पासवर्ड और अकाउंट सुरक्षा

मज़बूत पासवर्ड, टू-फ़ैक्टर ऑथेंटिकेशन और सुरक्षित अकाउंट रिकवरी की व्यावहारिक आदतें।

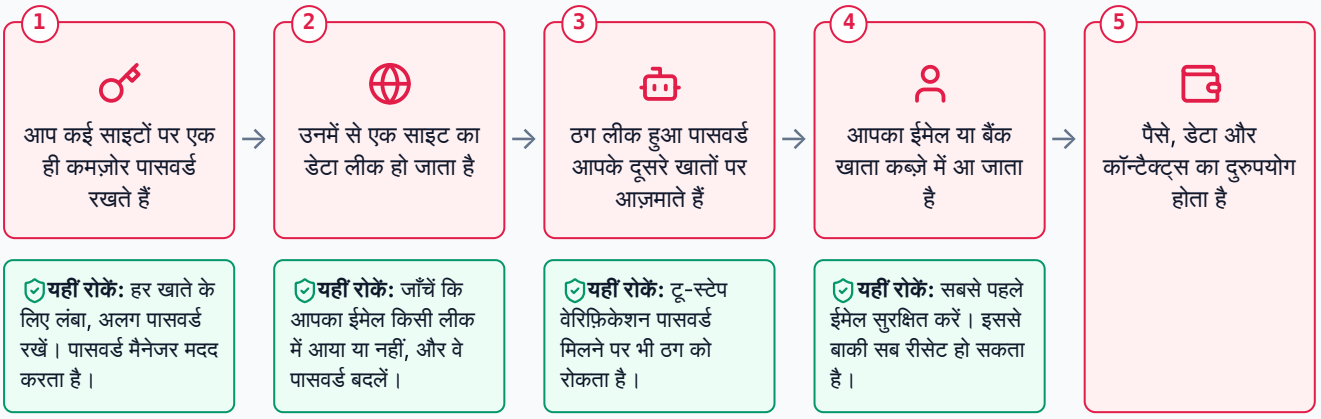
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

मज़बूत पासवर्ड सुरक्षा की सिर्फ़ एक परत है। सबसे बड़े खतरे हैं - हर जगह एक ही पासवर्ड रखना और फ़िशिंग में फँसना। जब कोई वेबसाइट पासवर्ड लीक करती है, तो हमलावर वही संयोजन आपके ईमेल, बैंकिंग और सोशल अकाउंट पर आज़माते 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

- ⚠ कई वेबसाइट पर एक जैसा पासवर्ड इस्तेमाल करना।
- ⚠ पासवर्ड छोटा है, कोई नाम, तारीख या आम शब्द है।
- ⚠ अनजान जगह या डिवाइस से लॉगिन के सिक्योरिटी अलर्ट मिलना।
- ⚠ आपका ईमेल या फ़ोन नंबर किसी ज्ञात डेटा लीक में दिखना।
- ⚠ ईमेल या बैंकिंग पर कभी टू-फ़ैक्टर ऑथेंटिकेशन चालू न किया हो।

बचाव के व्यावहारिक सुझाव

- लंबा पासफ़्रेज़ (कई असंबंधित शब्द) रखें या पासवर्ड मैनेजर से अलग-अलग पासवर्ड बनाएँ और सुरक्षित रखें।
- पासवर्ड दोबारा इस्तेमाल न करें, ख़ासकर ईमेल के लिए, क्योंकि उससे आपके बाकी अकाउंट रीसेट हो सकते हैं।
- टू-फ़ैक्टर ऑथेंटिकेशन चालू करें, संभव हो तो SMS की जगह ऑथेंटिकेटर ऐप से।
- रिकवरी ईमेल और फ़ोन नंबर अपडेट रखें।
- पासवर्ड साधारण नोट में न लिखें और चैट में साझा न करें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ 'password123' या जन्मतिथि रखना	✓ बेतरतीब शब्दों का लंबा पासफ़्रेज़ रखना
✗ हर साइट पर एक ही पासवर्ड रखना	✓ हर खाते के लिए अलग पासवर्ड रखना
✗ टू-स्टेप वेरिफ़िकेशन छोड़ देना	✓ इसे चालू करना, बेहतर है ऑथेंटिकेटर ऐप के साथ
✗ पासवर्ड नोट्स या चैट ऐप में रखना	✓ भरोसेमंद पासवर्ड मैनेजर में रखना

ऐसा हो जाए तो क्या करें

1. प्रभावित अकाउंट और जहाँ-जहाँ वही पासवर्ड था, वहाँ तुरंत पासवर्ड बदलें।
2. सभी सेशन से लॉग आउट करें और जुड़े हुए ऐप तथा रिकवरी विवरण जाँचें।
3. किसी भरोसेमंद चेकर से देखें कि आपका ईमेल किसी डेटा लीक में है या नहीं।
4. यदि पैसे या पहचान का दुरुपयोग हुआ है, तो cybercrime.gov.in पर (और वित्तीय ठगी के लिए 1930 पर) रिपोर्ट करें।

आधिकारिक रिपोर्टिंग संसाधन

- CERT-In (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल) - https://www.cert-in.org.in/
- Have I Been Pwned (तृतीय-पक्ष डेटा लीक जाँच) - https://haveibeenpwned.com/

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