AI आधारित ठगी

आवाज़ की नकल, डीपफ़ेक वीडियो और AI से लिखे संदेश - और वे सरल जाँचें जो अब भी काम करती हैं।

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

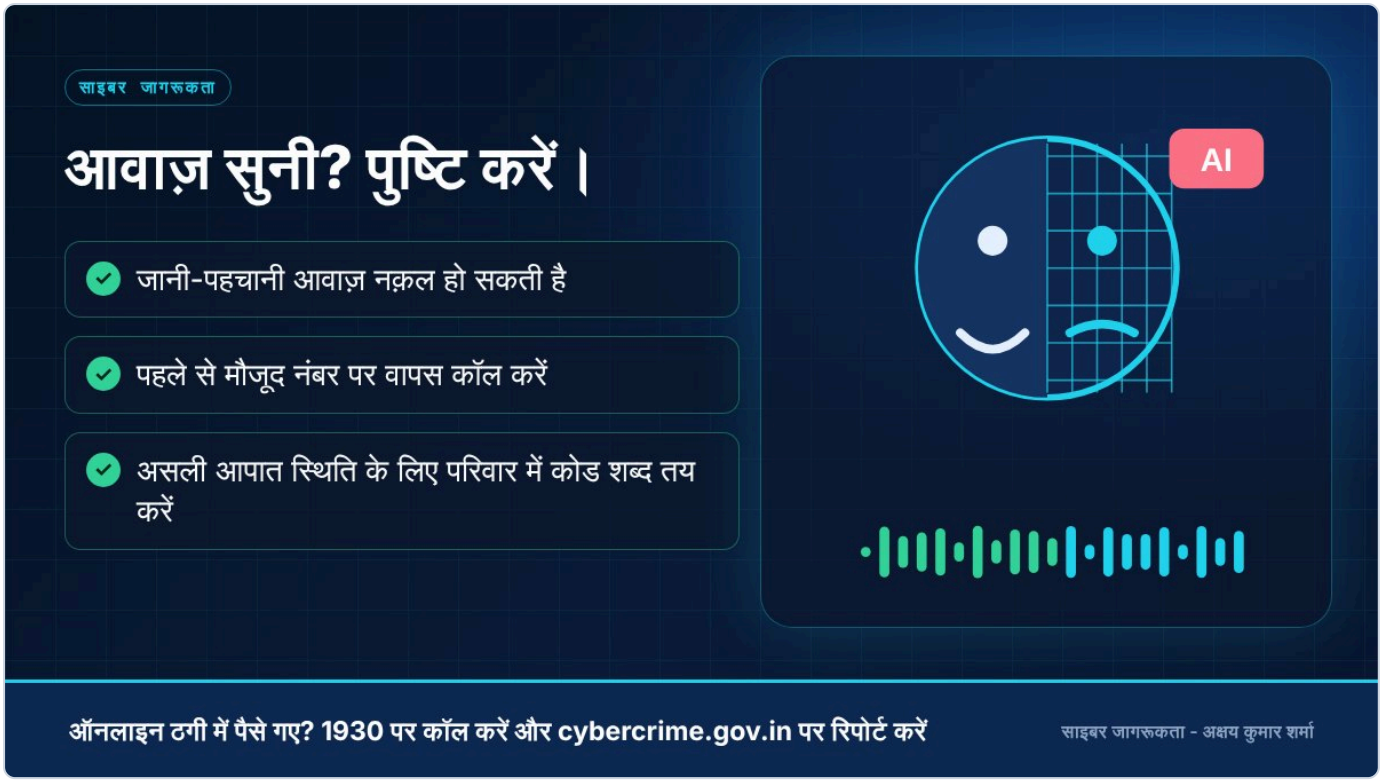
यह क्या है

AI टूल से किसी की आवाज़ की नकल करना, असली जैसे नकली वीडियो बनाना और किसी भी भाषा में विश्वसनीय संदेश लिखना आसान हो गया है। ठग किसी रिश्तेदार जैसी आवाज़ में आपातकालीन पैसे माँगते हुए कॉल कर सकता है, या किसी जानी-मानी हस्ती का नकली वीडियो दिखाकर निवेश का प्रचार कर सकता है। तकनीक नई है, पर तरीका वही पुराना है: भरोसा और जल्दबाज़ी।

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. ठग इंटरनेट से आवाज़, फ़ोटो और वीडियो इकट्ठा करते हैं
   - **यहीं रोकें:** सार्वजनिक आवाज़ और वीडियो सीमित रखें।
2. AI आवाज़ या चेहरे की नक़ल बना देता है (डीपफ़ेक)
3. आपको कॉल या वीडियो आता है: 'रिश्तेदार मुसीबत में है' या 'बॉस को पैसे चाहिए'
   - **यहीं रोकें:** व्यक्ति को उसके पहले से मौजूद नंबर पर कॉल करके पुष्टि करें।
4. आप घबराहट में पैसे भेज देते हैं
   - **यहीं रोकें:** रुकें। असली आपात स्थिति के लिए परिवार में एक कोड शब्द तय करें।
5. असली व्यक्ति ने वह कॉल की ही नहीं थी



आम चेतावनी के संकेत

- ⚠ नए नंबर से 'रिश्तेदार' या 'दोस्त' का अचानक पैसे माँगने वाला कॉल या वॉइस नोट।
- ⚠ किसी मशहूर व्यक्ति का किसी स्कीम या गिवअवे का प्रचार करता वीडियो या ऑडियो।
- ⚠ बिल्कुल सही लिखे संदेश जो असामान्य काम या भुगतान माँगते हैं।
- ⚠ वीडियो कॉल जिसमें चेहरे या होंठ की हरकत थोड़ी अजीब लगे, या कॉल की क्वालिटी सुविधाजनक रूप से ख़राब हो।
- ⚠ दूसरे माध्यम से जाँच न करने का दबाव।

बचाव के व्यावहारिक सुझाव

- परिवार में कोई 'सेफ़ वर्ड' तय करें या ऐसा सवाल पूछें जिसका जवाब सिर्फ़ असली व्यक्ति जानता हो।
- पैसे भेजने से पहले कॉल काटकर उस व्यक्ति के पुराने, ज्ञात नंबर पर फ़ोन करें।
- मशहूर हस्तियों वाले निवेश प्रचार से सावधान रहें और आधिकारिक माध्यम से जाँचें।
- सार्वजनिक रूप से आवाज़ और वीडियो के नमूने कम रखें और सोशल प्रोफ़ाइल निजी रखें।
- आवाज़ या चेहरा कितना भी असली लगे, जल्दबाज़ी को चेतावनी का संकेत मानें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ सिर्फ़ जानी-पहचानी आवाज़ पर भरोसा करना	✓ दूसरे माध्यम से पुष्टि करना
✗ 'इमरजेंसी' पर तुरंत पैसे भेजना	✓ रुककर व्यक्ति को सीधे कॉल करना
✗ निवेश का प्रचार करने वाले सेलिब्रिटी वीडियो पर यकीन करना	✓ उस व्यक्ति या कंपनी के आधिकारिक चैनल जाँचना
✗ अनजान AI ऐप में अपनी फ़ोटो अपलोड करना	✓ भरोसेमंद ऐप इस्तेमाल करना और प्राइवेसी शर्तें पढ़ना

ऐसा हो जाए तो क्या करें

1. सभी भुगतान रोकें और दूसरे माध्यम से जाँच करें।
2. कॉल, संदेश या नकली प्रोफ़ाइल की रिपोर्ट प्लेटफ़ॉर्म पर करें, और फ़ोन से आया हो तो संचार साथी पर भी।
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

- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.in/
- साइबर अपराध हेल्पलाइन 1930 (वित्तीय साइबर ठगी के लिए) - 1930
- संचार साथी - संदिग्ध धोखाधड़ी कॉल/संदेश की रिपोर्ट (चक्षु) - https://sancharsaathi.gov.in/
- CERT-In (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल) - https://www.cert-in.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