THE HINDU businessline.

Crypto heist: Why passwords remain the Achilles' Heel

Despite blockchain's promise, human vulnerabilities continue to plague crypto security.

Experts noted that lack of standardised safeguards further jeopardises the security of the crypto ecosystem | Photo Credit: REUTERS

The $44 million heist at CoinDCX has raised concerns over the safety of crypto assets, leaving investors perplexed about this asset class – which is supposed to be the safest – considering the extra layer of security in the form of blockchain. But the weakest link is as old as the first cybersecurity attack – stolen credentials using social engineering techniques.

Phishing and social engineering tactics are rampant across platforms, with stolen credentials being the single biggest risk for investors.

"People often get tricked into authorising rogue signatures or sharing seed phrases on fake sites. Deep-faked support calls and AI-driven romance scams add to the psychological pressure. So, the defence has to start with strong, phishing-resistant authentication," noted Sanjay Katkar, Joint Managing Director, Quick Heal Technologies Ltd.

Lock & key

Hardware security keys or passkeys combined with FIDO2 login make stolen SMS codes useless to attackers. (A FIDO2 key is a hardware device, typically a USB or NFC (Near Field Communication) key, that utilises Fast IDentity Online 2 security standard to enable password-less logins.)

Splitting keys with multi-party computation (MPC) eliminates that single point of failure because no one administrator ever holds the full secret. Smart exchanges can combine MPC with hardened hardware security modules and policy-driven approvals.

Self-custody users (who directly control and manage their cryptocurrency assets) should rely on reputable hardware wallets; keep firmware up to date; store recovery phrases offline, and invest in strong fraud-deterrent solutions.

He felt that a Basel-style accord for digital-asset custody would give institutions a clear playbook.

Ankit Sharma, Senior Director and Head – Solutions Engineering at Cyblbe, said that threats to the crypto ecosystem were constantly evolving and represent an array of attack vectors for exchanges and individual holders.

“The growing complexity of blockchain bridges has also made debit and credit considerations ripe for successful exploits and attacks by those with greater skill,” he said.

Sabotage, third-party threats

Insider threats and third-party compromise with trusted vendors also pose risks. Crypto or web3 platforms should establish a number of layered security provisions to replace any deficiencies in the current cybersecurity methods.

At the user level, the importance of security awareness, cold wallets, and strong authentication mechanisms cannot be understated.

Sharma said blockchain technology’s decentralised and unreliable architecture fundamentally disrupt the way traditional cybersecurity models work. Security models based on centralised perimeters and role-based access control do not serve the crypto-native world.

“The current state of security in the crypto ecosystem is impeded by two factors: inconsistency in regulation and lack of standardised technological safeguards,” he said.

He called for the establishment of decentralised threat intelligence networks which will provide ecosystem participants a method to collectively flag and neutralise exploitative actors as they arise.

Trishneet Arora, Founder & CEO of TAC Security, felt that these attacks usually might go unnoticed until a hacker finds an opportunity to exploit them. “As far as exchanges and wallets are concerned, the threats lie in phishing, insider threats, and next poor key management hygiene practice,” he said.

“Regulators, along with compliance bodies, need to shift their focus from mere data protection to ensuring enforceable standards on smart contracts, nodes, wallets, and bridges that form critical infrastructure in Web3 (the next phase of the internet). We believe that Web3 needs its own security compliance layer,” Arora said.