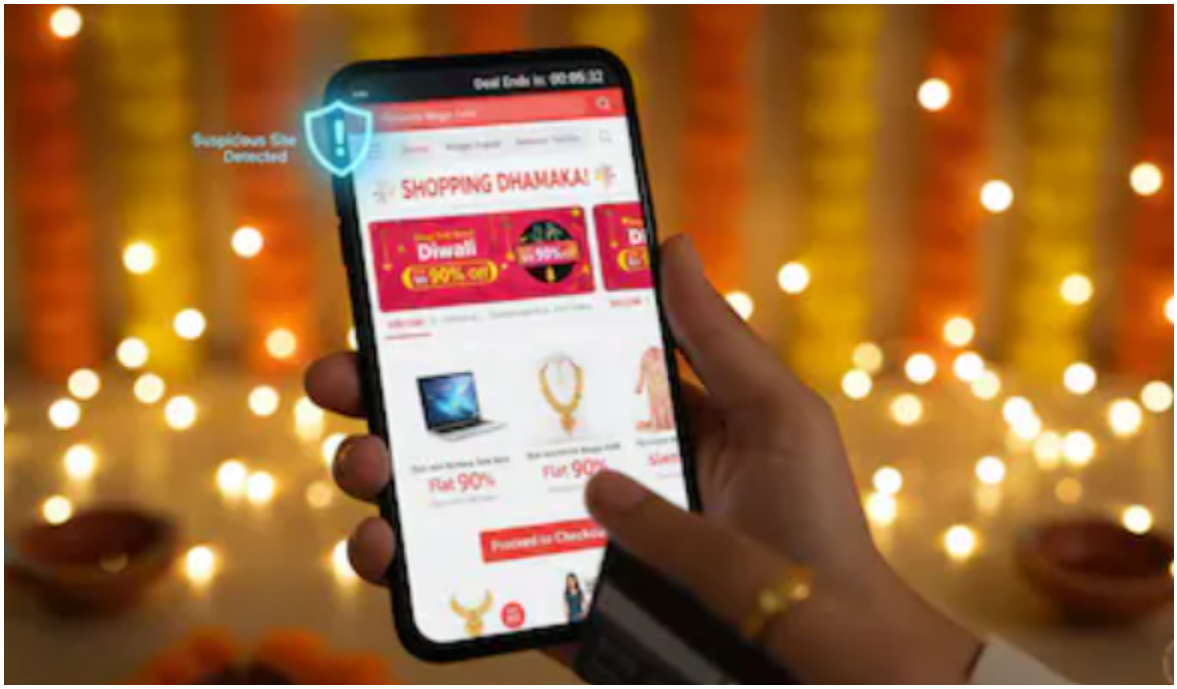
Festive season shopping: How to spot online scams and keep your money safe



Summary

Festive digital transactions face rising cyber scams like QR manipulation and AI phishing. Experts urge combining consumer vigilance with real-time fraud detection and automated warning networks to track suspicious mule accounts.

The festive season brings more than just shopping discounts and special offers. It also creates opportunities for cybercriminals to exploit consumers who are making frequent digital payments, tracking deliveries and responding to promotional messages.

Fake cashback offers, tampered QR codes, phishing links and impersonation of trusted brands are among the methods used to trick shoppers into transferring money or sharing sensitive financial details.

The growing use of artificial intelligence (AI) has made some of these attempts harder to identify, with fraudulent messages resembling genuine brand communications.

How festive-season payment scams work

One common method involves sending QR codes through WhatsApp or other messaging platforms, promising cashback, refunds, Diwali bonuses or gift hampers. Users are asked to scan the code and enter their UPI PIN to receive the money.

However, entering the PIN authorises a payment, resulting in a debit from the user's account.

Another method involves placing fake QR-code stickers over genuine merchant codes at shops, diverting payments to fraudsters.

PhonePe has cautioned consumers against such scams, reiterating that a UPI PIN is required to send money, not receive it. Users should verify the recipient's name and transaction amount before authorising payments.

Fraudsters also exploit the volume of promotional emails, order confirmations and delivery updates during festive sales. They may impersonate popular brands, circulate phishing links or direct shoppers to cloned websites offering unusually steep discounts.

Parag Khurana, Country Manager, India, Barracuda Networks, says the high volume of genuine promotional and payment communications makes it harder for consumers to distinguish legitimate messages from fraudulent ones.

Harish Kumar, CEO of Quick Heal Technologies, points out that AI and leaked personal data are making scam messages more convincing, sometimes incorporating details of consumers' recent shopping activity.

Why consumer vigilance alone is not enough

While consumers need to verify payment requests and shopping websites, businesses and financial institutions also have a role in preventing fraud.

Rajiv Beri, CTO of NPST, says banks need to move from detecting fraud after transactions have taken place to identifying suspicious behaviour before money moves. This includes monitoring signals such as devices linked to multiple accounts, clusters of small test payments and unusual changes in merchant transaction patterns.

He also highlights the importance of real-time early warning systems, particularly for identifying mule accounts.

Niraj Kumar, CTO at Onix, emphasises the need for businesses to use AI-driven systems to identify unusual transaction patterns and build infrastructure that can handle sudden spikes in festive-season traffic without compromising security.

Shrish Anand Lal, Executive Director and CBO, New Street, the company behind MiFiX.ai, says fraud increasingly targets consumer trust through cloned voices, forged documents and messages impersonating banks.

He highlights the need for banks to adapt their fraud controls quickly as new methods emerge, with AI-assisted detection supported by clear rules and human accountability.

Amit Relan, CEO and Co-Founder of mFilterIt, also points to counterfeit product listings, fake websites and brand impersonation across e-commerce marketplaces and social media. He says brands need to monitor the wider digital ecosystem, including third-party platforms, to identify fraudulent listings and phishing attempts.

What consumers should watch out for

- QR-code requests: Never enter a UPI PIN to receive cashback, refunds or rewards. Check the recipient's name before making a payment.
- Unsolicited links: Avoid clicking on unexpected discount, delivery or refund links received through SMS, email or messaging apps.
- Fake shopping websites: Check website addresses and seller credentials before entering payment details. Be cautious of deals that appear unusually attractive.
- Urgent payment requests: Treat messages demanding immediate action or threatening account restrictions as potential red flags. Verify them through official channels.
- Sensitive information: Never share OTPs, UPI PINs, passwords or card details with anyone claiming to represent a bank or payment platform.
- What to do if you become a victim

Report the transaction immediately to your bank and payment service provider. You can also report financial cyber fraud through the National Cyber Crime Reporting Portal at cybercrime.gov.in or call 1930. Prompt reporting can help authorities initiate action to trace and potentially freeze the money.

Suspicious calls and messages can also be reported through the Chakshu facility on the Sanchar Saathi portal.

Vijaypal Singh, Co-founder and CEO of Karta AI, highlights the importance of swift action by banks after a customer reports fraud. This may involve blocking a card, raising a dispute and checking other transactions for suspicious activity.

He says AI-led customer support systems should also maintain an auditable record of actions taken.