OTP और सोशल इंजीनियरिंग

ठग कंप्यूटर नहीं, इंसान को निशाना बनाते हैं - और OTP कभी साझा क्यों नहीं करना चाहिए।

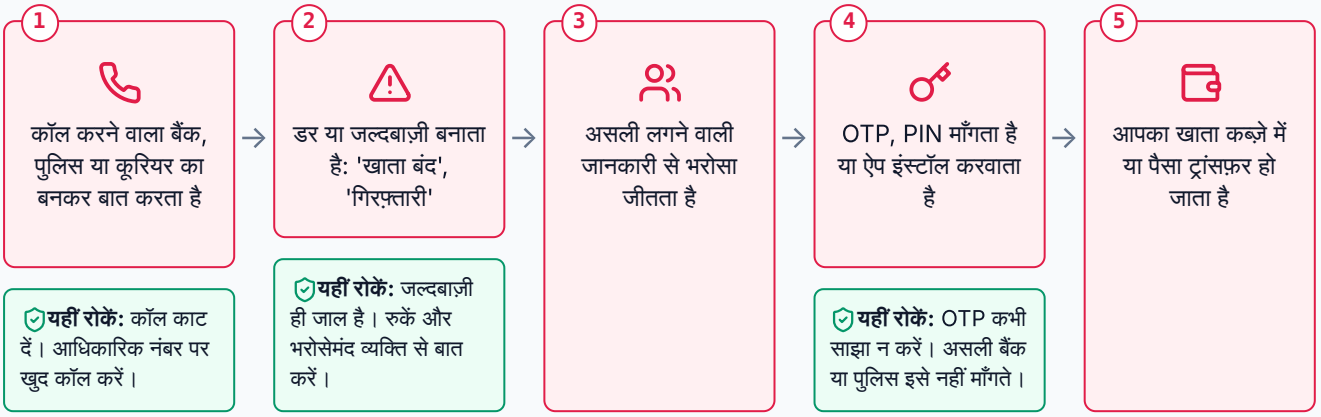
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

सोशल इंजीनियरिंग में भरोसे, डर, जल्दबाज़ी या लालच का इस्तेमाल करके किसी व्यक्ति से जानकारी निकलवाई जाती है या कोई काम करवाया जाता है। OTP इसलिए होता है कि आप साबित कर सकें कि मंज़ूरी आप दे रहे हैं। यदि आप OTP किसी कॉल करने वाले को बता देते हैं, तो आप ठग की कार्रवाई को मंज़ूरी दे देते हैं। इसमें 'डिजिटल अरेस्ट' जैसी कॉल भी आती हैं, जिनमें ठग पुलिस या जाँच एजेंसी बनकर कॉल या वीडियो कॉल करते हैं। अधिकारियों ने साफ़ सलाह दी है कि असली एजेंसियाँ वीडियो कॉल पर गिरफ़्तारी नहीं करतीं और न ही मामला निपटाने के लिए पैसे माँगती 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।





आम चेतावनी के संकेत

- ⚠ बैंक, पुलिस, कस्टम, कूरियर या सरकारी एजेंसी का बताकर कोई OTP, PIN या पैसे माँगे।
- ⚠ कहा जाए कि कॉल न काटें, परिवार को न बताएँ या वीडियो कॉल पर बने रहें।
- ⚠ गिरफ़्तारी, खाता फ़्रीज़ या कानूनी कार्रवाई की धमकी, जब तक आप तुरंत भुगतान या 'वेरिफ़ाई' न करें।
- ⚠ किसी पार्सल या SIM के 'अपराध से जुड़े' होने की कहानी जिसे आप स्वतंत्र रूप से जाँच नहीं सकते।
- ⚠ पैसे 'सुरक्षित खाते' में डालने को कहना।

बचाव के व्यावहारिक सुझाव

- OTP किसी को भी न बताएँ। असली संस्था इसे कभी नहीं माँगती।
- कॉल काट दें। फिर संस्था के आधिकारिक नंबर पर खुद कॉल करें।
- जल्दबाज़ी में न आएँ। किसी धमकी पर कार्रवाई से पहले परिवार या मित्र से बात करें।
- याद रखें: कोई असली एजेंसी वीडियो कॉल पर गिरफ़्तारी नहीं करती और केस बंद करने के लिए पैसे नहीं माँगती।
- सार्वजनिक रूप से अपनी निजी जानकारी कम से कम साझा करें - ठग इसी से अपनी बात विश्वसनीय बनाते हैं।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ खाता 'वेरिफ़ाई' करने के लिए OTP बताना	✓ OTP गोपनीय रखें। इसे सिर्फ़ आप आधिकारिक ऐप में डालें
✗ डर के कारण कॉल पर बने रहना	✓ कॉल काटकर आधिकारिक नंबर पर खुद कॉल करना
✗ 'डिजिटल अरेस्ट' वाली वीडियो कॉल पर यकीन करना	✓ समझें कि यह ठगी है। 1930 पर कॉल करके रिपोर्ट करें
✗ WhatsApp या SMS पर आया ऐप इंस्टॉल करना	✓ ऐप सिर्फ़ आधिकारिक ऐप स्टोर से इंस्टॉल करना

ऐसा हो जाए तो क्या करें

1. कॉल तुरंत काट दें और सभी भुगतान रोक दें।
2. संदिग्ध धोखाधड़ी वाली कॉल या संदेश की रिपोर्ट संचार साथी (चक्षु) पर करें।
3. तुरंत साइबर अपराध हेल्पलाइन 1930 पर कॉल करें - जल्दी रिपोर्ट करने से पैसा रोके जाने की संभावना बेहतर होती है।
4. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) पर भी शिकायत दर्ज करें।
5. अपने बैंक या पेमेंट ऐप को तुरंत सूचित करें और संबंधित कार्ड, खाता या UPI ID ब्लॉक करवाएँ।
6. स्क्रीनशॉट, ट्रांज़ैक्शन ID, फ़ोन नंबर, UPI ID और चैट सुरक्षित रखें। कुछ भी डिलीट न करें।
7. 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/
- संचार साथी - संदिग्ध धोखाधड़ी कॉल/संदेश की रिपोर्ट (चक्षु) - https://sancharsaathi.gov.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