BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Beware of housing portal scam

The victim said that he was looking for houses on rent on heavy deposit basis in the. He saw an advertisement on the portal by one of the service agency. He contacted the person whose number had been mentioned in the advertisement. A person responded to him and claimed to be an estate agent. He then sent him photographs of houses.

After the complainant selected a particular flat, the other accused pretending to be the homeowner asked him to make a payment in various bank accounts. The complainant ended up paying ₹22.31 lakh to various accounts after which the 'broker' and "flat owner" stopped responding to him. Realizing he had been duped, he approached the police and the North region cyber unit started probing the matter.

Promised "High Paying" jobs

Over 25 Indians were lured with "high-paying" jobs in foreign but taken to somewhere else, where they were forced to commit cyber fraud.

Victim told he flew in December 2022 hoping to earn good money but was taken to a place in somewhere else. Accused allegedly made victim and about two dozen Indians work in call centres that scammed people in Europe, the US and Canada through fake social media accounts, the official said.

The call centers imposed hefty fines on employees citing flimsy reasons. The complainant said he and three others were thrashed by the accused when they approached the Indian embassy for their return. After the intervention by the Indian embassy, the local police rescued the youngsters.

Over 100 tourists duped in online hotel booking scam

Scammers tricked tourists by making fake websites in the names of various hotels. They attracted victims by promising appealing discounts on travel packages and sightseeing. These fraudsters also created fake booking apps and websites for hotels that don't exist. Legitimate sea-view rooms in hotels typically cost between ₹4,000 to ₹10,000 per day, as per the report. The scammers, however, claim to offer rooms at lower prices, ranging from ₹2,000 to ₹4,000.

A victim found a hotel booking website offering a sea-facing room for ₹3,000 per day. They booked a room for November 2nd to 7th and were asked to pay ₹8,000 in advance on a payment platform. However, after arriving, they discovered that the hotel didn't actually exist. Another tourist was also searching online for a hotel. The victim reserved two rooms for November 3rd and paid an advance of ₹5,000. However, when victim tried to check in with his family, the hotel informed him that they had not accepted any such booking.

When he showed them the online transaction information, it became clear that the recipient's account was linked to cyber criminals.

Powered by GRAMAX CYBERSEC

How a woman lost ₹77,000 while returning spoilt milk to online grocery platform

A 65-year-old woman, found herself ensnared in an online scam while attempting to return spoilt milk purchased through an online grocery platform. The incident, resulted in victim losing a significant sum of ₹77,000 to a fraudulent scheme.

Resorting to the internet for assistance, victim attempted to contact the customer care service of the grocery platform. Upon dialing a number retrieved from her online search, she was met with an individual claiming to be a representative of the grocery platform.

Assuring her of a refund, the imposter guided victim through a series of steps, ultimately coercing her into divulging sensitive information, including her UPI PIN. received a WhatsApp message containing a purported UPI ID number "081958." Following the scammer's directives, she proceeded to initiate a transfer using her digital payment app, unaware of the deceit unfolding. Manipulating her actions, the fraudster orchestrated a sequence that led victim to enter her UPI PIN, resulting in a direct debit from her account.

Prowling on matrimonial websites

A notorious offender, who prowled on matrimonial websites and cheated women by promising to marry them and making off with their money. It's a estimate that he has pocketed ₹2.71 crore from one victim.

The accused, has been involved in a series of matrimonial frauds, targeting victims by creating fake profiles and deceiving them with promises of marriage and opportunities abroad. A 30-year-old woman filed a complaint stating that, she had connected with the profile of one victim on a matrimony app.

Claiming to be a US-based assistant director at Glenmark Pharma, he misled the victim into believing that she needed to increase her Cibil score to process a US partner visa. He convinced her to take out loans from various sources, including personal loans and credit cards, to boost her Cibil score.

Additionally, he roped in the victim's cousin, promising her a job at Microsoft in Australia. Subsequently, the accused and his team, manipulated the victim's cousin into taking loans, resulting in financial losses for both the victims to the tune of ₹2,71,79,044.

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.

Powered by
GRAMAX
CYBERSEC