fraud.

They charge customers a fee using various online methods and the hotels concerned are not even aware about it. Manali being a popular tourist destination witnesses a huge footfall throughout the year. To avoid inconvenience, most people prefer to book hotels in advance, usually online. In view of this rising trend, cybercriminals have become active and are cheating tourists by creating fake websites.

SIM card fraud

The fraud started unfolding with the victim receiving a text message that his SIM card would be deactivated in four hours. The fraudsters reportedly convinced him that the SIM card had been taken using his Aadhaar credentials.

A person, allegedly part of the racket, got in touch with the man over Skype and showed some fake notices and documents. He was asked to pay money to get the case frozen and told that it would be refunded later.

The man then paid ₹1.15 crore to five different bank accounts in six lots. When he was asked to pay money again, the man realized that he was being taken for a ride & fallen for scammers.

A 77-year-old physician lost 3 lakhs in fake electricity bill scam: What it is and how you can stay safe

A 77-year-old physician recently became a victim of an online scam, resulting in a loss of approximately Rs 3 lakh. The scam involved an individual posing as a representative from the electricity provider, who specifically targeted the elderly doctor by alleging outstanding bills.

The doctor received a threatening message from an unfamiliar number claiming to represent BSES.

The message warned of immediate disconnection of power unless overdue bills were settled on the same day. Feeling pressured, the doctor dialed the provided number and was coerced into paying Rs 10 under the guise of an upgrade. Subsequently, he was directed to click on a link where he inadvertently disclosed his debit card details.