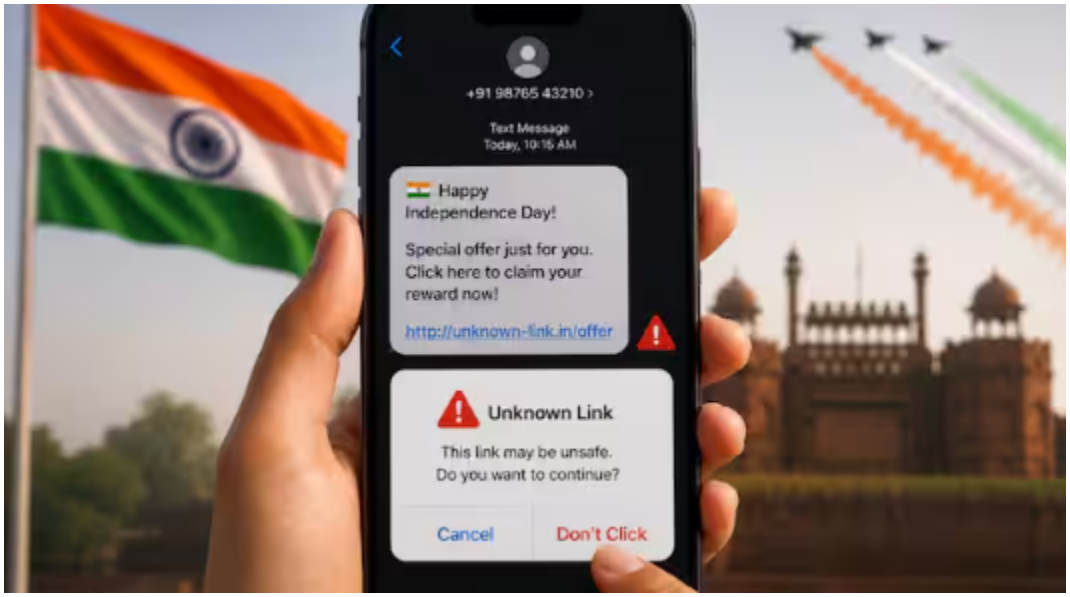
Firstpost.

Independence Day 2026: Why hackers love India's festive shopping rush

As India celebrates its Independence Day, with millions going for online shopping, cybercriminals see this as an opportunity to exploit urgency, trust and online transactions. From fake offers to AI-powered impersonation, experts warn that the weakest link may still be the person behind the screen.



India's Independence Day is a time for flags, patriotic messages, public events and, increasingly, a flurry of activity on smartphones. But as we celebrate August 15, there is another side to India's increasingly connected celebrations: every surge in digital activity creates more opportunities for cybercriminals to hunt for victims.

The broader cyber threat is already growing sharply. Data tracked by CERT-In shows that the number of cybersecurity incidents in India rose from 13.91 lakh in 2022 to 20.41 lakh in 2024, before reaching 29.44 lakh in 2025. Separately, a government backgrounder put the increase at 10.29 lakh to 22.68 lakh between 2022 and 2024, highlighting how rapidly India's digital attack surface is expanding.

Festivals and major national events add another layer to this problem. They bring more people online, more transactions, more promotional messages and, crucially, more reasons to click on a link without thinking twice.

Why festive season gives cybercriminals a bigger window to target Indians

The psychology of a festive period works neatly in a scammer's favour. There is excitement, urgency and an expectation that a good deal, delivery update or special offer could arrive at any moment.

McAfee's India festive shopping research found that 66 per cent of Indian consumers planned to shop online more than the previous year. It also found that 74 per cent believed cybercriminals were more prevalent during the festive season, while 41 per cent said they were more likely to act immediately when they saw a good deal. McAfee's Labs also protected users against nearly 24,000 suspicious or malicious URLs during the festive shopping period it studied.

That behaviour is precisely what attackers exploit.

"The festive season in India has become a peak hunting ground for cybercriminals, because they know that excitement, urgency, and heavy digital spending lower our guard," says Harish Kumar, CEO, Quick Heal Technologies.

The threat is not limited to traditional online shopping. India's expanding digital ecosystem means consumers can encounter suspicious links through WhatsApp, social media, SMS, email, payment platforms and even fake customer-care channels.

Ravindra Singh, Managing Director, Delcom Telesystems, told Firstpost that the combination of higher transaction volumes, limited-time offers and greater consumer engagement across e-commerce, messaging and payment platforms makes the festive period particularly attractive to attackers.

The most common types of cyber attacks in India

The scams themselves may look different, but many are built around the same trick: make the victim believe that something legitimate is happening.

Fake e-commerce websites and clone apps are among the most obvious examples. A site offering an unusually steep discount or a social-media page mimicking a familiar brand can appear convincing enough to make a user hand over payment details.

Then there are UPI and QR-code scams. A fraudulent refund, cashback or payment request can be presented as money coming to the consumer, when approving the transaction actually sends money out.

Phishing and smishing remain equally effective. A message claiming to be from a bank, courier company or online retailer can direct users to a malicious website designed to harvest credentials or financial information.

Varun Grover, Business Unit Head at mFilterIt, says the sheer volume of legitimate offers, advertisements and influencer-led promotions makes it harder for consumers to distinguish genuine campaigns from fraudulent ones. The problem can become more pronounced as digital adoption expands across Tier 2 and Tier 3 cities, bringing more first-time or less-experienced users into the ecosystem.

Quick Heal's Kumar adds that its India Cyber Threat Report 2026 recorded 265.52 million detections across more than eight million endpoints, averaging 505 detections every minute. Trojans and infectors accounted for nearly 70 per cent of the attacks recorded, he says, with social engineering playing a significant role.

How is AI playing a role?

The next generation of scams may not look like scams at all.

Generative AI is allowing criminals to create polished messages, convincing websites, cloned voices and highly personalised social-engineering campaigns at speed. The old warning signs — awkward language, spelling mistakes or obviously fake messages — are becoming less reliable.

The research found that 84 per cent of Indians were more concerned about deepfakes than a year earlier. Nearly half said they or someone they knew had encountered a deepfake shopping scam.

"The technology itself is not the threat, its misuse is," says Delcom's Singh, adding that AI is reducing the traditional warning signs consumers have relied upon.

mFilterIt's Grover similarly sees AI as an accelerator rather than an entirely new category of attack. It can automate and personalise phishing and social engineering, making attacks faster and harder to detect.

Kumar puts it more bluntly, "What we are witnessing is not AI turning rogue on its own, but adversaries weaponizing AI to industrialize deception."

The response, he argues, will require AI-assisted defence as well, alongside stronger authentication, monitoring and user awareness.

How to stay safe

The simplest defence remains surprisingly low-tech: slow down.

Do not click on festive or promotional links received through unsolicited SMS, WhatsApp or email. Instead, open the company's official app or website yourself. Check the URL before entering credentials or making a payment.

Never share an OTP, PIN or card details with someone claiming to represent a bank, retailer or delivery company. Be particularly cautious with QR codes and UPI collect requests presented as refunds, cashback or prize payments.

For brands, the challenge is broader. Grover says organisations need real-time monitoring across app stores, social platforms and advertising networks to detect cloned apps, fake domains, impersonation and suspicious traffic before these campaigns spread.

And as India's digital footprint continues to expand, cybersecurity can no longer be treated simply as a device-level problem.

"Pause before you click, verify before you pay, and never allow a sense of urgency to override basic security checks," says Singh.

That may be the most useful Independence Day reminder of all: in an increasingly connected India, digital freedom also comes with the responsibility to protect the trust that makes that connectivity work.