Festive Sales 2025: How To Stay Safe From Online Scams Amid Shopping Frenzy

Planning for festive shopping? Here's a complete guide to staying safe from online scammers.

The festive season has begun, and with it, people have already started indulging in online shopping. Online shoppers always look forward to huge discounts, attractive deals and cashback offered by top brands during the festive season. However, alongside the joy of shopping and gifting, there is also an increased risk of cyber fraud during this period.

Experts caution that cybercriminals are becoming more opportunistic, exploiting the surge in online activity during festivals. Through scam messages, phishing links and malicious QR codes, fraudsters attempt to steal sensitive data and financial information from both consumers and businesses.

Online Scam During Festive Season: Here's What Experts Suggest
According to Harsha Solanki, VP and GM Asia at Infobip, smishing attacks such as fraudulent SMS messages disguised as trusted brands have become common during festive seasons. These messages typically lure users with fake offers, refund notifications, OTP prompts, or delivery updates.

"Recently, McAfee identified over 75,000 such impersonation messages, many designed to create urgency and push users into clicking without verification," Solanki was quoted as saying by CNBC TV18.

She further explained that the risk is no longer limited to SMS alone. QR-code scams have emerged as a widespread technique, often redirecting people to malicious sites that look deceptively real.

Adding to this, Sneha Katkar, Head of Product Strategy at Quick Heal, stressed that festive sales bring a surge in fraudulent deals that appear legitimate. "Brands do not send messages from random numbers or use suspicious-looking domains. Always preview links before clicking — if they appear unusual, it is better to avoid them," she advised.

Katkar also highlighted the role of security tools. She suggested the use of trusted technologies such as Quick Heal AntiFraud.AI, which is designed to identify hidden threats, block malicious links and safeguard users against data-stealing apps.

Tips To Avoid Scams

To safeguard themselves, consumers are advised to be cautious of unexpected texts, refrain from clicking on unfamiliar links, and verify offers only through official websites or apps.
Cybersecurity experts also warn against replying with “STOP," as engaging with such messages can increase the risk of exposure.

Rising Risk For SMEs
The threat of cyber scams is not limited to individual consumers. Small and medium-sized enterprises (SMEs) face significant risks during the festive season, particularly when order volumes are at their peak. Fraudsters exploit these busy periods by circulating forged payment receipts, impersonating genuine suppliers, or embedding malicious QR codes into what appear to be festive greetings.

According to an advisory issued by FedEx under its Cyber Jagrukta Diwas initiative, citing data from the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI), nearly 74 per cent of SMEs reported at least one cyber incident last year. This highlights the urgent need for businesses to adopt stronger cybersecurity measures

Cybersecurity experts also warn against replying with “STOP," as engaging with such messages can increase the risk of exposure.

Rising Risk For SMEs
The threat of cyber scams is not limited to individual consumers. Small and medium-sized enterprises (SMEs) face significant risks during the festive season, particularly when order volumes are at their peak. Fraudsters exploit these busy periods by circulating forged payment receipts, impersonating genuine suppliers, or embedding malicious QR codes into what appear to be festive greetings.

According to an advisory issued by FedEx under its Cyber Jagrukta Diwas initiative, citing data from the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI), nearly 74 per cent of SMEs reported at least one cyber incident last year. This highlights the urgent need for businesses to adopt stronger cybersecurity measures

Use multi-factor authentication and restrict access to key business systems.

Establish a simple process for employees to report and log suspicious activity.