ET CISO.in
From The Economic Times

Quick heal technologies limited exposes alarming rise in AI chatbot scams across India

Quick Heal Technologies reveals a rise in AI chatbot scams in India. Criminals use AI to mimic trusted brands and target victims. These scams adapt in real-time, making them hard to detect. Seqrite Labs detects thousands of new AI fraud tools monthly. Quick Heal offers Antifraud.AI for protection. Users should be cautious of requests for sensitive information and unusual language.

Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has unveiled disturbing findings about the rapid proliferation of AI-powered chatbot scams that are reshaping India's cybercrime landscape. As artificial intelligence becomes increasingly sophisticated, criminals are exploiting pre-trained language models to deploy automated fraud factories that can simultaneously target thousands of victims while mimicking trusted brands including banks, delivery services and government agencies with unprecedented accuracy.

The comprehensive investigation conducted by researchers at Seqrite Labs, India's largest malware analysis facility, reveals that security labs are already detecting thousands of new AI-built fraud tools each month, marking AI chatbot scams as one of 2025's most significant digital threats. Unlike traditional phishing schemes, these automated systems can adapt conversations in real-time, pivoting from fake delivery fees to bogus customs fines or fraudulent tech support based on victim responses. This industrial-scale automation allows a single server to orchestrate thousands of simultaneous fraudulent conversations.

Quick Heal Technologies Limited's analysis identifies several dominant scam categories that exploit the natural trust people place in conversational interfaces. Fake customer support chatbots appear during manufactured crises such as suspected account breaches, and harvest credentials before victims realize they're not on legitimate banking websites. Romance scams have evolved to use language models that maintain weeks of emotional conversations, complete with AI-generated photos, before requesting "loans" or directing victims toward fraudulent crypto exchanges. Voice assistant frauds publish malicious skills disguised as harmless apps while using voice cloning technology to impersonate family members in emergency scenarios.

The sophistication of these operations is particularly concerning.
Criminals register look-alike domains such as dhi-delivery.com instead of dhl.com, scrape official brand assets within minutes, and create scripted handoffs that greet victims by name using data from previous breaches. Underground AI tools like FraudGPT generate polished phishing kits and craft personalized attacks that bypass spam filters by adapting their tone - formal for banking targets, casual for gaming enthusiasts. Recent examples of the same include elaborate DHL-branded chatbots that demand customs fees through convincing tracking interfaces, WhatsApp bots impersonating "Meta Security" that steal page credentials and payment methods, and voice cloning scams that use correct personal details scraped from breached databases to build false credibility during fraudulent rebate calls.
Warning signs that users should recognize include any chatbot requesting OTPs, banking information or passwords. Legitimate firms avoid collecting sensitive data through chat interfaces. Unusual grammar patterns, urgent language designed to bypass deliberation, and redirects to suspicious URLs with misspelled domains all signal potential fraud. Quick Heal Technologies Limited suggests that should users spot any single red flag, they immediately end the conversation.

To help unsuspecting users stay safe from such threats, Quick Heal Antifraud.AI, India's first AI-powered fraud prevention solution, provides multi-layered protection against these evolving threats. The cloud-based system cross-references every chat URL against live threat intelligence, blocks

known scam domains in real-time, and monitors dark web marketplaces for compromised user credentials. Advanced features include phishing detection with instant alerts, unauthorized access monitoring that flags suspicious microphone or camera activation, and fraud app detection that analyzes Android signatures against known digital fraud patterns.

As Al-generated content becomes indistinguishable from human communication, Quick Heal Technologies Limited emphasizes that the traditional advice to "trust your instincts" may no longer suffice. The company recommends using a combination of technological safeguards, verification protocols, and public education to combat what represents a fundamental shift in cybercriminal capabilities.