How to stay safe from scam messages and cyber fraud this festive season

Cyber experts warn that scam messages, forged payment receipts, and malicious QR codes rise during the festive rush, with both individuals and small businesses at risk. Staying alert and verifying before acting remain key defences.

The festive season often sees a surge in online shopping, payments, and digital communication, creating opportunities for cybercriminals to trick both consumers and businesses. Experts warn that fraudsters rely on scam messages, phishing links, and malicious QR codes to steal sensitive data or money.

Harsha Solanki, VP & GM Asia at Infobip, said smishing attacks — fraudulent SMS messages imitating trusted brands — have become common during festivals. These messages often carry fake offers, refund alerts, OTP requests, 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 noted.

She added that the risk is not limited to SMS, with QR-code scams being used to redirect people to malicious sites.

To stay safe, consumers should treat unexpected texts with caution, avoid clicking on unusual URLs, and verify offers only through official websites or apps.

Cybersecurity experts advise ignoring prompts to reply with “STOP,” as engaging with such messages can further expose users.

Strong digital hygiene, such as regularly updating device software and enabling multi-factor authentication, is also recommended.

Sneha Katkar, Head of Product Strategy at Quick Heal, highlighted that festive sales bring a surge in fake deals.

“Legitimate brands don’t send messages from odd numbers or use suspicious domains. Preview links before clicking — if they look unusual, avoid them,” she said.

Katkar suggested using trusted tools like Quick Heal AntiFraud.AI, which can flag hidden threats and data-stealing apps.

The threat is not limited to individuals.

Small and medium businesses (SMEs) also face heightened risks during the festive rush. According to an advisory issued by FedEx under Cyber Jagrukta Diwas, citing data from the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI), 74% of SMEs reported at least one cyber incident last year.

Scammers often exploit stretched teams and higher order volumes by sending forged payment

receipts, impersonating suppliers, or disguising malicious QR codes as festive greetings.

FedEx's advisory listed tips for SMEs to stay "scam-smart" during the festive season:

- Confirm UPI or bank transfers before dispatching goods.
- Verify any changes in bank details with trusted contacts.
- Train staff to recognise red flags such as urgent messages, suspicious QR codes, or unknown links.
- Use multi-factor authentication and restrict access to key business systems.
- Establish a simple process for employees to report and log suspicious activity.

Authorities encourage both individuals and businesses to report suspected fraud immediately to the Cyber Crime Helpline at 1930 or via cybercrime.gov.in.