

BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead



Woman loses Rs 1.94 lakh in scam after clicking on an Instagram link offering job at Amazon

After clicking on an Instagram job posting, the victim was sent to a WhatsApp group where con artists offered her large payouts for easy online work. Initially, she received small payments to build trust. However, the scammers convinced her to invest a larger sum, promising even higher returns. She transferred Rs 1.94 lakh to various UPI IDs between October 18 and 24. When she tried to withdraw her earnings, she realized she had been scammed. The scammers had disappeared, leaving her with significant financial loss. It's crucial to be cautious of such offers and verify the authenticity of any online opportunity before investing money or personal information.

Former TISS principal defrauded in 'digital arrest' cyber fraud

The complainant received a call from an unknown person on November 13. The caller claimed to be an executive from the State Bank of India (SBI). He told the complainant that there were dues against her SBI credit card, to which she responded that she doesn't have an SBI credit card. The 'SBI executive' then told her that her complaint had been taken and transferred to the police station, and she would soon get a call from them. After 30 minutes, the elderly got a call from a purported police officer who took the complainant's Aadhaar card details. Later, the former TISS principal received a call from one man claiming to be a CBI officer, who informed her that her Aadhaar number was used to open a bank account for transferring black money and the manager of the said bank had also been arrested.

Indian boys trapped in cyber fraud cells beaten up, given electric shocks

22-year-old boy was lured to Southeast Asia under the pretext of a job in a call centre. He is now trapped in a cyber-fraud centre in Meghalaya, facing torture and abuse. His two friends were also lured in the same scam, have returned to India, but Ajay remains captive due to his family's inability to pay the ransom demanded for his release. The family seeks help desperately from authorities to bring the captive back safely.

Company owned by a Minister was duped of Rs 2.08 Crores through cyber frauds

An accountant of a company owned by cabinet minister was allegedly duped of Rs 2.08 crores by cyber frauds, said the police on Saturday. The victim works for ABC company, owned by the minister and managed by his son. According to the complaint, the victim received a WhatsApp message on November 13 from a number displaying the minister's son's profile photo. The sender claimed it was a new number and sought sensitive financial information related to a proposed business meeting, the complainant said. Believing the message to be genuine, the victim shared the company's account details on that number following the instructions of the company's director.

Cyber Police Bust 'Digital Arrest' Fraud Gang

As per the information, a 76-year-old retired government officer lodged a complaint with the state Cybercrime Division that some people claiming to be from the Cyber Crime had duped him of ₹ 76 lakh by putting him under digital arrest via WhatsApp call. The caller accused the victim of plotting with a criminal who indulged in money laundering and claimed that a subpoena had been issued in his name by the High Court. The fraud caller impersonating a police official from the cybercrime gave him account numbers from different banks and directed him to deposit money in the said banks to clear him of the charges. As directed, the victim deposited ₹ 76 lakh in different bank accounts.

Con Man Posing as Buyer, Dupes 200 on OLX

The accused would pose as a potential buyer on the platform, agreeing to the seller's price without negotiation. Then, he would repost the same phone at a lower price and direct buyers to the original seller. Once the buyer made the payment through UPI, he would block both the buyer and the seller. The total amount defrauded is estimated to be around Rs 60 lakh.

