

Akshat Khetan, Cyber Legal Expert and Founder of AU Corporate Advisory and Legal Services, emphasizes the need for a digitally empowered society and robust cybersecurity frameworks to tackle the rising threats of frauds and scams in the digital era.

MUMBAI | MONDAY, 23 DEC 2024

Fraudsters on the prowl

■ Two kinds of cyber frauds that surged in 2024 — investment frauds and task job frauds

■ In 2022 and 2023, investment frauds or share trading frauds worth Rs 3.87 crore and Rs 7.76 crore respectively were reported at 5 cyber police stations. This year till June month Rs 191 crore worth investment frauds were reported, reveals RTI data.

■ Groups from other states target those who have newly started stock market investing or trading. Data of such vulnerable individuals are collected by floating advertisements or social media posts

■ 15-20% victims of share trading frauds reported to cyber police stations are chartered accountants, leading bank managers, doctors, professors, serving and retired IAS, IPS and IRS officers, lawyers, etc.

■ Job frauds or task frauds worth Rs 1.23 crore and Rs 40.77 crore were reported at 5 cyber police stations in 2022 and 2023, respectively. In 2024, till June month job frauds worth Rs 36.89 crore were reported

■ Most of the job frauds reported were task job frauds, by defrauding people through "work from home" advertisements

■ Digital arrest cyber fraud cases are surging in metro and tier two cities, prompting Prime Minister Narendra Modi to warn citizens against it

■ Fraudsters operate from Rajasthan to Cambodia, Haryana to Indonesia, police say

■ A cyber police officer said that cyber crime cases involving below Rs 15-20 lakh committed by gangs spread in Rajasthan (Bharatpur), Nuh/Mewat (Haryana), Jharkhand, West Bengal, etc., are generally

through KYC update, task job frauds, power bill non-payment, ATM card suspension, UPI payments fraud, etc.

— Frauds involving huge amounts are through digital arrests, investment/share trading frauds, etc., by professional gangs operating from Cambodia, Indonesia, Myanmar, Dubai and Ajman, along with a few Indian groups. Call centres by international groups, controlled and operated by suspected Chinese nationals, force Indians, Pakistani, Bangladeshi individuals into carrying out cyber frauds in India, police say.

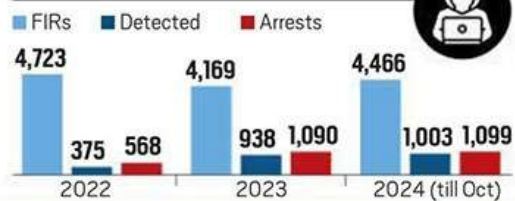
■ A senior police officer said fraudsters use internet based calls and Virtual Private Network (VPN) to target people, making it difficult to trace them. Since mule bank accounts are used in the fraud, the money trail ends after a point.

■ To dodge law enforcement agencies and vigilance of banking channels, fraud gangs use hawala operators to transfer money in US dollars in an eWallet. They convert money into USD to send it abroad by paying the taxes. Once the money crosses borders, it is gone.

■ A cyber police inspector said that the responsibility also lies on the securities company whose names are misused on digital space for duping people. These companies should identify gangs impersonating their platforms and report them.

— After Covid-induced lockdown, investments in stock market, SIP-mutual funds and insurance, along with work from home culture gained popularity. Fraudsters saw big opportunity are taking advantage of two "weaknesses" of human behavior — greed and fear — police say.

CYBER CRIME CASES IN MUMBAI



COMPLAINTS RECEIVED ON 1930 CYBER CRIME HELPLINE (DATA FOR 2023 & 2024)

Year	Registered Calls	Fraud Amount	Put on Hold
2023	91,357	₹262.51 cr	₹25.36 cr
2024*	5,03,545	₹1,181.43 cr	₹139.15 cr

(*Till November)

'BE AWARE, ALERT'

Cyber criminals and victims are spread all over the world. It's almost impossible now to catch the criminals since they operate without borders. There are no international protocols in place between countries for cooperation and coordination yet. The government is issuing public awareness advertisements. But the number of crimes and the loss are growing day by day. The only way is to educate people. Think, pause and act is the only way to stop the crimes.

D SIVANANDHAN,
FORMER MAHARASHTRA DGP

Citizens must remain alert and vigilant. They should not fear fraudsters impersonating law enforcement officers, as there is no concept of digital arrest or detention

in our legal framework. Instead of panicking, people are advised to approach police.

DATTA NALAWDE,
DCP CYBER

People should stay composed as scammers rely on anxiety and desperation. Around 6,000 complaints are reported daily on the National Cyber Crime Reporting portal with an average Rs 60 crore loss reported daily. Also, 1930 helpline received 60,000 calls daily, 3,700 fraud accounts reported per day and 35 per cent of reported amounts more than Rs 50 lakh. As India moves towards a digitally empowered society, the risks posed must not be ignored.

AKSHAT KHETAN,
CYBER LEGAL EXPERT AND
FOUNDER OF AU CORPORATE
ADVISORY AND LEGAL SERVICES