SECURING HUMAN FOUNDATION

⚠ साइबर सावधान

जागरूकता ही सुरक्षा

OTP या लिंक के बिना भी खाली हो सकता है आपका बैंक खाता!

ठग अब OTP माँगे बिना या लिंक भेजे बिना भी खाते से पैसे निकाल लेते हैं। जानिए वे कैसे ठगते हैं — और आप कैसे बच सकते हैं।



ठग कैसे ठगते हैं?

आधार बायोमेट्रिक (AePS) धोखाधड़ी

दस्तावेज़ों या संपत्ति रजिस्ट्री से उंगलियों के निशान की नकल बनाकर, आधार आधारित भुगतान (AePS) से बिना OTP के पैसे निकाल लेते हैं।

SIM स्वैप / e-SIM धोखाधड़ी

आपके नंबर का नया SIM या e-SIM निकलवा लेते हैं। फ़ोन "No Network" दिखाता है और सारे OTP ठग के पास पहुँच जाते हैं।

कॉल फ़ॉरवर्डिंग का खेल

"कूरियर" या "कस्टमर केयर" बनकर `*401*` जैसा कोड डायल करवाते हैं। फिर आपकी कॉल और OTP ठग के नंबर पर चले जाते हैं।

नकली APK फ़ाइल

WhatsApp पर "शादी का कार्ड", "ट्रैफ़िक चालान", "PM किसान" या "बैंक KYC" नाम से .apk फ़ाइल भेजते हैं। इंस्टॉल करते ही SMS और बैंक ऐप ठग के कब्ज़े में।

स्क्रीन शेयरिंग ऐप

"मदद" के बहाने AnyDesk, TeamViewer जैसे ऐप डाउनलोड करवाते हैं और आपका फ़ोन दूर बैठे चलाते हैं।

पब्लिक Wi-Fi और चार्जिंग पॉइंट

पब्लिक Wi-Fi या अनजान USB चार्जिंग पॉइंट पर बैंकिंग करने से फ़ोन का डेटा चोरी होने का खतरा रहता है।

ठगी हो तो तुरंत डायल करें 1930 | www.cybercrime.gov.in

SECURING HUMAN FOUNDATION

🛡 सुरक्षित रहें

सुरक्षित रहने के लिए क्या करें?

- ✓ **आधार बायोमेट्रिक लॉक करें** — myAadhaar पोर्टल (myaadhaar.uidai.gov.in) या mAadhaar ऐप से। ज़रूरत हो तभी अनलॉक करें।
- ✓ **"मास्क्ड आधार" दें** — फ़ोटोकॉपी देते समय उस पर उद्देश्य और तारीख लिखकर हस्ताक्षर करें।
- ✓ **ऐप सिर्फ़ Play Store / App Store से** — WhatsApp या SMS पर आई .apk फ़ाइल कभी न खोलें।
- ✓ **अनजान के कहने पर कोई कोड डायल न करें।** कॉल फ़ॉरवर्डिंग जाँचने के लिए `*#21#`, बंद करने के लिए `##002#` डायल करें।
- ✓ **फ़ोन में देर तक नेटवर्क न आए** तो तुरंत मोबाइल कंपनी और बैंक से संपर्क करें।
- ✓ **स्क्रीन शेयरिंग ऐप इंस्टॉल न करें** — कोई बैंक या कंपनी ऐसा करने को नहीं कहती।
- ✓ **ट्रांज़ैक्शन लिमिट कम रखें;** ज़रूरत न हो तो ऑनलाइन और अंतरराष्ट्रीय लेन-देन बंद रखें।
- ✓ **SMS और ईमेल अलर्ट चालू रखें** और बैंक स्टेटमेंट नियमित जाँचें।
- ✓ **पब्लिक Wi-Fi पर बैंकिंग न करें;** अपना चार्जर और मोबाइल डेटा इस्तेमाल करें।
- ✓ **बैंक कभी फ़ोन पर** PIN, पासवर्ड, CVV या OTP नहीं माँगता — किसी को न बताएँ।

🚨 ठगी हो जाए तो तुरंत क्या करें?

राष्ट्रीय साइबर क्राइम हेल्पलाइन

1930

24 × 7 · निःशुल्क

राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल

www.cybercrime.gov.in

ऑनलाइन शिकायत दर्ज करें

1. **तुरंत 1930 पर कॉल करें।** पहले घंटे (गोल्डन आवर) में शिकायत करने पर पैसे रोके जा सकते हैं।
2. **बैंक को सूचित करें** और खाता, कार्ड, UPI तुरंत ब्लॉक करवाएँ।
3. **सबूत सँभालकर रखें** — ट्रांज़ैक्शन ID, स्क्रीनशॉट, मैसेज और कॉल का विवरण।
4. **cybercrime.gov.in** पर शिकायत दर्ज करें और शिकायत नंबर सँभालकर रखें।

🚫 **संदिग्ध कॉल, SMS या WhatsApp मैसेज की शिकायत** संचार साथी पोर्टल पर "चक्षु" से करें: **www.sancharsaathi.gov.in**

याद रखें: डर या जल्दबाज़ी में फ़ैसला न लें — रुकें, सोचें, फिर कदम उठाएँ।