7 Social Media Shopping Scams to Avoid This Diwali

Learn how to spot seven social media shopping scams this Diwali, verify sellers, secure payments and protect your money with Quick Heal's safety tips.

Festive shopping is just a scroll away. One minute, you're watching Diwali décor reels; the next, you're eyeing a too-good-to-miss deal or an influencer's latest recommendation. But behind those festive offers and picture-perfect product posts, social media scams can turn shopping excitement into a costly mistake. Fake sellers, irresistible discounts and fraudulent payment requests are often just a click away.

According to Meta's India Retail Purchase Journey report, nearly 8 in 10 shoppers in India rely on social platforms for product discovery [1]. With festive deals flooding social media, shoppers need to know how to spot fake sellers and misleading offers before they fall victim to Diwali shopping scams.

7 Social Media Shopping Scams to Watch Out For

From fake shopping pages to fraudulent marketplace listings, these are some common social media scams to recognise before making your next festive purchase.

1. Fake Shopping Pages on Instagram and Facebook

Scammers create fake shopping pages that imitate popular brands or advertise heavily discounted clothing, electronics and festive gifts. They may copy product photos, logos and descriptions from genuine

businesses to appear credible. After receiving payment, they may block the buyer or disappear without delivering the product.

How to stay safe: Check the page's history, customer reviews and official website. Avoid paying unfamiliar sellers in advance.

2. Instagram Shopping Scams Through Fake Influencer Promotions

Fraudsters use fake influencer accounts or compromised profiles to promote counterfeit products and unrealistic festive deals. Professional-looking photos and fabricated testimonials can make these offers appear legitimate. Some scammers also impersonate creators through similar usernames to exploit their followers' trust.

How to stay safe from an Instagram shopping scam: Verify the influencer's identity, check tagged brand accounts and purchase through authorised sellers.

3. Facebook Marketplace Scams

A Facebook Marketplace scam may involve fake product listings, attractive prices or sellers demanding advance payments before shipping. Some scammers also share fake payment screenshots to deceive buyers and sellers. Buyers may be pressured to pay quickly by claims that several people are interested in the same item.

How to stay safe: Inspect products where possible, verify payments independently and avoid suspicious advance-payment requests.

4. Fake Festive Giveaway and Contest Scams

Scammers announce fake Diwali giveaways promising smartphones, gift vouchers or shopping hampers. Victims are asked to pay delivery charges, share personal details or click links to claim prizes. These links may lead to fraudulent websites that collect sensitive information.

How to stay safe from Diwali shopping scams: Verify contests through official brand accounts. Never pay unexpected fees to claim an unverified reward.

5. Fraudulent Social Media Advertisements

Sponsored advertisements may lead to cloned websites selling branded products at unusually low prices. These online shopping scams often collect payments or personal information without delivering genuine products. Countdown timers and claims of limited stock may pressure shoppers into purchasing without checking the seller.

How to stay safe: Check the website URL, return policy and seller credentials before ordering. A sponsored post does not automatically mean an offer is trustworthy.

6. Fake Customer Reviews and Testimonials

Fraudulent sellers use fabricated reviews, stolen product photographs and edited customer testimonials to build credibility. Some fake shopping pages even display copied comments to make buyers believe others have received their orders. A large follower count or a few positive reviews alone cannot establish that a seller is genuine.

How to stay safe: Look for independent reviews, consistent seller information and genuine customer feedback across multiple sources.

7. Social Media Payment and Refund Scams

Scammers impersonate sellers or customer support representatives and claim that a payment

failed or a refund is pending. They may request OTPs, UPI PINS or QR-code scans to steal money. Others send fake payment confirmations to convince sellers to hand over goods before the money arrives.

How to stay safe: Verify payment status through your banking app. Never share OTPs or enter your UPI PIN to receive a refund.

How to Avoid Social Media Shopping Scams This Festive Season

A few simple precautions can help you enjoy festive deals without exposing your money or personal information to unnecessary risks.

Verify sellers: Check account history, contact details and independent reviews.

Inspect links: Avoid shortened URLs and unfamiliar payment pages.

Use secure payments: Never share banking credentials or approve unexpected payment requests.

Protect your devices: Keep apps updated and use trusted cybersecurity software.

Report fraud quickly: Contact your bank if money is lost and call 1930 in India to report financial cyber fraud. You can also file a complaint through the National Cyber Crime Reporting Portal.

Before purchasing, compare prices across trusted retailers and read the seller's return and refund policies. If an offer creates pressure to pay immediately or move the conversation to an unfamiliar platform, pause and verify it first.

Shop Smart and Stay Safe with Quick Heal

Social media can make festive shopping convenient, but attractive offers and familiar-looking profiles should never replace verification. Take a moment to check sellers, payment requests and website links before placing an order.