Understanding money mule scam: What it is and how to stay safe from this bank account fraud

Amid rising mule account fraud in India, experts emphasise vigilance and proactive reporting to combat fraudulent schemes and safeguard bank accounts from exploitation.

A recent cyber cell investigation in Pune has uncovered a ₹4 crore online share trading scam, exposing a network of fraudulent online trading applications, money mule accounts, and the use of cryptocurrency channels to funnel funds to Hong Kong.

This revelation, though alarming, is not an isolated incident, as similar cases have surfaced in the past.

The rise of mule account fraud in India has been mentioned in the '2024 Digital Banking Fraud Trends in India' report by BioCatch, a leading digital fraud detection company.

Understanding mule account fraud

In simple terms, a mule account is a bank account that's deceitfully used by criminals to transfer illegally obtained money.

As explained by Dhiren V Dedhia, Head of Enterprise Solutions at CrossFraud, these individuals, termed

as money mules, serve as conduits for transferring funds.

"In order to circumvent regulatory restrictions, fraudsters exploit mule accounts to funnel money through Indian payment instruments, including bank accounts, credit cards, and digital wallets," Amit Relan, Co-Founder and CEO of mFilterIt told CNBC-TV18.

The person who owns the account, called a "money mule," may not realise they're involved in illegal activity. They receive funds into their account and then transfer them elsewhere, making it harder for authorities to trace the illegal transactions.

The modus operandi of fraudsters

Shikhar Aggarwal, Chairman of BLS E-Services, sheds light on the tactics employed by fraudsters to ensnare unsuspecting individuals into becoming money mules.

"Through electronic channels such as emails and social media, fraudsters lure victims with promises of lucrative incentives or commissions, thereby coercing them into facilitating illegal transactions," he said.

Vinod Nair, President of Noventiq India, stressed on the strategies employed by fraudsters, ranging from phishing attacks and business email compromise to ransomware and internal fraud.

Phishing and spear phishing attacks: Scammers send emails or messages that appear to be from a legitimate source, such as a bank or a known vendor, asking for sensitive information. Spear phishing is more targeted, aiming at specific individuals within an organisation.

Business Email Compromise (BEC): In these scams, fraudsters hack or spoof company email accounts to impersonate executives, managers, or suppliers. They might instruct employees to transfer funds or send sensitive data, exploiting the trust and authority of the purported sender.

This type of malware attack involves infiltrating a business's systems to encrypt files and data, rendering them inaccessible. The attackers then demand a ransom for the decryption key. These attacks can cripple operations and lead to significant financial losses.

Invoice fraud: Scammers might send fake invoices that appear to be from regular suppliers but with altered payment details. Unsuspecting employees might pay these without verifying, leading to financial loss.

Internal Fraud: Sometimes, the threat comes from within. Employees may exploit their access to confidential information or financial systems for personal gain.

The aftermath of fraudulent schemes

Once armed with personal or financial data obtained from victims, fraudsters exploit it for a myriad of nefarious activities, as articulated by Dedhia.

From identity theft to unauthorised transactions and involvement in mule account fraud, the ramifications of such schemes are far-reaching, exacerbating the vulnerability of individuals and organizations alike.

Safeguarding against fraudulent exploits

To mitigate the risks posed by mule account fraud, proactive measures are imperative.

Relan stressed on the significance of vigilance in scrutinising payment requests and avoiding engagement with dubious schemes.

"Avoid visiting illicit or untrustworthy websites, especially those related to gambling, gaming, or adult content. These sites may be fronts for mule account fraud or other illegal activities. Also, be cautious of job offers or opportunities that involve handling money transfers or payments on behalf of others. These could be schemes to use the account as a mule account for fraudulent activities," he told CNBC-TV18.com.

Additionally, proactive reporting of suspicious activities to relevant authorities is crucial in curbing the proliferation of mule account fraud.

Vishal Salvi, CEO at Quick Heal Technologies Limited emphasised the need to protect one's bank account from being ensnared in a mule account scam.

He stressed the importance of being cautious of unsolicited requests, especially those offering cash or transfers in exchange for a commission.

Engaging in such activities could unwittingly make one complicit in illegal actions, leading to severe legal consequences if caught.

In the event of a compromised account or any suspicion of fraudulent activity, immediate action is crucial. Individuals should report any such incidents to their bank and relevant law enforcement authorities to mitigate further risk and aid in the investigation.