मैलवेयर और संदिग्ध ऐप

हानिकारक ऐप और फ़ाइलें डिवाइस में कैसे पहुँचती हैं, और अपने फ़ोन-कंप्यूटर को साफ़ कैसे रखें।

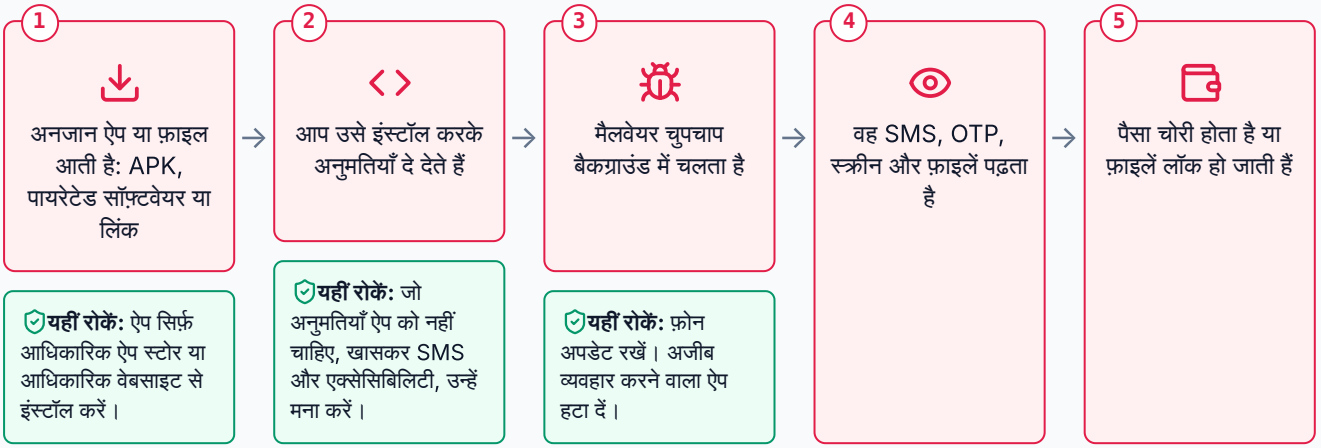
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

मैलवेयर ऐसा सॉफ़्टवेयर है जो आपको नुकसान पहुँचाने या आपकी जासूसी करने के लिए बनाया जाता है: पासवर्ड चुराना, संदेश पढ़ना, फ़ाइलें लॉक करना या डिवाइस पर कब्ज़ा करना। यह आम तौर पर नकली ऐप, चैट में भेजी गई APK फ़ाइलों, क्रैक सॉफ़्टवेयर या ईमेल अटैचमेंट से आता है।

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

- ⚠ चैट में भेजा गया ऐप या फ़ाइल, जिसे आधिकारिक ऐप स्टोर के बाहर से इंस्टॉल करने को कहा जाए।
- ⚠ ऐसे ऐप जो बिना स्पष्ट कारण एक्सेसिबिलिटी, SMS या डिवाइस-एडमिन अनुमति माँगें।
- ⚠ बैटरी जल्दी ख़त्म होना, डिवाइस धीमा होना, या अनजान ऐप दिखना।
- ⚠ पॉप-अप, रीडायरेक्ट, या आपके नंबर से ऐसे संदेश जाना जो आपने नहीं भेजे।
- ⚠ 'बैंक', 'KYC', 'बिजली बिल' या 'RTO चालान' के नाम पर संदेश में भेजा गया ऐप या APK।

बचाव के व्यावहारिक सुझाव

- ऐप केवल आधिकारिक ऐप स्टोर से इंस्टॉल करें और प्रकाशक तथा रिव्यू जाँचें।
- संदेशों में मिली APK फ़ाइलें कभी इंस्टॉल न करें, भले ही संपर्क ने भेजी हों।
- ऑपरेटिंग सिस्टम और ऐप अपडेट रखें और भरोसेमंद सिक्योरिटी ऐप इस्तेमाल करें।
- पायरेटेड या क्रैक सॉफ़्टवेयर से बचें।
- ऐप की अनुमतियाँ जाँचें और जो ऐप न पहचानें उसे हटा दें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ WhatsApp या Telegram पर आई APK इंस्टॉल करना	✓ सिर्फ़ आधिकारिक ऐप स्टोर इस्तेमाल करना
✕ क्रैक या पायरेटेड सॉफ़्टवेयर इस्तेमाल करना	✓ असली या मुफ़्त ओपन-सोर्स सॉफ़्टवेयर इस्तेमाल करना
✕ सिस्टम और ऐप अपडेट को अनदेखा करना	✓ फ़ोन और ऐप अपडेट रखना
✕ फ़ाइलों का बैकअप कभी न लेना	✓ नियमित बैकअप रखना, हो सके तो ऑफ़लाइन भी

ऐसा हो जाए तो क्या करें

1. इंटरनेट से डिस्कनेक्ट करें, संदिग्ध ऐप हटाएँ और सिक्योरिटी स्कैन चलाएँ।
2. किसी साफ़ डिवाइस से पासवर्ड बदलें, पहले ईमेल और बैंकिंग के।
3. यदि डिवाइस में बैंकिंग ऐप हैं तो बैंक से संपर्क करें। ज़रूरत हो तो ज़रूरी डेटा का बैकअप लेकर डिवाइस रीसेट करें।
4. cybercrime.gov.in पर रिपोर्ट करें, और पैसे गए हों तो 1930 पर।

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