PRESS RELEASE

12-11-2025

ED ATTACHES ASSETS WORTH Rs. 21.71 CRORE IN COINBASE PHISHING SCAM

Directorate of Enforcement, Headquarters Office, New Delhi has issued a Provisional Attachment Order on 12.11.2025 attaching assets valued at Rs. 21.71 Crore belonging to Chirag Tomar, his family members, and his associates named Rahul Anand, Akash Vaish and Piyush Prashar. The provisionally attached assets include 9 immovable properties in Delhi.

ED initiated investigation on the basis of newspaper report that an Indian National named Chirag Tomar was arrested in USA for stealing more than $20 million through use of fake or spoofed websites mimicking the cryptocurrency exchange website Coinbase. The investigation revealed that Chirag Tomar, currently in custody in USA, was involved in a large-scale cyber fraud by spoofing the website of the cryptocurrency exchange “Coinbase” and stealing cryptocurrency.

ED investigation revealed that the trusted websites were spoofed in such a way by search engine optimization that when the website would be searched, the spoofed website would appear at the top. The spoofed website appeared exactly similar to the trusted website except the contact details. When the users would enter the login credentials, the spoofed website would show it wrong.

Therefore, the users would contact the number given in the spoofed website which would eventually connect them to the calls managed by Chirag Tomar and his associates. Once the fraudsters gained access to the victim’s accounts, the fraudsters quickly transferred the victim’s cryptocurrency holdings to crypto currency wallets under their control. The stolen crypto currency would then be sold on various P2P crypto platforms and converted to INR.

Subsequently the money was transferred in the bank accounts of Chirag Tomar, his family members and his associates accounts and used to buy immovable properties. Chirag Tomar was arrested by USA authorities while entering USA in December 2023.

ED cautions citizens to remain vigilant against phishing scams and fraudulent communications. Such scams aim to steal personal and financial information through fake

websites, emails, messages or calls. The common signs of a spoofed (fake or fraudulent) website, which can help identify and avoid scams are as under: -

1. The web address looks similar to an official site but contains extra letters, symbols, or spelling errors.
2. Legitimate websites use secure connections (https://). Spoofed sites often use http:// or show “Not Secure.”
3. Fake sites may have low-quality images, blurry logos, mismatched fonts, or irregular page layouts.
4. Pop-ups asking you to download software, share information, or click on links are a red flag.
5. Official websites never ask for passwords, OTPs, bank details, or Aadhaar numbers through pop-up forms or emails.
6. Internal links on the website does not work, or some pages redirect to unrelated or suspicious sites.
7. Offers or claims that seem unusually generous or urgent (e.g., “Get free benefits” or “Claim now” or “Get High Returns”) are common phishing tactics.

Citizens are advised **not to click on unknown links**, **not to share OTPs, passwords, or bank details**, and to **verify the authenticity** of any communication before responding. The ED urges all citizens to stay alert and safeguard their personal information to prevent fraud.

The total attachment in the case so far stands at Rs. 64.15 Crore. Further investigation is under progress.