नाशिक | Wednesday, 23 September 2026

सावधान ! दिवाली सेल की आड़ मे निकाल देगें दिवाला — फर्जी वेबसाइट से ठगी से बचने के लिए पढ़े ये जरूरी बाते

Publisher

Published on 11 Oct 2025

त्योहारी सीजन में खरीदारी का उत्साह हर भारतीय के घर में देखने को मिलता है। दिवाली के मौके पर बाजारों से लेकर ऑनलाइन प्लेटफॉर्म तक हर जगह ऑफर्स और डिस्काउंट की बाढ़ आ जाती है। लेकिन इस चमक-दमक और सेल की आड़ में कई साइबर ठग भी सक्रिय हो जाते हैं। वे असली जैसी दिखने वाली फर्जी वेबसाइट और मोबाइल ऐप्स बनाकर लोगों को लुभाते हैं, और एक क्लिक में उनका **बैकं खाता खाली कर देते है**।

विशेषज्ञों का कहना है कि हर साल दिवाली के दौरान **ई-कॉमर्स फ्रॉड** के मामले लगभग 35% तक बढ़ जाते हैं। खासकर जब लोग भारी छूट देखकर तुरंत खरीदारी का निर्णय ले लेते हैं। ऐसे में **थोड़ी सी लापरवाही भारी आर्थिक नुकसान** का कारण बन सकती है।

दिवाली के इस शॉपिंग सीजन में फर्जी वेबसाइट्स और स्कैमर्स की चाल पहले से ज्यादा चालाक हो गई है। वे अब न सिर्फ **असली वेबसाइट्स जैसी डिजाइन, लोगो और नाम** का उपयोग करते हैं बल्कि **डोमेन नाम भी बेहद मिलते-जुलते** रखते हैं। जैसे “amaz0n.in” या “flipkarrt.com” जैसी साइटें, जो पहली नजर में असली लगती हैं।

इन साइटों पर नकली उत्पादों के नाम पर भुगतान लेने के बाद या तो सामान भेजा ही नहीं जाता या **बेहद घटिया प्रोडक्ट** डिलीवर कर दिया जाता है। कई बार तो ये वेबसाइट्स सिर्फ आपके **कार्ड या बैकं डिटेल्स चोरी करने** के लिए बनाई जाती हैं।

कैसे पहचाने फंर्जी ई-कॉमर्स वेबसाइट

दिवाली सेल के दौरान अगर आप किसी नई वेबसाइट से खरीदारी करने जा रहे हैं, तो कुछ बातों का ध्यान रखना बेहद जरूरी है। सबसे पहले वेबसाइट का **URL ध्यान से देखे**। असली वेबसाइट हमेशा “https://” से शुरू होती है और उसके साथ **ताले (lock) का निशान** दिखता है। अगर यह नहीं दिख रहा, तो उस साइट से दूरी बनाएं।

दूसरा, **वेबसाइट की वर्तनी (spelling)** जांचें। स्कैमर्स अक्सर लोकप्रिय ब्रांड्स के नाम में थोड़ा बदलाव करके फर्जी साइट बनाते हैं, जैसे "flipkar.com" या "amazone.in"।
तीसरा, वेबसाइट के "About Us" और "Contact Us" पेज देखें। फर्जी वेबसाइट्स पर अधूरी जानकारी या **फर्जी पते और नंबर** दिए जाते हैं।

इसके अलावा, अगर वेबसाइट पर **बहुत ही सस्ते दामों मे मंहगे प्रोडक्ट्स** ऑफर किए जा रहे हों, तो यह चेतावनी का संकेत है। कोई भी असली कंपनी बाजार दर से 70–80% कम दाम पर असली ब्रांडेड सामान नहीं बेचती।

साइबर एक्सपर्ट्स की सलाह

साइबर सुरक्षा विशेषज्ञों का कहना है कि इस तरह की ठगी से बचने के लिए हमेशा **विश्वसनीय प्लेटफॉर्म या ऐप्स** जैसे Amazon, Flipkart, Myntra, Ajio, Meesho आदि से ही शॉपिंग करें।
अगर किसी नए ऑनलाइन स्टोर से खरीदारी करनी ही है, तो पहले उस साइट का **रीव्यू पढ़े** ंऔर उसके **सोशल मीडिया अकाउंट्स की जांच करे** ं। कई बार स्कैमर्स नकली सोशल मीडिया पेज बनाते हैं जिन पर असली जैसे फॉलोअर्स दिखते हैं, लेकिन गहराई से देखने पर उनकी पोस्टिंग संदिग्ध होती है।

साथ ही, **ऑनलाइन पेमेटं करने से पहले UPI ID या बैकं अकाउंट की वैधता जांचे** ं। किसी अज्ञात व्यक्ति या कंपनी के अकाउंट में सीधे पैसे ट्रांसफर न करें। कैश ऑन डिलीवरी (COD) का विकल्प उपलब्ध हो तो उसे प्राथमिकता दें।

ठगी की शिकायत कहां करे ं

अगर आप किसी ऑनलाइन ठगी का शिकार हो गए हैं, तो तुरंत **साइबर क्राइम हेल्पलाइन नंबर 1930** पर संपर्क करें या **www.cybercrime.gov.in** वेबसाइट पर शिकायत दर्ज करें।
कई बार समय पर शिकायत करने से पुलिस या बैंक खाते को फ्रीज़ कर ठगी गई रकम वापस दिलाने में मदद कर सकती है।

सरकार और ई-कॉमर्स कंपनियों की चेतावनी

हाल ही में इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) ने उपभोक्ताओं को चेताया है कि त्योहारों के मौसम में फर्जी वेबसाइट्स, SMS, और ईमेल से सावधान रहें। मंत्रालय ने कहा है कि "**किसी भी लिंक पर क्लिक करने से पहले दो बार सोचे** ं।"
Flipkart और Amazon जैसी कंपनियों ने भी अपने ग्राहकों को ईमेल और नोटिफिकेशन के जरिए आगाह किया है कि वे किसी **थर्ड पार्टी वेबसाइट** या **कूपन लिंक** से लॉगिन न करें।

दिवाली खुशियों और समृद्धि का पर्व है, लेकिन इन खुशियों में साइबर ठग खलल डालने की कोशिश कर रहे हैं। इसलिए अगर आप भी इस दिवाली ऑनलाइन शॉपिंग करने जा रहे हैं, तो थोड़ी सी सतर्कता आपको बड़े नुकसान से बचा सकती है।

DISCLAIMER: the views/contents expressed/presented herein, within this advertorial and promotional feature are the sole and exclusive responsibility of individual clients/expert/their authorised representative/Publisher, to which effect, publication house/its representative/affiliates are not responsible/liable whatsover.