How AI is turning online shopping into a cybercrime trap

The festive shopping season is a time for countdowns, flash sales and irresistible discounts. But behind the rush to grab a bargain, a parallel marketplace is thriving, one where familiar brands are impersonated, celebrity endorsements are fabricated and shoppers are persuaded to hand over their money or personal information.

Hire Brand Experts

As India's festive commerce gathers pace, cyber fraudsters are becoming increasingly adept at exploiting the urgency and trust that drive online purchases. Recent warnings around fake Flipkart Big Billion Days 2026 offers have highlighted how deceptive discount links, cloned payment portals and fraudulent promotions can circulate through social media and messaging platforms, often appearing convincing enough to escape immediate suspicion.

Artificial intelligence is raising the stakes. Fraudsters can now create polished promotional creatives, clone voices and faces, and tailor messages to individual consumers at a scale that would previously have required significant time and effort. The result is a new generation of scams that does not necessarily look suspicious. Increasingly, it looks like the real thing.

For businesses, the threat extends beyond financial losses to customer confidence, brand reputation and the integrity of digital commerce itself.

When fraudsters think like performance marketers

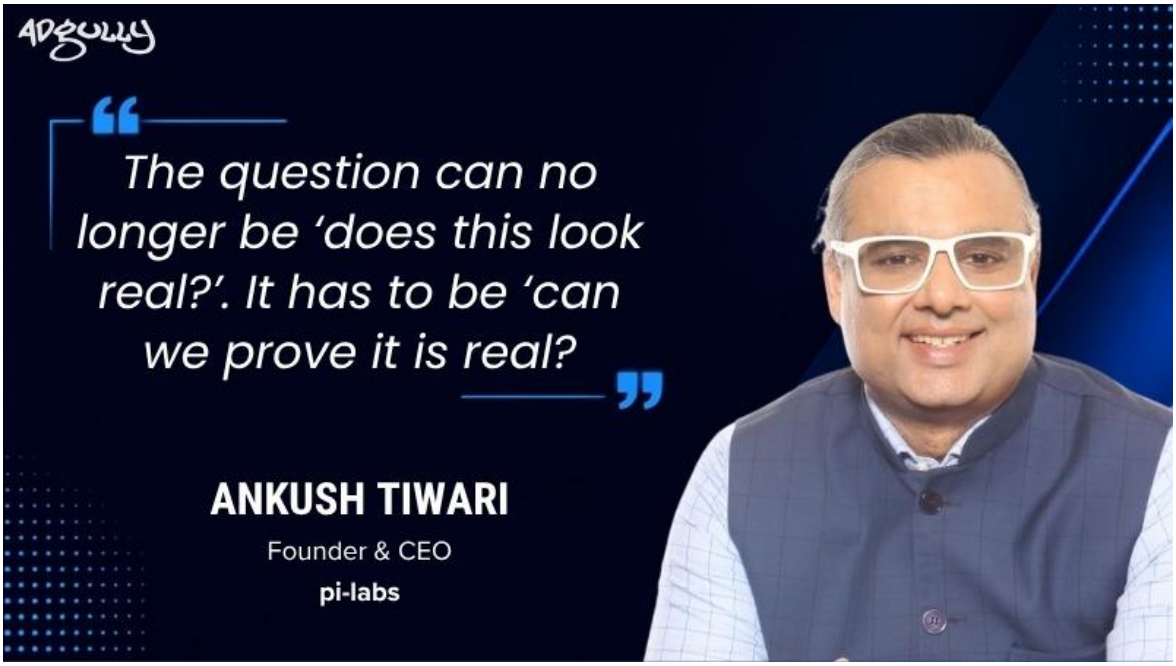
The mechanics of festive fraud are beginning to resemble a sophisticated marketing campaign, complete with an attention-grabbing creative, a conversion funnel and a checkout designed to extract money.

Ankush Tiwari, Founder and CEO of pi-labs, says India's most effective scammers are operating like performance marketers, building each stage of a campaign to overcome shoppers' suspicions. The critical difference is that the creative may now be a deepfake.

Tiwari points to an October 19 warning from the Indian Cyber Crime Coordination Centre (I4C) concerning Facebook and Instagram advertisements that used deepfake videos of the Prime Minister, Finance Minister and Chief Ministers to promote fake rewards. Film stars, influencers and business leaders are also vulnerable to this form of impersonation.

The process can be deceptively simple: fraudsters lift footage from publicly available videos, clone a voice from a short audio sample, synchronise the speaker's lips to a fabricated script and distribute the result through sponsored advertisements or newly created social media pages.

The deception works because people have become accustomed to questioning suspicious links and poorly written messages, but may still place considerable trust in a familiar face speaking on video.



"People have learnt to doubt a strange link or a badly written SMS, but almost nobody doubts a familiar face speaking on video," Tiwari says.

For brands, this creates an uncomfortable problem: the celebrity or business leader they hired to build credibility can be impersonated by a scammer selling a fake version of their promotion.

Once a deepfake captures attention, the next step is to move the shopper away from the official platform. Fake accounts using a retailer's branding can direct consumers to look-alike websites, while fraudulent gift links may lead to malicious applications designed to steal one-time passwords and spread themselves through victims' contact lists.

At the payment stage, shoppers may encounter cloned checkout pages or scratch cards that disguise UPI collect requests as rewards. A transaction that appears to be a chance to win a festive gift can instead result in an unauthorised debit.

Tiwari also highlights the use of AI-generated faces and cloned voices to circumvent video-based know-your-customer checks, potentially helping criminals open mule accounts used to receive fraudulent proceeds. In this way, the same technology can help sell a fake offer and obscure the trail of the money it generates.

Learn Engineering

For Tiwari, conventional awareness campaigns are no longer enough. When deepfakes are designed to look authentic, consumers cannot rely on visual cues alone. He argues that the question must shift from whether a video looks real to whether its authenticity can be established.

His advice to shoppers is direct. “A video is not proof. If an offer comes to you, don’t follow it. Go and find it on the official app yourself.”

AI makes every scam feel personal

Deepfakes are only one part of the problem. AI is also helping cybercriminals move beyond generic phishing messages towards highly personalised deception.

Bikash Barai, Co-Founder of FireCompass, says one of the biggest changes is the ability to personalise fraud at scale. Previously, scammers typically chose between sending the same message to thousands of people and spending time researching individual targets. AI can now combine both approaches.

Barai cites a 2026 USENIX Security study involving 7,700 participants, which found that AI-personalised phishing emails received 2.4 times as many clicks as generic emails, with personalisation costing as little as three cents per email.

Harish Kumar G S, CEO, Quick Heal Technologies Limited, similarly warns that festive scams are becoming harder to identify because criminals are using AI, leaked information and behavioural cues to make communications feel timely and personal.

His recommendation is to disrupt the urgency that drives these attacks. Consumers should pause, independently verify the source and make payments only through a brand's official website or application.

Hire Brand Experts

Technology can flag suspicious activity, but a consumer who refuses to be rushed remains an important line of defence.

Quick Heal's AntiFraud.AI is designed to complement these habits through features such as scam-link protection, fraud-call alerts, suspicious-app detection, secure-payment checks and dark-web monitoring. Kumar says modern fraud protection must address both malicious technology and the manipulation of human trust.

Learn Engineering

The new currency of fraud is borrowed trust

AI may make fake promotions more convincing, but the underlying strategy remains familiar: borrow credibility from a source the victim already trusts.

Vineet Recriwal, Founder of The Native, says the biggest change this festive season is that scams no longer necessarily resemble scams. A fraudulent Big Billion Days offer shared on WhatsApp may feature the right colours, fonts and countdown timers, and even include a video of a familiar face endorsing the deal.

AI has made it cheaper and easier to reproduce brand-like promotional material at scale, stripping away many of the visual clues consumers once relied on to identify fakes.

Recriwal identifies three recurring tactics. The first is borrowed credibility, through deepfake videos of celebrities and business leaders or cloned brand pages running paid advertisements alongside genuine

campaigns. The second is trust passed through personal networks: a festive gift or scratch-card link forwarded by a relative in a family group may attract far less suspicion than an unsolicited SMS.

The third is the payment trap. Cloned checkout pages, fake payment-failure messages and QR codes presented as refund or cashback mechanisms can turn a seemingly legitimate purchase into a financial loss. By the time shoppers reach the payment screen, they may already have accepted the offer as genuine, making them less likely to scrutinise the final step.

“What ties all of this together is urgency,” Recriwal says. During festive sales, brands themselves encourage consumers to act quickly, and fraudsters exploit that same sense of urgency.

HireBrand Experts

Akshaara Lalwani, Founder and CEO of Communicate India, sees the problem as both a cybersecurity challenge and a crisis of consumer trust and brand valuation.

HireBrand Experts

She describes the shift from conventional email phishing to sophisticated brand-identity hijacking, in which scammers exploit the very mechanisms brands use to establish credibility. AI-generated videos and cloned voices can impersonate public figures and brand ambassadors, while sponsored advertisements can lend fraudulent promotions an appearance of legitimacy.

Lalwani also highlights interactive scratch-and-win schemes and festive vouchers that require users to forward links to five or ten contacts to claim a reward. By encouraging consumers to distribute the offer themselves, fraudsters exploit peer-to-peer trust. A link received from a family member may be treated as safe without the usual checks.

The responsibility cannot rest on shoppers alone

While consumers must remain alert, experts caution against making individual vigilance the only defence against increasingly sophisticated fraud.

Amit Relan, Co-Founder and CEO of mFilterIt, says festive sales have become one of the biggest moments in India's digital economy, and fraudsters treat them as an opportunity to exploit shoppers racing against countdown timers and flash discounts.

Fake offers, phishing links, look-alike websites and counterfeit listings can appear authentic at first glance. The warnings around fraudulent Big Billion Days 2026 offers demonstrate how quickly a trusted brand name can become bait.

HireBrand Experts

Relan recommends that shoppers check sellers, examine website addresses carefully and avoid offers that arrive unexpectedly. But he stresses that consumers should not be expected to carry the burden alone.

Fraud response, Relan argues, cannot begin only after a customer has lost money. Brands, e-commerce platforms and digital intermediaries must share responsibility for finding and shutting down threats at their source.

Parag Khurana, Country Manager for India at Barracuda Networks, underlines the challenge created by the sheer volume of festive communications. Consumers are already receiving genuine promotional emails, order confirmations and delivery updates, making it harder to distinguish legitimate messages from convincing phishing attempts.

The risks also extend into the workplace. An employee using a work laptop to shop during the festive season can expose a business to threats, while staff holidays may leave security teams stretched. Threat actors do not take time off, Khurana points out, so organisations must maintain visibility across their environments and ensure the right protections remain in place.

His message is that safer festive shopping requires shared responsibility. “Consumers must pause and verify before clicking, while businesses need the security controls and monitoring capabilities to detect suspicious activity quickly.”

From festive warnings to year-round protection

The challenge facing India’s digital marketplace is no longer simply how to educate consumers to spot suspicious messages. AI-generated fraud can reproduce the look, language and tone of legitimate communications with increasing accuracy. A polished creative, familiar face or personalised message is no longer reliable proof of authenticity.

That makes independent verification essential. Consumers should access offers directly through official applications or websites rather than relying on links received through messages or social media. They should be cautious about requests for OTPs, unexpected payment authorisations and QR codes presented as a way to receive refunds or rewards.