डिजिटल फुटप्रिंट और प्राइवेसी

आप ऑनलाइन क्या छोड़ जाते हैं, उसे कौन देख सकता है, और जोखिम कैसे घटाएँ।

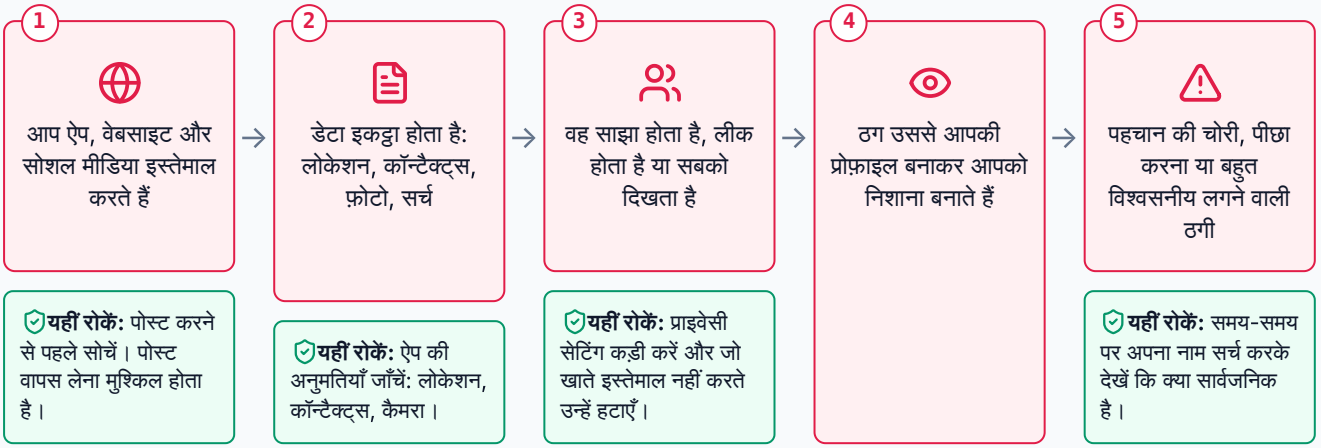
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

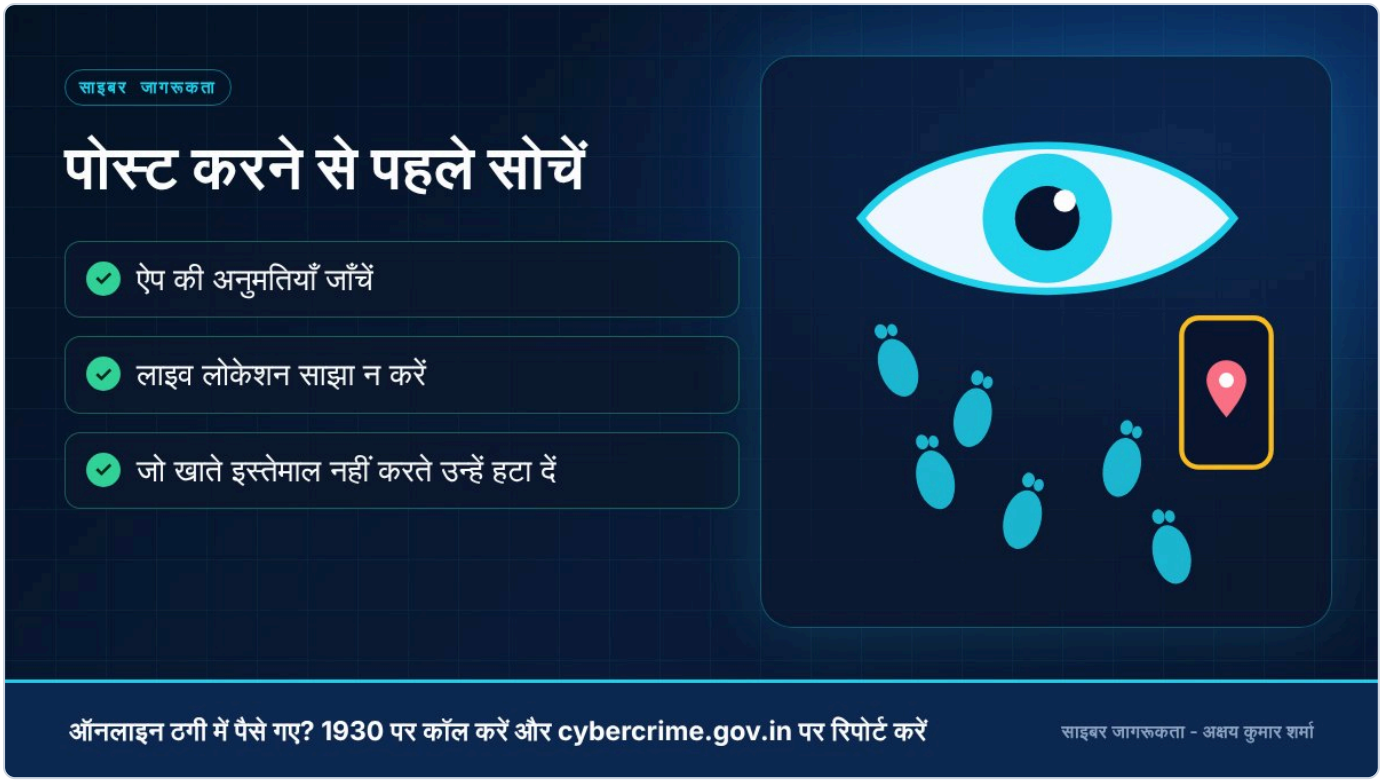
यह क्या है

आपका डिजिटल फ़ुटप्रिंट ऑनलाइन आपकी जानकारी का वह निशान है: पोस्ट, फ़ोटो, कमेंट, ऐप डेटा, लोकेशन और वेबसाइट द्वारा जुटाई गई जानकारी। ठग और पीछा करने वाले छोटी-छोटी जानकारी जोड़कर आपकी नकल कर सकते हैं या आपको निशाना बना सकते 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

- ⚠ ऐप ऐसी अनुमतियाँ माँगें जिनकी ज़रूरत नहीं, जैसे साधारण टूल के लिए कॉन्टैक्ट या लोकेशन।
- ⚠ सार्वजनिक प्रोफ़ाइल पर फ़ोन नंबर, पता, स्कूल/कार्यस्थल या रोज़ की दिनचर्या दिखना।
- ⚠ दस्तावेज़ों, टिकट या कार्ड की फ़ोटो अक्सर ऑनलाइन साझा करना।
- ⚠ पुराने अकाउंट जो आप इस्तेमाल नहीं करते, अब भी चालू हैं।
- ⚠ अजनबी आपकी निजी जानकारी जानते हैं, जबकि आपने बताई नहीं।

बचाव के व्यावहारिक सुझाव

- ऐप की अनुमतियाँ जाँचें और गैर-ज़रूरी हटा दें।
- सोशल प्रोफ़ाइल को अपनी सहूलियत के अनुसार सबसे निजी सेटिंग पर रखें।
- ID दस्तावेज़, बोर्डिंग पास, टिकट या लाइव लोकेशन पोस्ट न करें।
- जो अकाउंट और ऐप अब इस्तेमाल नहीं करते, उन्हें हटा दें।
- पोस्ट करने से पहले सोचें: एक बार साझा होने के बाद वह कहाँ जाएगा, इस पर पूरा नियंत्रण नहीं रहता।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ हर ऐप को हर अनुमति देना	✓ सिर्फ़ वही अनुमति देना जो ऐप को सच में चाहिए
✗ लाइव लोकेशन और यात्रा की योजना पोस्ट करना	✓ बाद में और सिर्फ़ करीबी लोगों से साझा करना
✗ बैंकिंग के लिए सार्वजनिक Wi-Fi इस्तेमाल करना	✓ मोबाइल डेटा या भरोसेमंद नेटवर्क इस्तेमाल करना
✗ पहचान पत्रों की फ़ोटो यूँ ही भेज देना	✓ सिर्फ़ ज़रूरत पर और भरोसेमंद पक्ष को ही देना

ऐसा हो जाए तो क्या करें

1. पोस्ट या जानकारी हटाएँ या छिपाएँ और ज़रूरत हो तो साइट/प्लेटफ़ॉर्म से उसे हटवाने का अनुरोध करें।
2. प्राइवेसी सेटिंग कड़ी करें और यदि निजी जानकारी से पासवर्ड का अंदाज़ा लग सकता है तो पासवर्ड बदलें।
3. यदि कोई आपकी जानकारी का दुरुपयोग या उत्पीड़न कर रहा है, तो सबूत सुरक्षित रखें और cybercrime.gov.in पर रिपोर्ट करें।

आधिकारिक रिपोर्टिंग संसाधन

- CERT-In (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल) - https://www.cert-in.org.in/
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.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