10 Festive Season Scams You Should Watch Out for in 2026



The festive season fetches exciting sales, online shopping, digital payments and gift deliveries. But the rush to grab a deal or claim a reward can also create opportunities for cybercriminals. From fake shopping websites to AI-generated celebrity endorsements, festive season scams are becoming harder to recognise.

The scale of the problem is huge. According to India's Ministry of Home Affairs, more than 24 lakh financial cyber fraud complaints were reported in 2025, involving over ₹22,495 crore. The figures underscore why staying alert to online scams and digital fraud matters, especially when festive shopping and payments increase.

Top 10 Festival Scams to Watch Out For

Scammers often use familiar brands, urgent messages and tempting offers to gain your trust. Here are 10 common scams to recognise and the precautions that can help you avoid them.

1. Fake Festive Sale and Shopping Scams

Scammers create fake shopping websites and social media ads offering unbelievable discounts on smartphones, electronics and other festive essentials. Buyers may receive counterfeit products or nothing after making payment.

How to stay safe: Shop through trusted platforms, verify website URLs and avoid deals that seem too good to be true.

2. Fake UPI Cashback and Payment Scams

Fraudsters promise festive cashback, refunds or rewards to trick users into scanning QR codes or approving payment requests. Entering your UPI PIN authorises a payment rather than helping you receive money.

How to stay safe: Never enter your UPI PIN to receive cashback. Verify the recipient and transaction amount before approving payments.

3. Fake Courier and Parcel Delivery Scams

Messages claiming a parcel is delayed due to an incorrect address, unpaid fee, or incomplete KYC may contain malicious links. These can lead to fake payment pages designed to steal banking details.

How to stay safe: Track parcels through official courier websites or apps. Avoid unsolicited links and never share OTPs or banking details.

4. Phishing Emails and Festive Offer Messages

Scammers impersonate banks, retailers and payment providers through emails or SMS messages advertising exclusive deals. Links may lead to fake login pages that steal passwords, card details and Fake OTPs.

How to stay safe: Check the sender and website URL. Visit official websites directly instead of clicking unexpected links.

5. AI-Generated Deepfake and Impersonation Scams

AI-generated videos and cloned voices can make fake celebrity endorsements, investment offers, or urgent requests for money appear genuine. Familiar faces and voices are no longer reliable proof of identity.

How to stay safe: Verify claims through official channels and confirm unusual money requests independently before transferring funds.

6. Fake Festive Giveaways and Lucky Draws

Fraudsters announce fake prizes, including smartphones, shopping vouchers and holiday packages. Victims are asked to pay processing fees or share personal information to claim rewards they never won.

How to stay safe: Verify giveaways through official brand accounts. Never pay unexpected fees or share sensitive details to claim unverified prizes.

7. Fake Customer Care and Refund Scams

Fake support representatives exploit failed payments, cancellations and delayed deliveries. They may ask victims to share OTPs, scan QR codes or install remote-access apps, potentially exposing sensitive information.

How to stay safe: Use customer care details listed on official websites. Never share banking credentials or install apps at an unknown caller’s request.

8. Fake Investment, Gold and Festive Bonus Schemes

Scammers promote fraudulent trading platforms, digital fraud gold offers and festive investment bonuses promising unusually high or guaranteed returns. Victims may lose their money when they attempt to withdraw their investments.

How to stay safe: Verify investment providers independently and avoid guaranteed-profit claims or pressure to invest immediately.

9. Fake Charity and Donation Appeals

Fraudsters exploit festive generosity through fake donation campaigns featuring emotional stories, copied photographs and fraudulent payment details.

How to stay safe: Verify charities before donating and use their official payment channels. Be cautious of urgent appeals that discourage verification.

10. WhatsApp Account Takeover and Festive Message Scams

Fake greetings, gift links and voting requests can lead to malicious websites or attempts to steal WhatsApp verification codes. Scammers may then impersonate victims and ask their contacts for money.

How to stay safe: Never share verification codes, enable two-step verification and confirm unusual requests through a phone call.

How to Protect Yourself from Festive Season Scams in 2026

Recognising individual scams is important, but building safer digital habits can help you avoid many forms of online fraud.

Keep these precautions in mind throughout the festive season:

Pause before you click: Check unexpected links, QR codes and payment requests before interacting with them.

Protect your credentials: Never disclose passwords, OTPs, UPI PINs or card security details.

Keep your devices updated: Install operating system, browser and application updates to address known security vulnerabilities.

Use trusted security software: A reliable security solution can help detect malicious websites, suspicious files and other online frauds, depending on its capabilities and settings.

Verify before you pay: Check the merchant, recipient and transaction amount before confirming a payment.

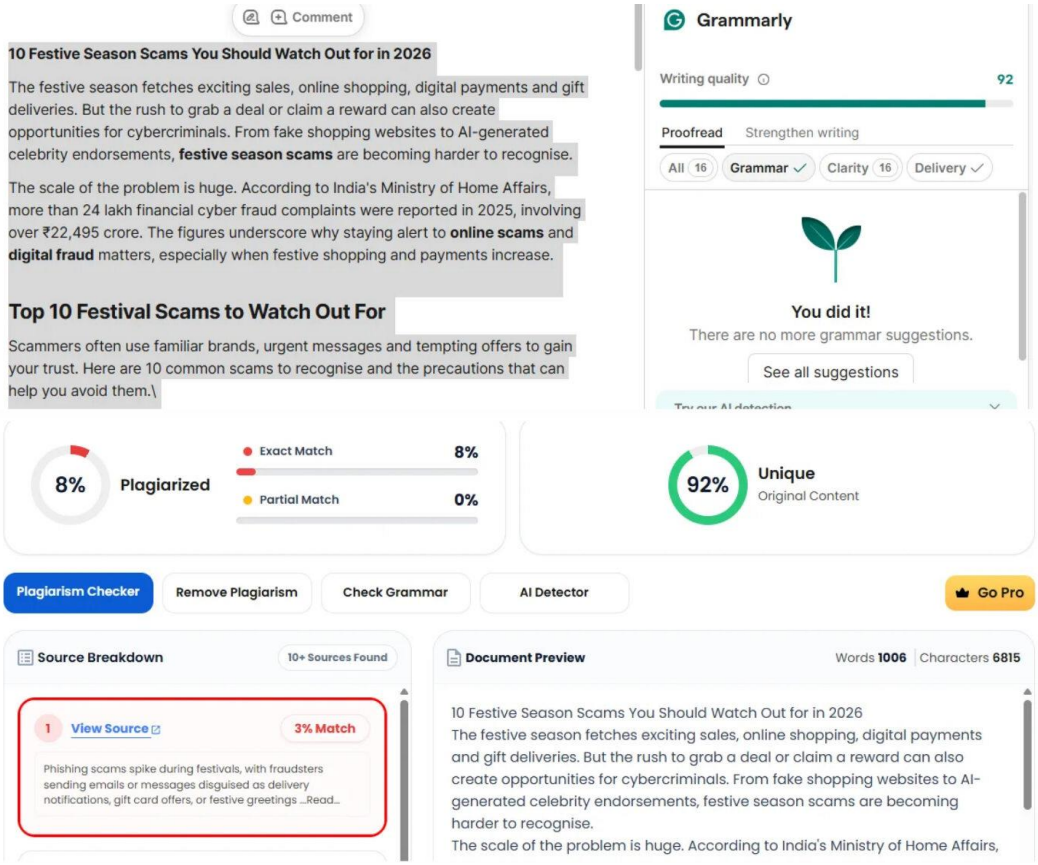
Report suspected fraud quickly: If you lose money to an online financial scam in India, contact your bank or payment provider immediately and call 1930 to report the incident. You can also file a complaint through the National Cyber Crime Reporting Portal.

Quick action can help authorities and financial institutions respond to a fraudulent transaction, although recovering the money is not guaranteed.

Celebrate Safely with the Right Cybersecurity Measures

Festival scams often succeed because they exploit familiar situations: an exciting discount, a long-awaited delivery, a generous giveaway or an urgent request from someone you trust. Taking a moment to verify a message or payment request can make a significant difference.

Alongside safe browsing and responsible digital payment habits, using a trusted security solution can add another layer of protection. Quick Heal's cybersecurity solutions are designed to help users protect their devices and navigate digital fraud threats with greater confidence.



This festive season, enjoy the offers, share the celebrations and stay alert to suspicious activity. A little caution can help keep your celebrations joyful and your digital life safer.