Deepfake AI Trading Scams Target Global Investors - Against Invaders - N

Data: 2025-08-14 00:48:52

Autor: Inteligência Against Invaders

A surge in fraudulent “AI-powered” trading platforms has been observed exploiting deepfake

technology and fabricated online content to deceive investors.

According to a new investigation by Group-IB, scammers are deploying convincing fake videos, phony reviews and targeted online ads to lure victims into fraudulent investment schemes.

At the heart of these campaigns are AI-generated deepfake videos featuring public figures, such as Dutch politician Geert Wilders, endorsing fictional trading platforms.

These videos mimic authentic news broadcasts, complete with synthetic voice cloning and staged urgency to create a sense of exclusivity. Victims are directed to fabricated news articles containing false expert interviews, doctored chartsand glowing testimonials, all designed to prompt registration.

Once users sign up, they are directed toward platforms that request a small initial deposit, typically $100–$250, to avoid arousing suspicion. The sites often demand sensitive personal data, including ID scans, proof of residenceand even credit card images, under the guise of account verification.

Read more on deepfake fraud: The Corporate Deepfake Invasion: Safeguarding Enterprises in the AI Era

Multi-Channel Distribution

Researchers identified a network of YouTube channels, social media accountsand blog posts on platforms like Medium and Blogspot promoting these scams. The operations use localized content scripts to match a user’s country and language, increasing credibility.

Campaigns are tailored to target users in countries including India, the UK, Germany, France, Spain, Belgium, Mexico, Canada, Australia, the Czech Republic, Argentina, Japan and Turkey.

Key tactics identified include:

- AI-generated videos impersonating public figures
-

Fake review sites hosted on free blogging platforms

- Social media pages promoting fraudulent platforms with casual, relatable posts
- Localization of scam websites via IP and language detection

The platforms are reportedly inaccessible from US and Israeli IP addresses, suggesting a focus on other regions.

Coordinated Infrastructure

Using network graph analysis, Group-IB linked a small number of registrants to dozens of scam domains, many of which shared the same registrar and technical details. Some were connected to alternative fraudulent trading sites, including AccuTraderOnline and 10kAPPA.

The report warns that these scams combine professional design, psychological pressureand social proof to erode victims' skepticism.

"This scheme, which utilizes social proof, psychological pressure, and professional design, is highly effective," the researchers concluded.

The findings highlight the need for vigilance, particularly when encountering investment offers tied to AI, deepfake endorsements or unverified online reviews.