THE TIMES OF INDIA

Beware this festive season! Cyber criminals go personal with a new wave of frauds; here's what you should know

TIMESOFINDIA.COM | Sep 29, 2025, 04.08 PM IST

Cyber fraud activities are up this festive season, with AI generated tools making the attacks more personal and targeted.

Cybersecurity companies report a nearly 40% rise in attacks during festivals, with up to 15% behaviour-based. From targeting shoppers with personalised phishing links to embedding malware in festive e-cards, scammers now aim at emotions rather than devices.

"With GenAI coming into the picture, it becomes extremely easy for fraudsters to create communication that's customised and very contextual in nature," Sneha Katkar, head of product strategy at Quick Heal Technologies told ET.

"Fraud is not about the device; it is about the person. That is where it becomes critical for the fraudster to have enough information about you to convince you that they are authentic," Katkar explained.

Quick Heal noted that behaviour-based attacks accounted for 15% of detections in 2024, with this year's number expected to rise sharply.

In one instance, a Mumbai content writer Divya thought she was helping a friend when she transferred Rs 6,000 for a food processor. The WhatsApp message came from an unknown number using her roommate's profile picture. "She asked me to pay Rs 6,000 for a food processor for her mother in Surat,

saying her UPI wasn't working. She was looking for processors two days before, so I paid," Divya said. However, she later discovered that she had been scammed.

"I realised I was scammed."

While it remains unclear how the scammer knew Divya had been searching for processors with her roommate, experts say AI and machine learning make it easier for criminals to craft phishing links and messages that match users' online activity.

Festivals like Dussehra and Diwali, when 95% of Indians plan shopping, are prime targets, ET reported. "Phishing links in emails and SMS are the oldest trick in the playbook. But now, you have AI-generated celebrity endorsements with deals on top products, spreading through social media. We see a 40% increase in such scams during these months compared to the first quarter," said Pratim Mukherjee, senior director at McAfee.

Advanced persistent threat groups also "follow the emotion and thus, follow the money," said Jaydeep Singh, general manager at Kaspersky India.

These groups operate like corporations, providing malware as a service and focusing on specific regions at particular times, with India often among the top five targets.

Katkar warned that scammers are also exploiting festive greetings. "People also share e-greeting cards during festivals, where an image or animation gets downloaded. But those are actually mobile trojans, which later hack apps like WhatsApp and send random messages to your contacts, posing as you, asking for money. If 100 people receive such messages, at least four or five end up sending money since it wouldn't be such a huge amount."

Despite increased awareness campaigns, Reuben Koh, director of security strategy, Asia Pacific and Japan at Akamai Technologies, called the rise of GenAI a "wild card," as per an ET report.

"Cyber criminals are using fewer of the conventional methods of fraudulent activities since they are easier to detect and counter. By the time we have pattern-matched something, another type of scam would have emerged," he said.