फ़िशिंग और नकली वेबसाइट

नकली ईमेल, SMS और वेबसाइट कैसे आपसे लॉगिन, पैसे या निजी जानकारी हड़प लेते हैं।

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

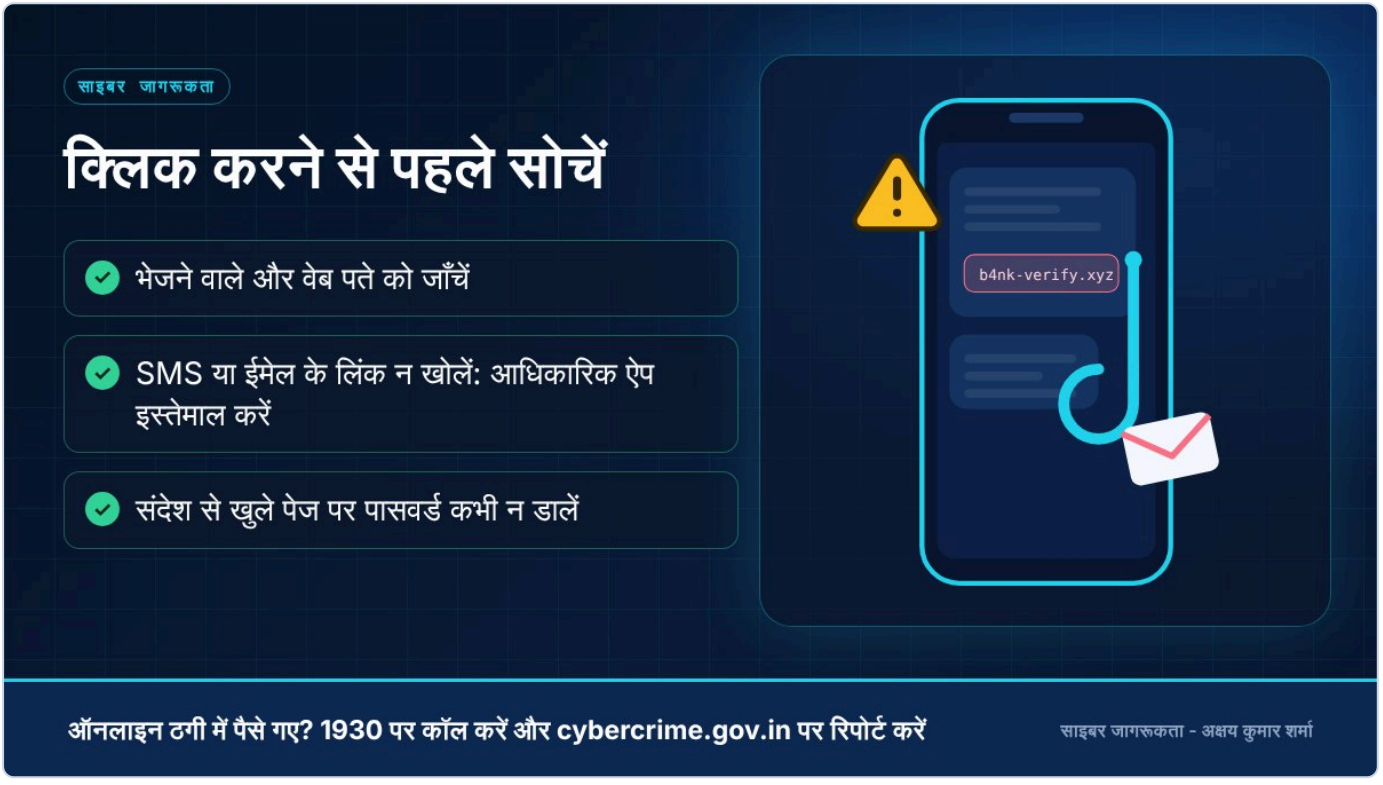
यह क्या है

फ़िशिंग में ठग किसी भरोसेमंद संस्था - जैसे बैंक, कूरियर, सरकारी विभाग या कोई जानी-पहचानी कंपनी - का रूप धरकर आपसे लिंक खुलवाते हैं, फ़ाइल डाउनलोड करवाते हैं या आपकी जानकारी भरवाते हैं। लिंक अक्सर ऐसी नकली वेबसाइट पर ले जाता है जो असली जैसी दिखती है। वहाँ भरी गई हर जानकारी सीधे ठग तक पहुँच जाती 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।

1. नकली ईमेल या SMS आता है
   - **यहीं रोकें:** भेजने वाले को जाँचें। जल्दबाज़ी वाली धमकी चेतावनी का संकेत है।
2. आप लिंक पर क्लिक करते हैं
   - **यहीं रोकें:** क्लिक न करें। आधिकारिक ऐप खोलें या पता खुद टाइप करें।
3. हू-ब-हू नकली वेबसाइट खुलती है
   - **यहीं रोकें:** वेब पता अक्षर-अक्षर पढ़ें। सिर्फ़ ताले का निशान सबूत नहीं है।
4. आप लॉगिन या कार्ड की जानकारी डालते हैं
   - **यहीं रोकें:** संदेश से खुले पेज पर कभी जानकारी न डालें।
5. ठग आपका खाता या पैसा ले लेता है



आम चेतावनी के संकेत

- ⚠ जल्दबाज़ी या डराने वाली भाषा: 'आपका खाता आज ही बंद हो जाएगा', 'आख़िरी चेतावनी'।
- ⚠ भेजने वाले का पता या वेबसाइट का पता असली से थोड़ा अलग होता है (अक्षर बदले हुए, अजीब डोमेन)।
- ⚠ बिना माँगे आया कोई लिंक या अटैचमेंट, ख़ासकर अनजान नंबर या पते से।
- ⚠ लिंक के ज़रिए पासवर्ड, OTP, कार्ड विवरण या KYC अपडेट माँगना।
- ⚠ वर्तनी की गलतियाँ, अजीब बनावट, या संदेश से खुला लॉगिन पेज।

बचाव के व्यावहारिक सुझाव

- अनचाहे संदेशों के लिंक पर क्लिक न करें। आधिकारिक ऐप खोलें या वेबसाइट का पता खुद टाइप करें।
- कोई भी जानकारी भरने से पहले पूरा वेब पता ध्यान से जाँचें।
- ज़रूरी खातों पर टू-फ़ैक्टर ऑथेंटिकेशन चालू रखें।
- फ़ोन, ब्राउज़र और सिक्योरिटी सॉफ़्टवेयर अपडेट रखें।
- संदेह हो तो संस्था की आधिकारिक वेबसाइट या कार्ड पर छपे नंबर पर संपर्क करें, संदेश में दिए नंबर पर नहीं।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ 'खाता बंद होगा' वाले SMS का लिंक खोलना	✓ बैंक का आधिकारिक ऐप सीधे खोलना
✕ सिर्फ़ ताले का निशान देखकर साइट पर भरोसा करना	✓ पूरा वेब पता ध्यान से पढ़ना
✕ बिना अपेक्षा वाली अटैचमेंट खोलना	✓ भेजने वाले से पहले से जाने हुए नंबर पर पुष्टि करना
✕ संदेश से खुले पेज पर पासवर्ड डालना	✓ पता खुद टाइप करना या बुकमार्क इस्तेमाल करना

ऐसा हो जाए तो क्या करें

1. यदि सिर्फ़ लिंक खोला है, तो पेज बंद करें, कुछ भी न भरें और डिवाइस का सिक्योरिटी स्कैन चलाएँ।
2. यदि पासवर्ड डाल दिया है, तो असली वेबसाइट पर तुरंत बदलें और जहाँ-जहाँ वही पासवर्ड इस्तेमाल किया है वहाँ भी बदलें।
3. यदि बैंकिंग या कार्ड जानकारी दी है, तो तुरंत बैंक से संपर्क करें और नीचे दिए गए चरण अपनाएँ।
4. तुरंत साइबर अपराध हेल्पलाइन 1930 पर कॉल करें - जल्दी रिपोर्ट करने से पैसा रोके जाने की संभावना बेहतर होती है।
5. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) पर भी शिकायत दर्ज करें।
6. अपने बैंक या पेमेंट ऐप को तुरंत सूचित करें और संबंधित कार्ड, खाता या UPI ID ब्लॉक करवाएँ।
7. स्क्रीनशॉट, ट्रांज़ैक्शन ID, फ़ोन नंबर, UPI ID और चैट सुरक्षित रखें। कुछ भी डिलीट न करें।
8. 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