UPI और पेमेंट धोखाधड़ी जागरूकता

UPI की आम ठगियाँ - नकली कलेक्ट रिक्वेस्ट, QR कोड और फ़र्ज़ी रिफ़ंड - और उनसे बचाव।

ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

UPI से भुगतान तेज़ होता है, इसीलिए ठग भी इसका फ़ायदा उठाते हैं। एक ज़रूरी नियम: UPI PIN सिर्फ़ पैसे भेजते समय डाला जाता है। पैसे पाने के लिए PIN की कभी ज़रूरत नहीं होती। ठग इसी भ्रम का फ़ायदा नकली रिक्वेस्ट, QR कोड, फ़र्ज़ी कस्टमर केयर और 'रिफ़ंड' की कहानियों से उठाते हैं।

यह कैसे काम करता है - और आप इसे कहाँ रोक सकते हैं

लाल बॉक्स ठग की चाल दिखाते हैं। हरे बॉक्स बताते हैं कि आप कड़ी को कहाँ तोड़ सकते हैं।

1. कोई अजनबी कॉल, संदेश, QR कोड या कलेक्ट रिक्वेस्ट भेजता है
2. दावा करता है कि आपको पैसा, रिफंड या इनाम मिलेगा
   - **यहीं रोकें:** पैसा पाने के लिए PIN या स्कैन की ज़रूरत नहीं होती।
3. स्कैन करने, मंज़ूर करने या UPI PIN डालने को कहता है
   - **यहीं रोकें:** अनजान कलेक्ट रिक्वेस्ट अस्वीकार करें। 'पाने' के लिए PIN कभी न डालें।
4. आपके खाते से पैसा निकल जाता है
   - **यहीं रोकें:** तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।



आम चेतावनी के संकेत

- ⚠ कोई कहे कि पैसे या रिफ़ंड 'पाने' के लिए QR स्कैन करें या PIN डालें।
- ⚠ अनजान व्यक्ति की ओर से 'कलेक्ट रिक्वेस्ट' आना, या खरीदार का सामान्य भुगतान की जगह रिक्वेस्ट भेजने पर अड़ना।
- ⚠ बैंक, डिलीवरी सेवा या वॉलेट का बताकर कोई कॉल करे और स्क्रीन-शेयरिंग ऐप इंस्टॉल करने को कहे।
- ⚠ सर्च रिज़ल्ट या सोशल मीडिया से मिला कस्टमर केयर नंबर, आधिकारिक ऐप या वेबसाइट का नहीं।
- ⚠ तुरंत कार्रवाई का दबाव, या ऐसा ऑफ़र जो सच होने के लिए बहुत अच्छा लगे।

बचाव के व्यावहारिक सुझाव

- पैसे पाने के लिए कभी UPI PIN न डालें। अगर स्क्रीन PIN माँग रही है, तो आप पैसे भेज रहे हैं।
- हर पेमेंट रिक्वेस्ट ध्यान से पढ़ें और अनचाही रिक्वेस्ट अस्वीकार करें।
- किसी के कहने पर रिमोट-एक्सेस या स्क्रीन-शेयरिंग ऐप इंस्टॉल न करें।
- कस्टमर केयर नंबर केवल आधिकारिक ऐप, वेबसाइट या कार्ड से लें।
- ट्रांज़ैक्शन लिमिट सही रखें, ऐप लॉक और पेमेंट अलर्ट चालू रखें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ पैसा 'पाने' के लिए QR स्कैन करना	✓ याद रखें: PIN और स्कैन सिर्फ़ पैसा भेजने के लिए हैं
✕ बिना अपेक्षा वाली कलेक्ट रिक्वेस्ट मंज़ूर करना	✓ उसे अस्वीकार करें और UPI ID की रिपोर्ट करें
✕ सर्च में मिले 'कस्टमर केयर' नंबर पर कॉल करना	✓ आधिकारिक ऐप के अंदर का हेल्प सेक्शन इस्तेमाल करना
✕ 'सपोर्ट' के कहने पर स्क्रीन-शेयरिंग ऐप इंस्टॉल करना	✓ मना करें। असली सपोर्ट को आपके फ़ोन का रिमोट एक्सेस नहीं चाहिए

ऐसा हो जाए तो क्या करें

1. तुरंत साइबर अपराध हेल्पलाइन 1930 पर कॉल करें - जल्दी रिपोर्ट करने से पैसा रोके जाने की संभावना बेहतर होती है।
2. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) पर भी शिकायत दर्ज करें।
3. अपने बैंक या पेमेंट ऐप को तुरंत सूचित करें और संबंधित कार्ड, खाता या UPI ID ब्लॉक करवाएँ।
4. स्क्रीनशॉट, ट्रांज़ैक्शन ID, फ़ोन नंबर, UPI ID और चैट सुरक्षित रखें। कुछ भी डिलीट न करें।
5. प्रभावित खातों के पासवर्ड बदलें, और बाद में पैसे 'वापस दिलाने' का दावा करने वाले किसी भी व्यक्ति को OTP या PIN न दें।

आधिकारिक रिपोर्टिंग संसाधन

- साइबर अपराध हेल्पलाइन 1930 (वित्तीय साइबर ठगी के लिए) - 1930
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.in/
- NPCI (UPI) - आधिकारिक जानकारी - https://www.npci.org.in/

- भारतीय रिज़र्व बैंक - जन जागरूकता - https://www.rbi.org.in/

अपना बैंकिंग पासवर्ड, OTP, UPI PIN, कार्ड CVV या पूरा कार्ड नंबर किसी को भी न बताएँ - चाहे वह खुद को बैंक, पुलिस या सरकारी कार्यालय का बताए। यह वेबसाइट कभी भी ये जानकारी नहीं माँगेगी।

यह वेबसाइट केवल शैक्षिक जानकारी के लिए है। यह कोई सरकारी रिपोर्टिंग पोर्टल या आपातकालीन सेवा नहीं है। यदि आप साइबर ठगी का शिकार हुए हैं, तो हर पेज पर दिए गए आधिकारिक माध्यमों से रिपोर्ट करें।
Akshay Kumar Sharma - https://www.youtube.com/@cybersecwithakshay