साइबर जागरूकता गाइड

ऑनलाइन खतरों पर सरल भाषा में गाइड, चित्रों सहित

लेखक Akshay Kumar Sharma

1. फ़िशिंग और नकली वेबसाइट
2. UPI और पेमेंट धोखाधड़ी जागरूकता
3. OTP और सोशल इंजीनियरिंग
4. ऑनलाइन नौकरी और निवेश ठगी
5. सोशल मीडिया सुरक्षा
6. पासवर्ड और अकाउंट सुरक्षा
7. डिजिटल फ़ुटप्रिंट और प्राइवेसी
8. AI आधारित ठगी
9. मैलवेयर और संदिग्ध ऐप
10. विद्यार्थियों और परिवारों के लिए साइबर सुरक्षा

यह केवल शैक्षिक जानकारी है। संपर्क विवरण हमेशा सूचीबद्ध आधिकारिक वेबसाइटों पर जाँचें।

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।

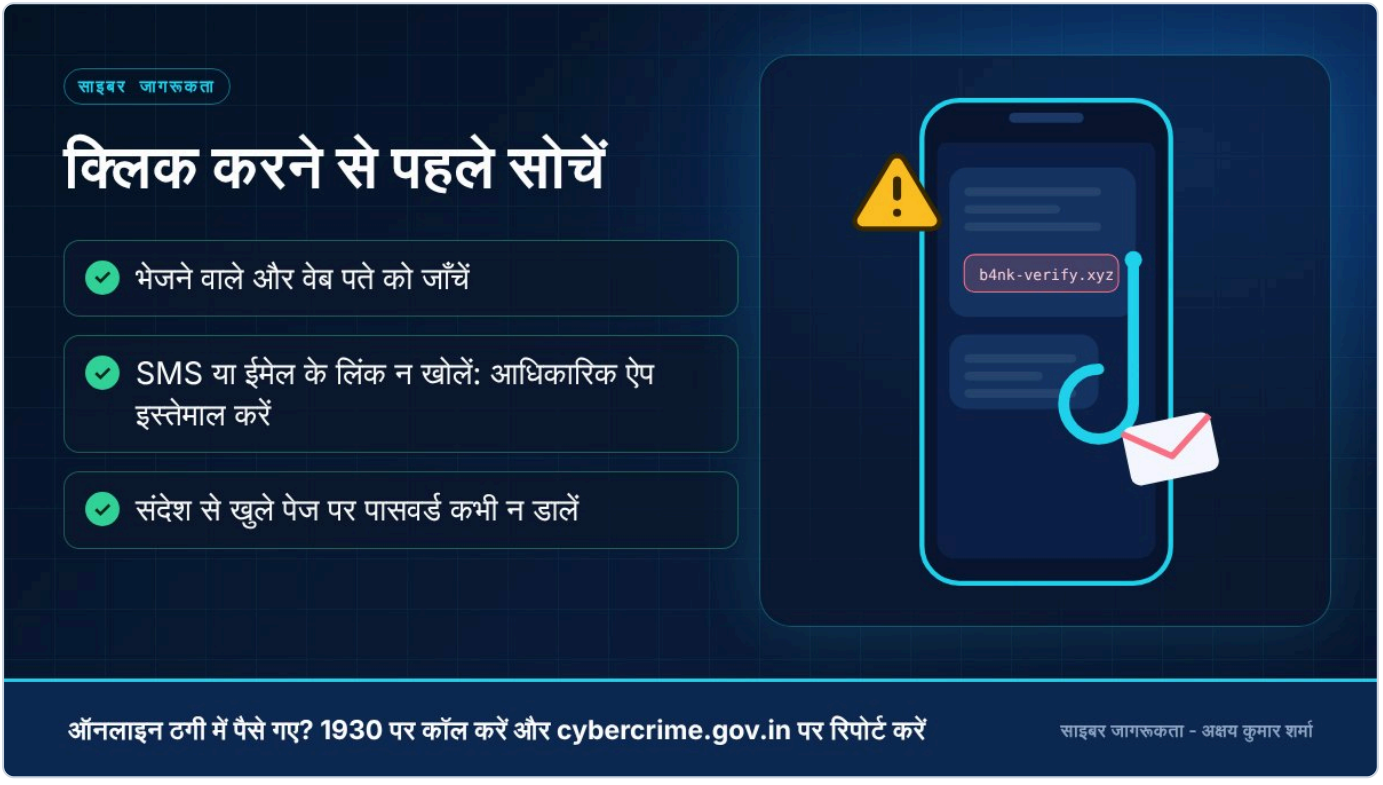
यह क्या है

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

UPI और पेमेंट धोखाधड़ी जागरूकता

UPI की आम ठगियाँ - नकली कलेक्ट रिक्वेस्ट, QR कोड और फ़र्ज़ी रिफ़ंड - और उनसे बचाव।

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

यह क्या है

UPI से भुगतान तेज़ होता है, इसीलिए ठग भी इसका फ़ायदा उठाते हैं। एक ज़रूरी नियम: UPI PIN सिर्फ़ पैसे भेजते समय डाला जाता है। पैसे पाने के लिए PIN की कभी ज़रूरत नहीं होती। ठग इसी भ्रम का फ़ायदा नकली रिक्वेस्ट, QR कोड, फ़र्ज़ी कस्टमर केयर और 'रिफ़ंड' की कहानियों से उठाते 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।

1. कोई अजनबी कॉल, संदेश, QR कोड या कलेक्ट रिक्वेस्ट भेजता है
2. दावा करता है कि आपको पैसा, रिफंड या इनाम मिलेगा
   - **यहीं रोकें:** पैसा पाने के लिए PIN या स्कैन की ज़रूरत नहीं होती।
3. स्कैन करने, मंज़ूर करने या UPI PIN डालने को कहता है
   - **यहीं रोकें:** अनजान कलेक्ट रिक्वेस्ट अस्वीकार करें। 'पाने' के लिए PIN कभी न डालें।
4. आपके खाते से पैसा निकल जाता है
   - **यहीं रोकें:** तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।



आम चेतावनी के संकेत

- ⚠ कोई कहे कि पैसे या रिफ़ंड 'पाने' के लिए QR स्कैन करें या PIN डालें।
- ⚠ अनजान व्यक्ति की ओर से 'कलेक्ट रिक्वेस्ट' आना, या खरीदार का सामान्य भुगतान की जगह रिक्वेस्ट भेजने पर अड़ना।
- ⚠ बैंक, डिलीवरी सेवा या वॉलेट का बताकर कोई कॉल करे और स्क्रीन-शेयरिंग ऐप इंस्टॉल करने को कहे।
- ⚠ सर्च रिज़ल्ट या सोशल मीडिया से मिला कस्टमर केयर नंबर, आधिकारिक ऐप या वेबसाइट का नहीं।
- ⚠ तुरंत कार्रवाई का दबाव, या ऐसा ऑफ़र जो सच होने के लिए बहुत अच्छा लगे।

बचाव के व्यावहारिक सुझाव

- पैसे पाने के लिए कभी UPI PIN न डालें। अगर स्क्रीन PIN माँग रही है, तो आप पैसे भेज रहे हैं।
- हर पेमेंट रिक्वेस्ट ध्यान से पढ़ें और अनचाही रिक्वेस्ट अस्वीकार करें।
- किसी के कहने पर रिमोट-एक्सेस या स्क्रीन-शेयरिंग ऐप इंस्टॉल न करें।
- कस्टमर केयर नंबर केवल आधिकारिक ऐप, वेबसाइट या कार्ड से लें।
- ट्रांज़ैक्शन लिमिट सही रखें, ऐप लॉक और पेमेंट अलर्ट चालू रखें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ पैसा 'पाने' के लिए QR स्कैन करना	✓ याद रखें: PIN और स्कैन सिर्फ़ पैसा भेजने के लिए हैं
✕ बिना अपेक्षा वाली कलेक्ट रिक्वेस्ट मंज़ूर करना	✓ उसे अस्वीकार करें और UPI ID की रिपोर्ट करें
✕ सर्च में मिले 'कस्टमर केयर' नंबर पर कॉल करना	✓ आधिकारिक ऐप के अंदर का हेल्प सेक्शन इस्तेमाल करना
✕ 'सपोर्ट' के कहने पर स्क्रीन-शेयरिंग ऐप इंस्टॉल करना	✓ मना करें। असली सपोर्ट को आपके फ़ोन का रिमोट एक्सेस नहीं चाहिए

ऐसा हो जाए तो क्या करें

1. तुरंत साइबर अपराध हेल्पलाइन 1930 पर कॉल करें - जल्दी रिपोर्ट करने से पैसा रोके जाने की संभावना बेहतर होती है।
2. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) पर भी शिकायत दर्ज करें।
3. अपने बैंक या पेमेंट ऐप को तुरंत सूचित करें और संबंधित कार्ड, खाता या UPI ID ब्लॉक करवाएँ।
4. स्क्रीनशॉट, ट्रांज़ैक्शन ID, फ़ोन नंबर, UPI ID और चैट सुरक्षित रखें। कुछ भी डिलीट न करें।
5. 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

- साइबर अपराध हेल्पलाइन 1930 (वित्तीय साइबर ठगी के लिए) - 1930
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.in/
- NPCI (UPI) - आधिकारिक जानकारी - https://www.npci.org.in/

- भारतीय रिज़र्व बैंक - जन जागरूकता - https://www.rbi.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

OTP और सोशल इंजीनियरिंग

ठग कंप्यूटर नहीं, इंसान को निशाना बनाते हैं - और OTP कभी साझा क्यों नहीं करना चाहिए।

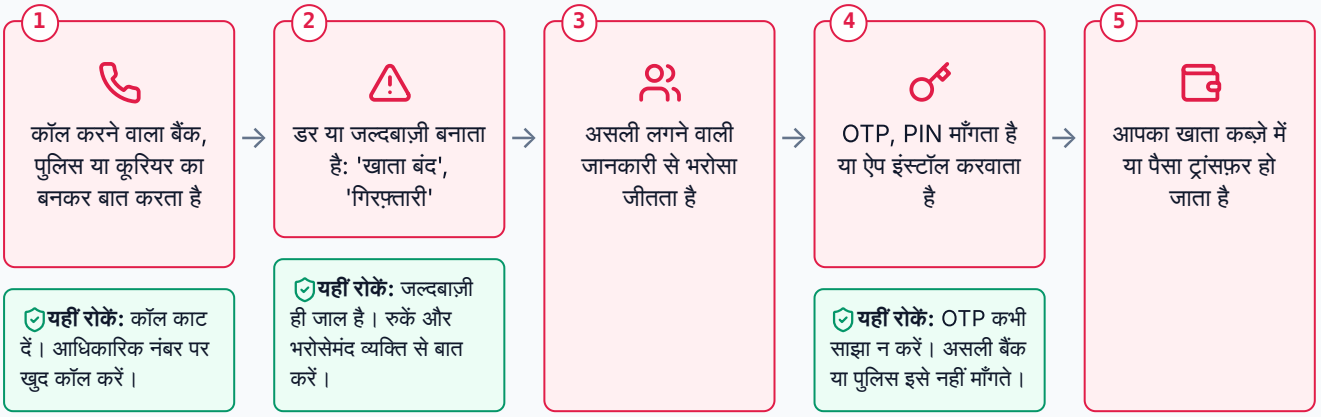
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

सोशल इंजीनियरिंग में भरोसे, डर, जल्दबाज़ी या लालच का इस्तेमाल करके किसी व्यक्ति से जानकारी निकलवाई जाती है या कोई काम करवाया जाता है। OTP इसलिए होता है कि आप साबित कर सकें कि मंज़ूरी आप दे रहे हैं। यदि आप OTP किसी कॉल करने वाले को बता देते हैं, तो आप ठग की कार्रवाई को मंज़ूरी दे देते हैं। इसमें 'डिजिटल अरेस्ट' जैसी कॉल भी आती हैं, जिनमें ठग पुलिस या जाँच एजेंसी बनकर कॉल या वीडियो कॉल करते हैं। अधिकारियों ने साफ़ सलाह दी है कि असली एजेंसियाँ वीडियो कॉल पर गिरफ़्तारी नहीं करतीं और न ही मामला निपटाने के लिए पैसे माँगती 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

- ⚠ बैंक, पुलिस, कस्टम, कूरियर या सरकारी एजेंसी का बताकर कोई OTP, PIN या पैसे माँगे।
- ⚠ कहा जाए कि कॉल न काटें, परिवार को न बताएँ या वीडियो कॉल पर बने रहें।
- ⚠ गिरफ़्तारी, खाता फ़्रीज़ या कानूनी कार्रवाई की धमकी, जब तक आप तुरंत भुगतान या 'वेरिफ़ाई' न करें।
- ⚠ किसी पार्सल या SIM के 'अपराध से जुड़े' होने की कहानी जिसे आप स्वतंत्र रूप से जाँच नहीं सकते।
- ⚠ पैसे 'सुरक्षित खाते' में डालने को कहना।

बचाव के व्यावहारिक सुझाव

- OTP किसी को भी न बताएँ। असली संस्था इसे कभी नहीं माँगती।
- कॉल काट दें। फिर संस्था के आधिकारिक नंबर पर खुद कॉल करें।
- जल्दबाज़ी में न आएँ। किसी धमकी पर कार्रवाई से पहले परिवार या मित्र से बात करें।
- याद रखें: कोई असली एजेंसी वीडियो कॉल पर गिरफ़्तारी नहीं करती और केस बंद करने के लिए पैसे नहीं माँगती।
- सार्वजनिक रूप से अपनी निजी जानकारी कम से कम साझा करें - ठग इसी से अपनी बात विश्वसनीय बनाते हैं।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ खाता 'वेरिफ़ाई' करने के लिए OTP बताना	✓ OTP गोपनीय रखें। इसे सिर्फ़ आप आधिकारिक ऐप में डालें
✗ डर के कारण कॉल पर बने रहना	✓ कॉल काटकर आधिकारिक नंबर पर खुद कॉल करना
✗ 'डिजिटल अरेस्ट' वाली वीडियो कॉल पर यकीन करना	✓ समझें कि यह ठगी है। 1930 पर कॉल करके रिपोर्ट करें
✗ WhatsApp या SMS पर आया ऐप इंस्टॉल करना	✓ ऐप सिर्फ़ आधिकारिक ऐप स्टोर से इंस्टॉल करना

ऐसा हो जाए तो क्या करें

1. कॉल तुरंत काट दें और सभी भुगतान रोक दें।
2. संदिग्ध धोखाधड़ी वाली कॉल या संदेश की रिपोर्ट संचार साथी (चक्षु) पर करें।
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

- साइबर अपराध हेल्पलाइन 1930 (वित्तीय साइबर ठगी के लिए) - 1930
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.in/
- संचार साथी - संदिग्ध धोखाधड़ी कॉल/संदेश की रिपोर्ट (चक्षु) - https://sancharsaathi.gov.in/
- भारतीय रिज़र्व बैंक - जन जागरूकता - https://www.rbi.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

ऑनलाइन नौकरी और निवेश ठगी

फ़र्ज़ी वर्क-फ्रॉम-होम नौकरी, टास्क स्कैम और 'पक्के रिटर्न' की स्कीमें - इन्हें जल्दी पहचानें।

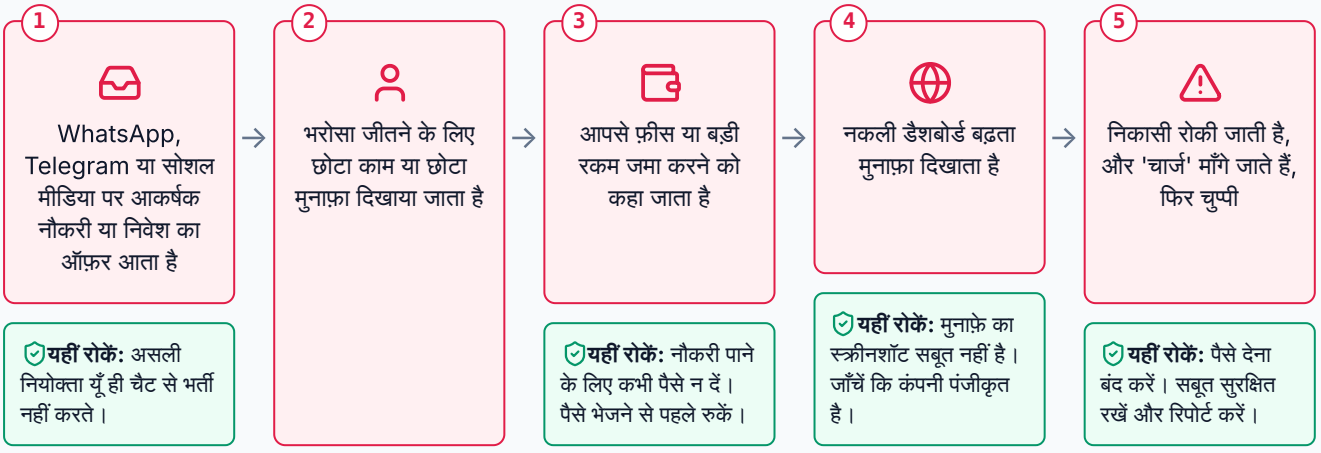
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

यह क्या है

ये ठगियाँ आसान कमाई का वादा करती हैं: रोज़ कुछ मिनट का पार्ट-टाइम काम, वीडियो लाइक करने पर इनाम, या पक्के ऊँचे रिटर्न वाला निवेश। ये अक्सर मैसेजिंग ऐप या सोशल मीडिया से शुरू होती हैं। पहले छोटा 'मुनाफ़ा' दिखाकर भरोसा जीता जाता है, फिर बड़ी-बड़ी रकम जमा करवाई जाती है जिसे निकाला नहीं जा सकता।

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

- ⚠ WhatsApp या Telegram पर अनजान नंबर से नौकरी का ऑफ़र, बहुत आसान काम के लिए ऊँची कमाई।
- ⚠ काम शुरू करने या पैसे निकालने से पहले 'रजिस्ट्रेशन', 'सिक्योरिटी' या 'प्रोसेसिंग' फ़ीस माँगना।
- ⚠ बहुत कम या बिना जोखिम के पक्का या असामान्य रूप से ऊँचा रिटर्न।
- ⚠ पहले का मुनाफ़ा 'अनलॉक' करने के लिए और जमा करने का दबाव।
- ⚠ कंपनी की कोई जाँच-योग्य जानकारी नहीं, या चैट में भेजा गया अनियंत्रित प्लेटफ़ॉर्म या ऐप लिंक।

बचाव के व्यावहारिक सुझाव

- असली नियोक्ता नौकरी देने के लिए पैसे नहीं लेता। कंपनी को उसकी आधिकारिक वेबसाइट पर जाँचें।
- 'पक्के रिटर्न' को खतरे की घंटी मानें। जाँचें कि निवेश संस्था या सलाहकार संबंधित नियामक के पास पंजीकृत है या नहीं।
- अजनबियों द्वारा जोड़े गए निवेश ग्रुप में शामिल न हों और उनके भेजे ऐप इंस्टॉल न करें।
- नौकरी या निवेश के लिए किसी निजी खाते में भुगतान न करें।
- बड़ा आर्थिक फ़ैसला लेने से पहले किसी भरोसेमंद व्यक्ति से सलाह लें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✗ नौकरी के लिए 'रजिस्ट्रेशन फ़ीस' देना	✓ याद रखें: असली नौकरी में उम्मीदवार से पैसे नहीं लिए जाते
✗ 'गारंटीड' ऊँचे रिटर्न पर भरोसा करना	✓ समझें कि कोई ईमानदार निवेश मुनाफ़े की गारंटी नहीं देता
✗ अनजान नंबरों के 'टिप्स' ग्रुप में जुड़ना	✓ सिर्फ़ पंजीकृत और विनियमित मध्यस्थों का उपयोग करना
✗ अजनबियों के 'लाइक करो, कमाओ' काम करना	✓ अनजान लोगों के पार्ट-टाइम काम के ऑफ़र अनदेखा करना

ऐसा हो जाए तो क्या करें

1. पैसे भेजना तुरंत बंद करें, भले ही कहा जाए कि अगला भुगतान आपकी रकम 'रिलीज़' करा देगा।
2. तुरंत साइबर अपराध हेल्पलाइन 1930 पर कॉल करें - जल्दी रिपोर्ट करने से पैसा रोके जाने की संभावना बेहतर होती है।
3. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) पर भी शिकायत दर्ज करें।
4. अपने बैंक या पेमेंट ऐप को तुरंत सूचित करें और संबंधित कार्ड, खाता या UPI ID ब्लॉक करवाएँ।
5. स्क्रीनशॉट, ट्रांज़ैक्शन ID, फ़ोन नंबर, UPI ID और चैट सुरक्षित रखें। कुछ भी डिलीट न करें।
6. 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

- साइबर अपराध हेल्पलाइन 1930 (वित्तीय साइबर ठगी के लिए) - 1930
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.gov.in/
- भारतीय रिज़र्व बैंक - जन जागरूकता - https://www.rbi.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

सोशल मीडिया सुरक्षा

अपने अकाउंट को हैकिंग, नकली प्रोफ़ाइल और उत्पीड़न से बचाएँ।

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

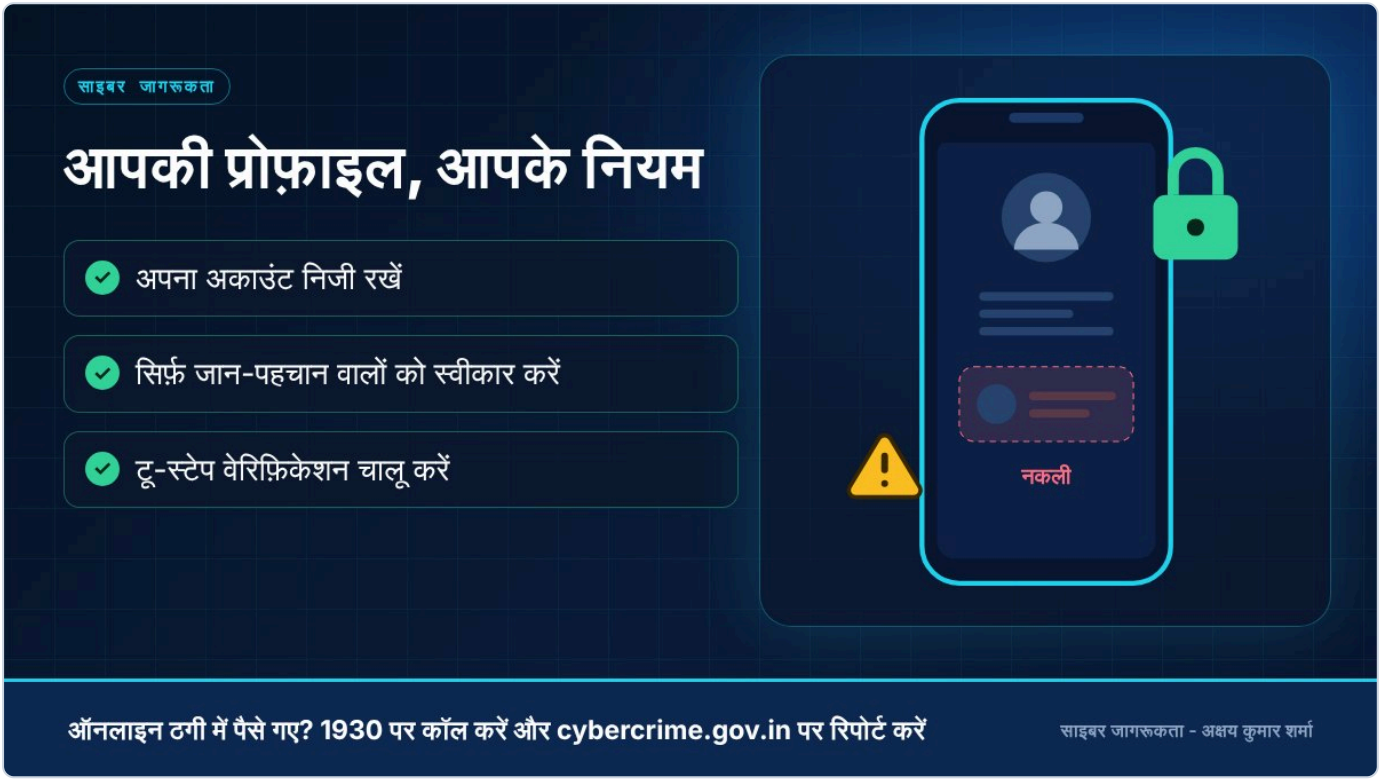
यह क्या है

सोशल मीडिया अकाउंट में आपकी पहचान, फ़ोटो और संपर्क होते हैं। हमलावर अकाउंट हैक करके आपके दोस्तों को ठगते हैं, आपकी फ़ोटो से नकली प्रोफ़ाइल बनाते हैं, या आपकी पोस्ट से पासवर्ड और सिक्योरिटी जवाब का अंदाज़ा लगाते 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।

1. आप निजी जानकारी और फ़ोटो सार्वजनिक रूप से डालते हैं
   - **यहीं रोकें:** कम साझा करें और प्रोफ़ाइल निजी रखें।
2. कोई ठग आपकी प्रोफ़ाइल का अध्ययन करता है
3. नकली फ़्रेंड रिक्वेस्ट, आपकी प्रोफ़ाइल की नक़ल या फ़िशिंग संदेश आता है
   - **यहीं रोकें:** सिर्फ़ जान-पहचान वालों को स्वीकार करें। अजीब अनुरोध की कॉल करके पुष्टि करें।
4. आप धोखे में आ जाते हैं या आपका अकाउंट हैक हो जाता है
   - **यहीं रोकें:** टू-स्टेप वेरिफ़िकेशन अभी चालू करें।
5. आपके दोस्तों को आपके नाम से ठगी के संदेश जाते हैं



आम चेतावनी के संकेत

- ⚠ ऐसे लॉगिन अलर्ट या पासवर्ड-रीसेट ईमेल जो आपने नहीं माँगे।
- ⚠ दोस्तों को आपके अकाउंट से अजीब संदेश मिलना, जैसे पैसे की माँग।
- ⚠ किसी परिचित की नकल करने वाला फ़्रेंड रिक्वेस्ट या संदेश।
- ⚠ मुफ़्त फ़ॉलोअर, इनाम या 'आपकी प्रोफ़ाइल किसने देखी' जैसे लिंक वाले संदेश।
- ⚠ लॉगिन इतिहास में अनजान डिवाइस दिखना।

बचाव के व्यावहारिक सुझाव

- मज़बूत और अलग पासवर्ड रखें तथा टू-फ़ैक्टर ऑथेंटिकेशन चालू करें।
- प्राइवेसी सेटिंग समय-समय पर जाँचें और तय करें कि आपकी जानकारी कौन देख सकता है।
- अजनबियों की रिक्वेस्ट स्वीकार न करें और संदेश में आए लिंक से लॉगिन न करें।
- आपके अकाउंट का एक्सेस माँगने वाले थर्ड-पार्टी ऐप से सावधान रहें।
- जन्मतिथि या पालतू का नाम जैसी जानकारी, जो सिक्योरिटी जवाब हो सकती है, पोस्ट करने से बचें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ फ़ोन नंबर, पता और जन्मदिन वाली सार्वजनिक प्रोफ़ाइल	✓ कम निजी जानकारी वाली निजी प्रोफ़ाइल
✕ हर फ़्रेंड रिक्वेस्ट स्वीकार करना	✓ जान-पहचान वालों को स्वीकार करना और म्यूचुअल फ़्रेंड्स जाँचना
✕ दोस्तों के भी संदेशों के लिंक पर क्लिक करना	✓ दोस्त से कॉल पर पूछना कि संदेश असली है या नहीं
✕ हर जगह एक ही पासवर्ड रखना	✓ अलग पासवर्ड और टू-स्टेप वेरिफ़िकेशन इस्तेमाल करना

ऐसा हो जाए तो क्या करें

1. प्लेटफ़ॉर्म की सिक्योरिटी सेटिंग से पासवर्ड बदलें और सभी डिवाइस से लॉग आउट करें।
2. प्लेटफ़ॉर्म के आधिकारिक अकाउंट रिकवरी और रिपोर्ट विकल्प इस्तेमाल करें।
3. अपने संपर्कों को बताएँ कि आपका अकाउंट हैक हुआ था।
4. नकली प्रोफ़ाइल, उत्पीड़न या ठगी की रिपोर्ट प्लेटफ़ॉर्म पर और ज़रूरत हो तो cybercrime.gov.in पर करें।

आधिकारिक रिपोर्टिंग संसाधन

- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (cybercrime.gov.in) - https://cybercrime.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

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।

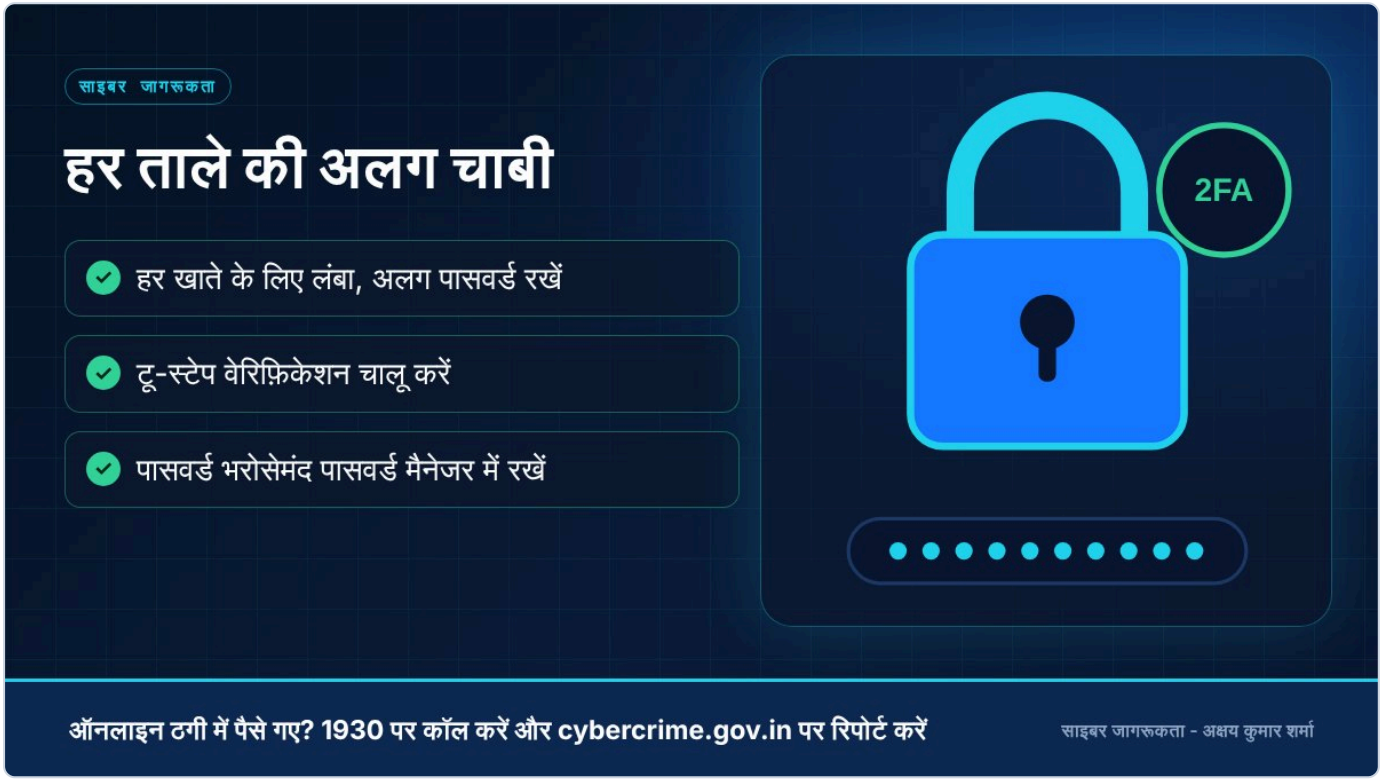
यह क्या है

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।

1	2	3	4	5
आप कई साइटों पर एक ही कमज़ोर पासवर्ड रखते हैं	उनमें से एक साइट का डेटा लीक हो जाता है	ठग लीक हुआ पासवर्ड आपके दूसरे खातों पर आज़माते हैं	आपका ईमेल या बैंक खाता कब्ज़े में आ जाता है	पैसे, डेटा और कॉन्टैक्ट्स का दुरुपयोग होता है
यहीं रोकें: हर खाते के लिए लंबा, अलग पासवर्ड रखें। पासवर्ड मैनेजर मदद करता है।	**यहीं रोकें:** जाँचें कि आपका ईमेल किसी लीक में आया या नहीं, और वे पासवर्ड बदलें।	**यहीं रोकें:** टू-स्टेप वेरिफ़िकेशन पासवर्ड मिलने पर भी ठग को रोकता है।	**यहीं रोकें:** सबसे पहले ईमेल सुरक्षित करें। इससे बाकी सब रीसेट हो सकता है।	



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

डिजिटल फुटप्रिंट और प्राइवेसी

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

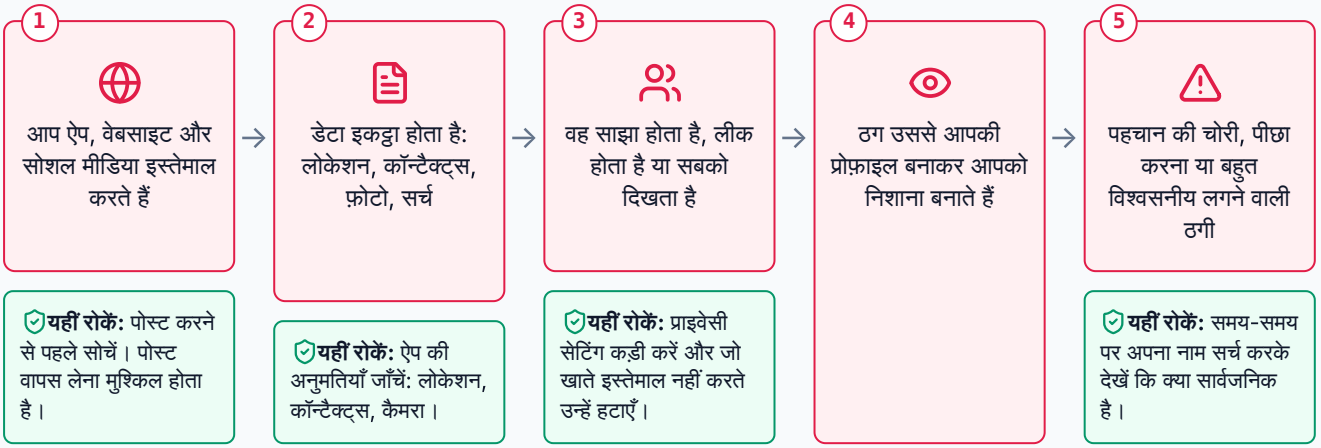
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

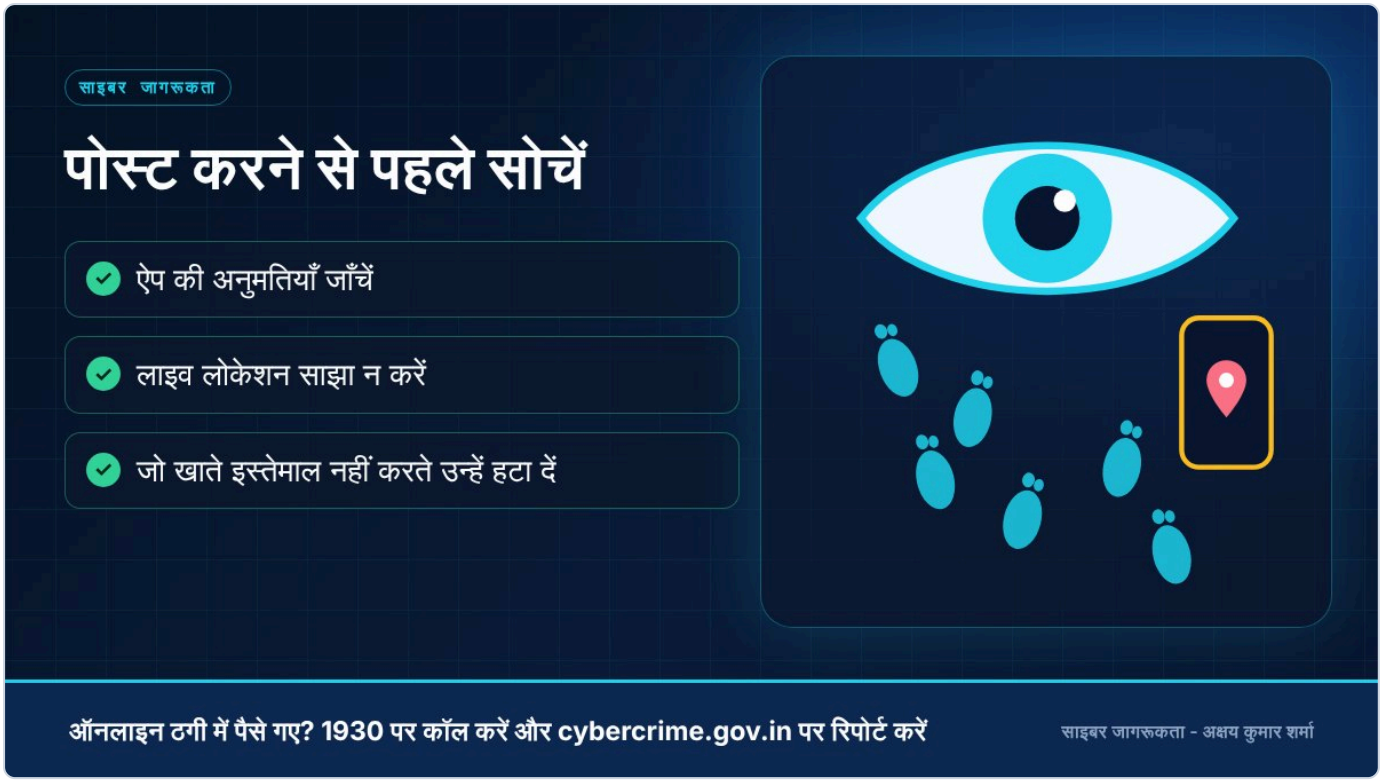
यह क्या है

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

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।

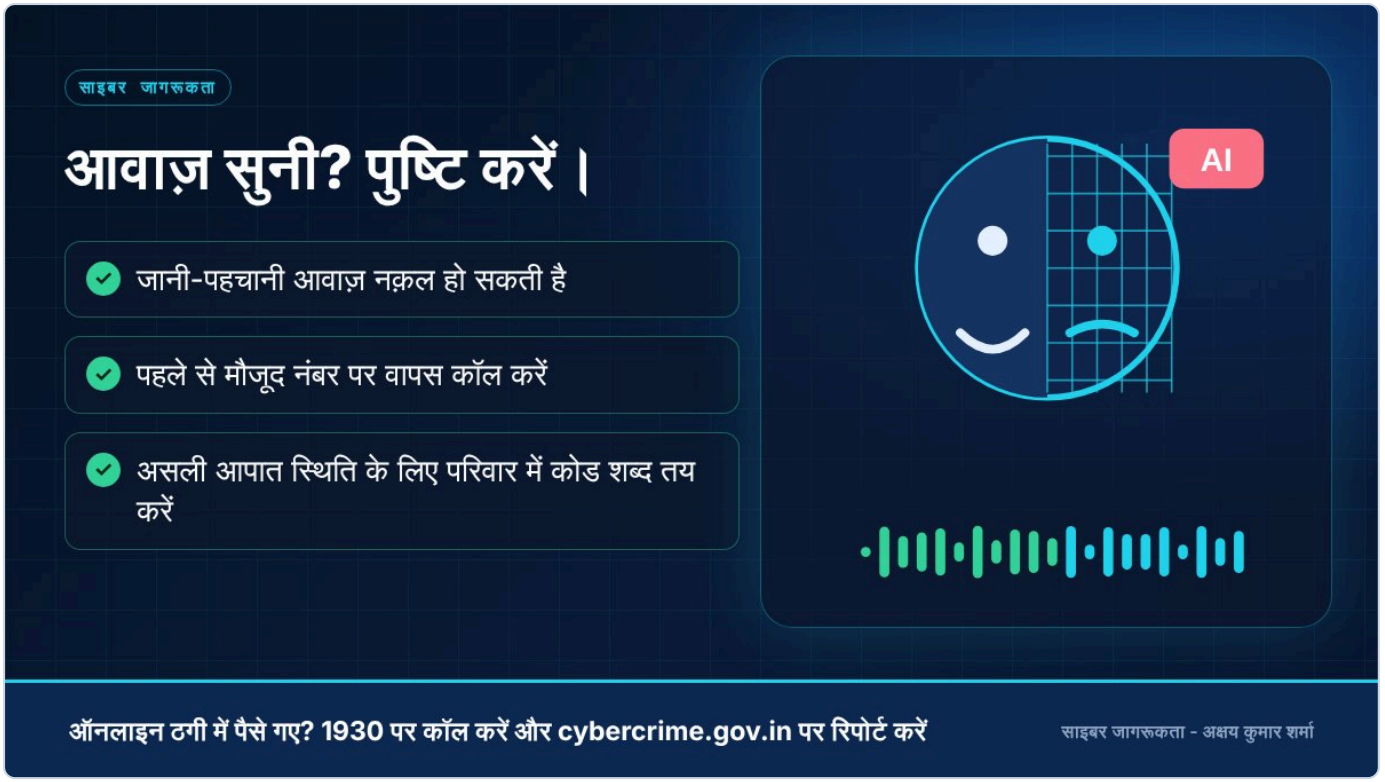
यह क्या है

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

मैलवेयर और संदिग्ध ऐप

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

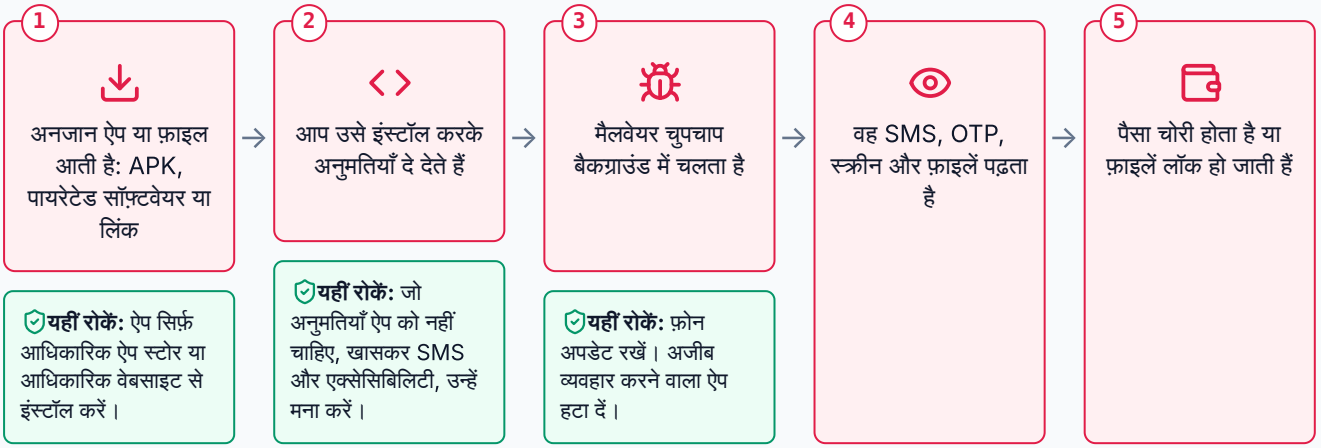
ऑनलाइन ठगी में पैसे गए? तुरंत 1930 पर कॉल करें और cybercrime.gov.in पर रिपोर्ट करें।

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

विद्यार्थियों और परिवारों के लिए साइबर सुरक्षा

विद्यार्थियों, अभिभावकों और बुज़ुर्गों के लिए रोज़मर्रा की डिजिटल सुरक्षा - ऑनलाइन बुलिंग और गेमिंग के जोखिम सहित।

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

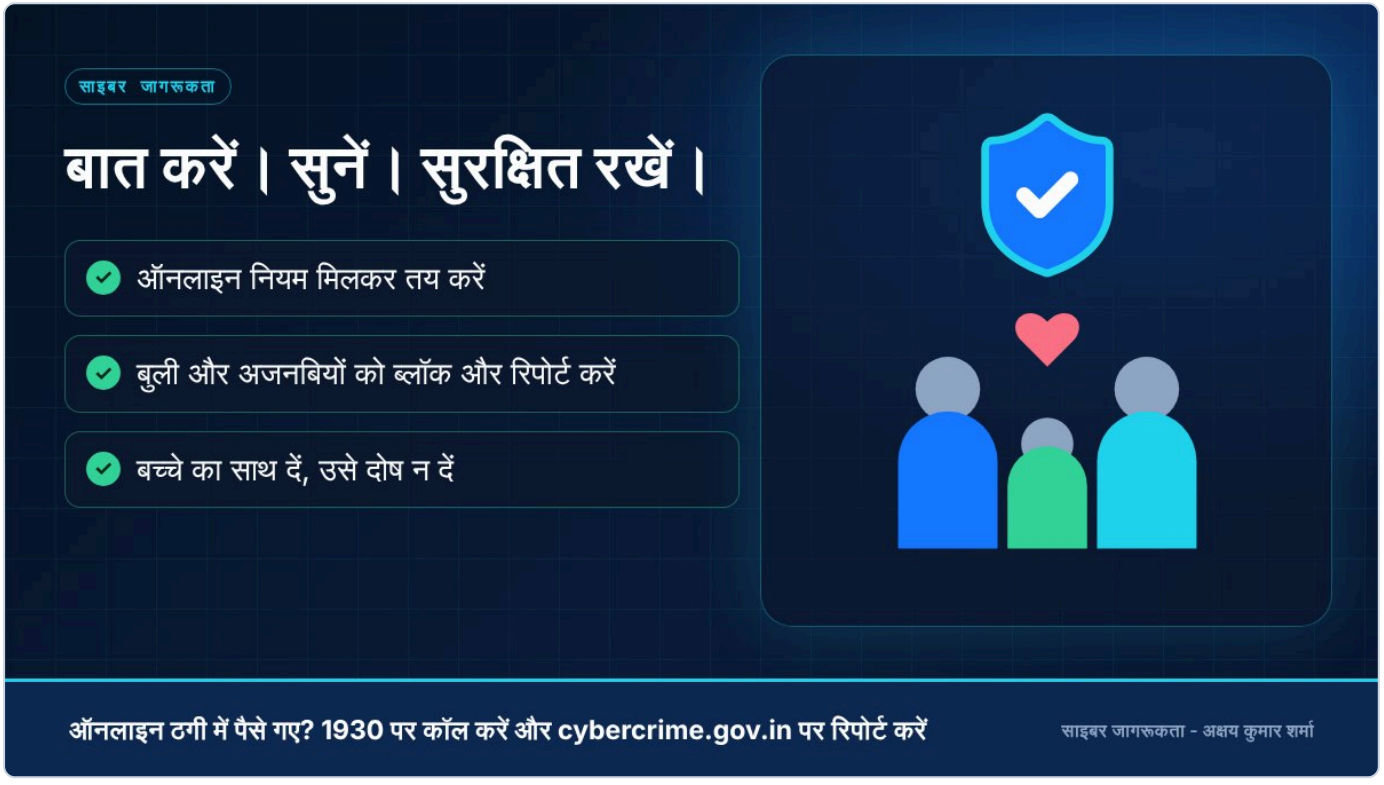
यह क्या है

विद्यार्थी और परिवार पढ़ाई, गेमिंग, भुगतान और सामाजिक जीवन के लिए ऑनलाइन रहते हैं। जोखिमों में ऑनलाइन बुलिंग, स्कॉलरशिप या पार्ट-टाइम नौकरी के नाम पर ठगी, अजनबियों का असुरक्षित संपर्क, ज़्यादा जानकारी साझा करना और कमज़ोर अकाउंट सुरक्षा शामिल हैं। घर में खुलकर बात करना सबसे बड़ी सुरक्षा 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	2	3	4
बच्चा या विद्यार्थी ऑनलाइन जाता है: गेम, सोशल मीडिया, चैट	कोई अजनबी, बुली या ठग संपर्क करता है	बच्चा जानकारी या फ़ोटो साझा करता है, या अजनबी पर भरोसा करता है	नुकसान होता है: ठगी, बुलिंग, उत्पीड़न या ब्लैकमेल
यहीं रोकें: खुलकर बात करें। मिलकर नियम तय करें और प्राइवेसी कंट्रोल लगाएँ।	**यहीं रोकें:** ब्लॉक करें और रिपोर्ट करें। सबूत के लिए स्क्रीनशॉट रखें।	**यहीं रोकें:** OTP, पासवर्ड या निजी फ़ोटो कभी साझा न करें। किसी भरोसेमंद बड़े को बताएँ।	**यहीं रोकें:** cybercrime.gov.in पर रिपोर्ट करें। बच्चे का साथ दें, उसे दोष न दें।



आम चेतावनी के संकेत

- ⚠ संदेशों के बाद बच्चा या विद्यार्थी चुप-चुप, चिंतित रहे या डिवाइस से बचे।
- ⚠ अजनबी का फ़ोटो, निजी जानकारी माँगना या दूसरे ऐप पर चलने को कहना।
- ⚠ 'स्कॉलरशिप', 'मुफ़्त गिफ़्ट' या 'नौकरी' के ऑफ़र जो फ़ीस या बैंक जानकारी माँगें।
- ⚠ परिवार की जानकारी के बिना गेमिंग या इन-ऐप खरीदारी।
- ⚠ बुज़ुर्गों को इनाम, KYC या मुसीबत में फँसे रिश्तेदार के बारे में कॉल आना।

बचाव के व्यावहारिक सुझाव

- 🛡 खुलकर बात करें और भरोसा दिलाएँ कि कुछ गलत लगे तो बिना डाँट के डर के कोई भी आपके पास आ सकता है।
- 🛡 मज़बूत पासवर्ड, टू-फ़ैक्टर ऑथेंटिकेशन और बच्चे की उम्र के अनुसार पैरेंटल या प्राइवेसी कंट्रोल इस्तेमाल करें।
- 🛡 बुनियादी बातें सिखाएँ: OTP साझा न करें, अनजान लिंक न खोलें, ऑनलाइन संपर्क से अकेले न मिलें।
- 🛡 डिवाइस और ऐप अपडेट रखें और बच्चों के अकाउंट पर भुगतान के विकल्प सीमित रखें।
- 🛡 बुज़ुर्गों के लिए पेमेंट अलर्ट चालू करवाएँ और असामान्य भुगतान से पहले परिवार से पूछने की आदत डालें।

जोखिम भरी आदत बनाम सुरक्षित आदत

जोखिम भरा	सुरक्षित
✕ समस्या बताने पर बच्चे को डाँटना	✓ शांत रहकर सुनना और साथ देना
✕ दोस्तों को पासवर्ड बताना	✓ सिर्फ़ माता-पिता या अभिभावक को बताना
✕ ऑनलाइन गेम में अजनबियों से चैट करना	✓ उन दोस्तों के साथ खेलना जिन्हें आप असल में जानते हैं
✕ डर या शर्म से साइबरबुलिंग छिपाना	✓ सबूत रखना, ब्लॉक करना और रिपोर्ट करना

ऐसा हो जाए तो क्या करें

1. शांत रहें और संबंधित व्यक्ति का साथ दें। उन्हें दोष न दें।
2. स्क्रीनशॉट और संदेश सबूत के रूप में रखें, फिर प्लेटफ़ॉर्म पर अकाउंट ब्लॉक और रिपोर्ट करें।
3. गंभीर उत्पीड़न या ठगी की रिपोर्ट cybercrime.gov.in पर करें और वित्तीय ठगी के लिए 1930 पर कॉल करें।
4. यदि मामला सहपाठियों से जुड़ा है तो स्कूल या कॉलेज को शामिल करें।

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
- 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