

Quick Heal sounds alarm on sophisticated AI-driven investment frauds



Artificial Intelligence is transforming finance with automation and forecasting, but Seqrite Labs researchers warn scammers exploit its credibility through fake ads, forged celebrity endorsements, and counterfeit trading sites that simulate legitimacy before trapping investors with blocked withdrawals

Quick Heal Technologies has recently identified an alarming surge in complex AI-driven trading scams that have defrauded investors of crores of rupees by masquerading as legitimate investment platforms. The company's latest research, conducted by the team of researchers at Seqrite Labs, India's largest malware analysis platform, reveals how fraudsters employ deepfake-infested platforms, professional-looking dashboards, and strategic small payouts to lure victims before vanishing with substantial deposits.

Artificial Intelligence is revolutionizing finance by enabling automated decision-making and market forecasting, but scammers are exploiting its credibility to construct elaborate hoaxes. Researchers at

Seqrite Labs have documented campaigns in which criminals deploy polished advertisements on social media and messaging apps, complete with forged endorsements from high-profile figures, to redirect unsuspecting users to counterfeit trading sites. These platforms simulate real-time market charts and permit initial small withdrawals to establish trust, only to demand larger sums and ultimately block access when victims seek to reclaim funds.

Elderly duped by AI scams

Two recent cases highlight the scope of this threat. In June 2025, a 79-year-old retiree from Bengaluru was duped of ₹34.6 lakh after responding to a Facebook ad featuring a deepfake video of Infosys co-founder N.R. Narayana Murthy. Believing the platform genuine, she authorized successive payments for taxes and service fees before discovering the fraud and reporting it to local authorities. That same month, a retired IAS officer in Hyderabad lost ₹3.37 crore following a WhatsApp invitation to an “AI-powered” trading app. Only after transferring multiple instalments did he realize withdrawals were impossible and the scammers had disappeared.

Quick Heal AntiFraud.AI intercepts these schemes at every stage. Its SMS and WhatsApp filter automatically quarantines messages containing malicious links before they reach users, while browser-based protections issue real-time warnings on suspicious websites, even those not yet blacklisted. AntiFraud.AI continually updates its blocklist to capture emerging threats and employs behavioral analysis to detect spoofed login pages and fake security certificates.

Steps to avoid digital fraud

Quick Heal Technologies advises users to verify regulatory credentials before trading, insist on transparent team information and technical documentation, and exercise skepticism toward platforms promising guaranteed high returns. Install mobile and desktop security solutions capable of detecting obfuscated payloads and anomalous web behavior, and immediately report any suspicious activity to cybercrime.gov.in or the national helpline at 1930.