OPTIV

DSCI
PROMOTING DATA PROTECTION

India
Meri Digital Suraksha
2026







एक आसान गाइड
ऑनलाइन सुरक्षित रहने के लिए










Meri Digital Suraksha

गाइड के बारे में

यह सेफ्टी गाइड 'मेरी डिजिटल सुरक्षा' के अंतर्गत बनाई गई है, जो DSCI और OPTIV की एक साइबर सुरक्षा जागरूकता पहल है।

यह डिजिटल पेमेंट्स ऑनलाइन बैंकिंग सेफ्टी, ईमेल सिक्योरिटी, ऐप सिक्योरिटी, सोशल मीडिया सेफ्टी, प्राइवेसी प्रोटेक्शन, डिजिटल वेल बीइंग और साइबर क्राइम रिड्रेसल

जैसे ज़रूरी क्षेत्रों को एक व्यावहारिक और आसान गाइड में एक साथ लाता है। यह गाइड बेस्ट प्रैक्टिसेज़ और साइबर हाइजीन के बारे में बताती है, साथ ही प्रचलित साइबर स्कैम्स और शब्दावलियों के प्रति जागरूक करती है ताकि आप सतर्क रह सकें और डिजिटल दुनिया में आत्मविश्वास के साथ आगे बढ़ सकें।

विषय सूची

I. साइबर सिक्योरिटी बेस्ट प्रैक्टिसेज़

डिजिटल पेमेंट्स और ऑनलाइन बैंकिंग सेफ्टी 08

ऐप सिक्योरिटी 13

ईमेल सिक्योरिटी 18

सोशल मीडिया सेफ्टी 23

II. प्राइवेसी बेस्ट प्रैक्टिसेज़ 26

III. डिजिटल हाइजीन

डिवाइस और अकाउंट हाइजीन 34

पासवर्ड हाइजीन 36

डिजिटल वेलबीइंग 38

IV. साइबरक्राइम रिड्रेसल 39

साइबर सिक्योरिटी बेस्ट प्रैक्टिसेज़



डिजिटल पेमेंट करने, ऐप्स का उपयोग करने, ईमेल का जवाब देने और सोशल मीडिया पर बातचीत जैसी रोज़मर्रा की गतिविधियों में, जालसाजों द्वारा अपनाए जाने वाले विभिन्न साइबर हमलों के कारण कुछ हद तक साइबर जोखिम हमेशा मौजूद रहता है।

स्मार्ट डिजिटल आदतें अपनाने का एक ही सुनहरा नियम है: हर कॉल, मैसेज या लिंक पर रुकें, उसे वेरिफाई करें और फिर कोई एक्शन लें।

यह सेक्शन डिजिटल पेमेंट्स, ऐप सिक्योरिटी, ईमेल और सोशल मीडिया से जुड़ी प्रैक्टिकल सिक्योरिटी आदतों के बारे में बताता है।



डिजिटल पेमेंट्स और ऑनलाइन बैंकिंग सेफ्टी

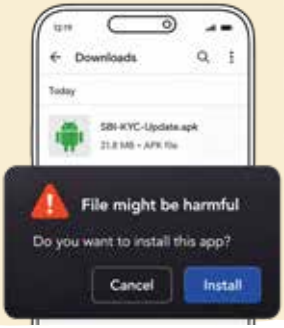
डिजिटल पेमेंट्स रोज़ाना के लेन-देन को तेज़ और आसान बना देते हैं, लेकिन इनमें हमारा पैसा और फाइनेंशियल जानकारी शामिल होती है। **इसीलिए डिजिटल पेमेंट्स और बैंकिंग सिक्योरिटी ज़रूरी है: एक धोखाधड़ी वाला या गलत ट्रांजेक्शन आपके पैसे को जोखिम में डाल सकता है और उसे वापस पाना मुश्किल हो सकता है।**



डिजिटल शब्दावली

1 APK फाइल

एक APK (एंड्रॉइड पैकेज किट) फ़ाइल एंड्रॉइड ऑपरेटिंग सिस्टम में मोबाइल ऐप्स इंस्टॉल करने का स्टैंडर्ड फॉर्मेट है। अनजान वेबसाइटों, लिंक या मैसेज से APK फ़ाइलें डाउनलोड और इंस्टॉल करने में मैलवेयर, डेटा चोरी और फाइनेंशियल फ्रॉड जैसे बड़े सुरक्षा जोखिम हो सकते हैं।



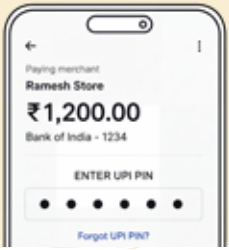


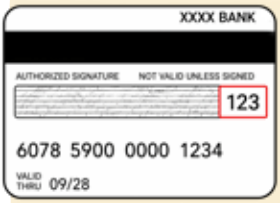
2 रिमोट एक्सेस/ स्क्रीन-शेयरिंग ऐप

यह एक सॉफ्टवेयर प्रोग्राम है जो आपको अपना डिवाइस किसी दूसरे व्यक्ति को दिखाने और किसी अलग जगह से अपने डिवाइस को कंट्रोल करने, या अपनी स्क्रीन को लाइव देखने की सुविधा देता है। इसके सामान्य उदाहरण **एनीडेस्क, टीमव्यूअर, क्विकसपोर्ट और रस्टडेस्क हैं।**

3 UPI (यूनिफाइड पेमेंट्स इंटरफेस) पिन

एक UPI पिन एक निजी सिक्योरिटी कोड है जिसका इस्तेमाल UPI ऐप्स के जरिए मनी ट्रांसफर को अप्रूव करने के लिए किया जाता है।



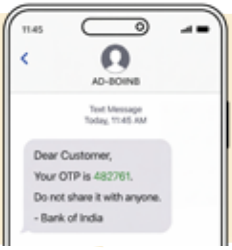


4 CVV

CVV एक सिक्योरिटी कोड है जो ऑनलाइन पेमेंट के लिए आपके डेबिट या क्रेडिट कार्ड पर प्रिंट होता है।

5 OTP (वन-टाइम पासवर्ड)

लॉगिन या ट्रांजेक्शन को वेरिफाई करने के लिए आपके मोबाइल नंबर या ईमेल पर भेजा गया एक टेम्परेरी सिक्योरिटी कोड।





6 KYC (नो योर कस्टमर)

एक प्रोसेस जिसका इस्तेमाल बैंक और ऐप्स आधिकारिक डॉक्यूमेंट्स के ज़रिए कस्टमर की असली पहचान की जाँच और वेरिफिकेशन करने के लिए करते हैं। यूजर्स को वैलिडेट करने के लिए E-KYC, वीडियो KYC के साथ-साथ सेंट्रल KYC (CKYC) जैसे प्रचलित तरीकों का इस्तेमाल किया जाता है।

7 QR कोड

QR कोड एक चौकोर बारकोड होता है जिसे पेमेंट जैसे डिजिटल काम पूरे करने के लिए आपके फोन कैमरे का इस्तेमाल करके स्कैन किया जा सकता है।



सुरक्षित रहने के तरीके

- ऑफ़िशियल बैंकिंग और पेमेंट ऐप्स का ही इस्तेमाल करें। उन्हें केवल अपने फ़ोन के ऑफ़िशियल ऐप स्टोर से ही डाउनलोड करें; मैसेज के ज़रिए भेजे गए लिंक या APK फ़ाइलों से बचें।

- अपना UPI पिन, OTP, क्रेडिट/डेबिट कार्ड CVV और पिन पासवर्ड या कार्ड की पूरी जानकारी कभी भी किसी के साथ शेयर न करें।

- किसी भी UPI पेमेंट को अप्रूव करने से पहले प्राप्तकर्ता और राशि की जाँच कर लें, भले ही उसमें "रिफंड," "कैशबैक" या "इनाम" लिखा हो।

- पेमेंट करने के लिए OTP डालने से पहले, ट्रांजेक्शन की राशि और पाने वाले की जानकारी को वेरिफाई करने के लिए हमेशा OTP SMS को पहले चेक करें।

- QR कोड्स से सावधान रहें। QRर कोड स्कैन करने से भुगतान किया जा सकता है; पैसे या रिफंड प्राप्त करने के लिए केवल QR कोड स्कैन न करें।

- अपने फोन का रिमोट एक्सेस किसी को न दें। किसी अनजान कॉलर के कहने पर कभी भी रिमोट-एक्सेस या स्क्रीन-शेयरिंग ऐप इंस्टॉल न करें।



- अनपेक्षित KYC कॉल या मैसेज को अनदेखा करें और अपने बैंक के ऑफिशियल चैनल के ज़रिए उनसे संपर्क करें।
- जल्दबाज़ी में आकर कोई पेमेंट न करें। डर, दबाव या समय सीमा से जुड़े अनुरोधों की स्वतंत्र रूप से जाँच करने के लिए समय निकालें।
- अपने ट्रांजेक्शन अलर्ट चेक करें। ट्रांजेक्शन नोटिफिकेशन ऑन रखें और किसी भी असामान्य गतिविधि को तुरंत रिपोर्ट करें।
- अपने ट्रांजेक्शन अलर्ट चेक करें। ट्रांजेक्शन नोटिफिकेशन ऑन रखें और किसी भी असामान्य गतिविधि को तुरंत रिपोर्ट करें।
- अपना बैंक अकाउंट केवल अपने लेन-देन के लिए इस्तेमाल करें। कमीशन के बदले किसी और का पैसा अपने खाते में लेने या आगे भेजने की अनुमति न दें।
- बैंक का कस्टमर केयर नंबर उसकी आधिकारिक वेबसाइट, ऐप या पासबुक से लें। मैसेज या इंटरनेट पर खोजने से मिले किसी भी नंबर पर भरोसा न करें।



हमेशा याद रखें

एक UPI पिन की ज़रूरत सिर्फ पैसे भेजने के लिए होती है, पैसे पाने के लिए कभी नहीं। अगर कोई आपसे रिफंड या कैशबैक देने के लिए आपका पिन माँगता है, तो यह हमेशा एक स्कैम होता है।





कॉमन डिजिटल पेमेंट्स और बैंकिंग सिक्योरिटी से जुड़े स्कैम्स



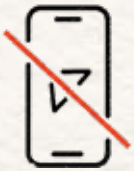
फेक KYC/अकाउंट ब्लॉकिंग स्कैम

कोई कॉलर या मैसेज आपके बैंक से होने का नाटक करता है और कहता है कि आपका KYC अपडेट करने की ज़रूरत है वरना आपका अकाउंट ब्लॉक कर दिया जाएगा। आपको किसी नकली वेबसाइट पर भेजा जा सकता है, जानकारी साझा करने के लिए कहा जा सकता है या पेमेंट करने के लिए कहा जा सकता है।

फेक रिफंड/कैशबैक स्कैम

एक UPI पिन की ज़रूरत सिर्फ पैसे भेजने के लिए होती है, पैसे पाने के लिए कभी नहीं। अगर कोई आपसे रिफंड या कैशबैक देने के लिए आपका पिन माँगता है, तो यह हमेशा एक स्कैम होता है।





रिमोट एक्सेस स्कैम

एक फ्रॉडस्टर आपको रिमोट-एक्सेस या स्क्रीन-शेयरिंग ऐप इंस्टॉल करने के लिए मना लेता है, यह दावा करते हुए कि बैंकिंग या पेमेंट की समस्या को हल करने के लिए इसकी ज़रूरत है। एक बार एक्सेस मिलने के बाद, वे आपके डिवाइस पर एक्टिविटी को देख या कंट्रोल कर सकते हैं।

मनी म्यूल/अकाउंट मिसयूज़ स्कैम

कोई आपके बैंक अकाउंट के ज़रिए पैसे पाने और ट्रांसफर करने के लिए पैसे या कमीशन का ऑफर देता है। यह पैसा धोखाधड़ी से हासिल किया गया हो सकता है, जिससे आपका अकाउंट भी धोखाधड़ी का हिस्सा बन जाता है।





QR कोड पेमेंट स्कैम

एक जालसाज़ यह दावा करते हुए QR कोड भेजता है या दिखाता है कि पेमेंट, रिफंड या रिवॉर्ड पाने के लिए इसकी ज़रूरत है। इसे स्कैन करने से आपके अकाउंट से पेमेंट जा सकता है।

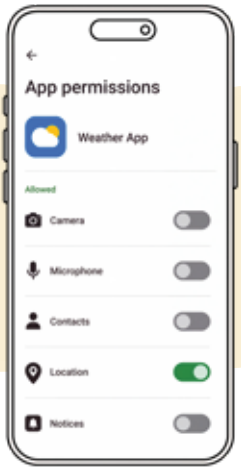
ऐप सिक्योरिटी

ऐप्स रोज़ाना के कामों को आसान बनाते हैं, लेकिन वे हमारे फोन पर अलग-अलग फीचर्स और जानकारी तक पहुँच सकते हैं। **इसीलिए ऐप सिक्योरिटी ज़रूरी है: एक असुरक्षित ऐप इस पहुँच का गलत इस्तेमाल कर सकता है, निजी जानकारी को उजागर कर सकता है या आपके अकाउंट्स और पैसों को जोखिम में डाल सकता है।**

कॉमन डिजिटल शब्दावली को समझना

1 ऐप परमिशन्स

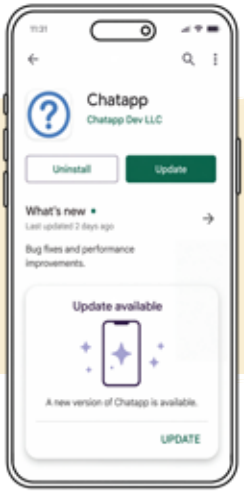
ऐप परमिशन्स वे अप्रूवल हैं जो आप किसी ऐप को अपने फोन की कुछ खास फीचर्स या जानकारी तक पहुँचने के लिए देते हैं, जैसे कि आपका कैमरा, माइक्रोफोन, कॉन्टैक्ट्स, फोटोज या लोकेशन।



2 ऑफिशियल ऐप स्टोर

Google Play Store Apple App Store

ऑफिशियल ऐप स्टोर आपके फोन निर्माता और ऑपरेटिंग सिस्टम (OS) प्रदाता द्वारा आधिकारिक तौर पर वेरिफाइड ऐप्स डाउनलोड करने के लिए प्रदान किया गया एक भरोसेमंद स्थान है। एंड्रॉइड फोन पर, यह आमतौर पर **गूगल प्ले स्टोर** होता है, और आईफोन पर, **एप्पल ऐप स्टोर।**



3 ऐप अपडेट

ऐप अपडेट ऐप डेवलपर द्वारा जारी किया गया एक नया वर्शन है। यह समस्याओं को ठीक कर सकता है, सिक्योरिटी में सुधार कर सकता है या नए फीचर्स जोड़ सकता है।



4 ऐप कैश/डेटा

ऐप कैश और डेटा वह जानकारी होती है जो आपके फोन पर किसी ऐप द्वारा स्थानीय रूप से स्टोर की जाती है। कैश में आमतौर पर टेम्परेरी फाइलें होती हैं, जबकि ऐप डेटा में सेव की गई सेटिंग्स, प्राथमिकताएं और अन्य जानकारी शामिल हो सकती है।



रक्षित रहने के तरीके

- सिर्फ ऑफिशियल ऐप स्टोर का ही इस्तेमाल करें और इंस्टॉल करने से पहले ऐप का नाम, डेवलपर, रिव्यू और रेटिंग जरूर चेक करें।

- सिर्फ वही ऐप्स इंस्टॉल करें जिनकी आपको ज़रूरत है। सोशल मीडिया, व्हाट्सएप या मैसेज के ज़रिए सुझाए गए अनजान ऐप्स से बचें, खासकर वे जो ट्रेंडिंग फीचर्स, रिवॉर्ड्स या गेम्स का लालच देते हैं।

- ऐप परमिशन्स चेक करें। किसी ऐप को केवल उतनी ही एक्सेस दें जितनी उसे ज़रूरत है। एक कैलकुलेटर को आपके कॉन्टैक्ट्स की ज़रूरत नहीं होती है, और एक साधारण फोटो-एडिटिंग ऐप को आपकी लोकेशन एक्सेस की ज़रूरत नहीं होती है।

- अपने फोन और ऐप्स को अपडेट रखें। सुरक्षा की कमियों को ठीक करने के लिए उपलब्ध होने पर अपडेट इंस्टॉल करें।

- अकाउंट तभी बनाएँ जब ज़रूरी हो। चेक करें कि ऐप क्या जानकारी माँग रहा है और क्या आपको वाकई अकाउंट की ज़रूरत है।



- अपने फोन और संवेदनशील ऐप्स को पिन, फिंगरप्रिंट या फेस लॉक से सुरक्षित रखें, और अनधिकृत एक्सेस को रोकने के लिए वित्तीय और अन्य संवेदनशील ऐप्स के लिए टू-फैक्टर ऑथेंटिकेशन (2FA) सक्षम करें।

- अपने ऐप्स और परमिशन्स को रिव्यू करें। उन ऐप्स को हटा दें जिनका आप अब उपयोग नहीं करते हैं और चेक करें कि मौजूदा ऐप्स के पास अभी भी केवल वही एक्सेस है जिसकी उन्हें ज़रूरत है।

- सुरक्षा चेतावनियों पर ध्यान दें। अगर आपका फोन या कोई ऐप सुरक्षा चेतावनी दिखाता है, तो आगे बढ़ने से पहले रुकें और ज जाँच करें।

- किसी भी ऐप को डाउनलोड करने और उसमें संवेदनशील जानकारी डालने से पहले उसकी जाँच कर लें। जब तक आप यह पक्का न कर लें कि ऐप असली है, तब तक अपना OTP, PIN, पासवर्ड या बैंकिंग विवरण कभी न डालें।

- किसी भी ऐप को डाउनलोड करने और उसमें संवेदनशील जानकारी डालने से पहले उसकी जाँच कर लें। जब तक आप यह पक्का न कर लें कि ऐप असली है, तब तक अपना OTP, PIN, पासवर्ड या बैंकिंग विवरण कभी न डालें।



हमेशा याद रखें

ऑफिशियल ऐप स्टोर पर मौजूद ऐप्स भी कभी-कभी धोखाधड़ी वाले या हानिकारक हो सकते हैं। इंस्टॉल करने से पहले, ऐप का नाम, लोगो, डेवलपर और रिव्यूज़ को चेक करें ताकि यह पक्का हो सके कि आपको असली ऐप ही मिला है।



फेक ऐप स्कैम्स

एक फेक ऐप को असली ऐप जैसा दिखने के लिए बनाया जाता है ताकि आप इसे गलती से इंस्टॉल कर लें। इसमें किसी भरोसेमंद ऐप जैसा ही लोगो, रंग और नाम इस्तेमाल किया जा सकता है, लेकिन छोटी-छोटी डिटेल्स अलग हो सकती हैं।



फेक शॉपिंग ऐप

धोखाधड़ी करने वाले ऐसे ऐप्स बना सकते हैं जो भारी छूट वाले प्रोडक्ट्स, लिमिटेड-टाइम डील्स या स्पेशल ऑफर्स देते हैं। आपको गूगल सर्च, सोशल मीडिया या मैसेज के ज़रिए ऐसे प्रमोशन देखने को मिल सकते हैं। यह ऐप एक असली शॉपिंग प्लेटफॉर्म की तरह लग सकता है और बिना प्रोडक्ट डिलीवर किए आपका पेमेंट ले सकता है।



फेक गवर्नमेंट या सर्विस ऐप

धोखाधड़ी करने वाले ऐसे ऐप्स बना सकते हैं जो सरकारी सेवाएं, सब्सिडी, सर्टिफिकेट, यूटिलिटी सेवाएं या अन्य सार्वजनिक सेवाएँ देने का नाटक करते हैं। आपको ऐसे ऐप्स गूगल सर्च, सोशल मीडिया या मैसेज के ज़रिए मिल सकते हैं। यह ऐप असली लग सकता है और आपसे आधार, पैन, OTP या अन्य व्यक्तिगत जानकारी साझा करने के लिए कह सकता है।



फेक बैंकिंग या कस्टमर सपोर्ट ऐप

फ्रॉडस्टर्स ऐसे ऐप्स बना सकते हैं जो बैंकिंग, पेमेंट या कस्टमर-सपोर्ट सर्विस होने का नाटक करते हैं। आपको सर्च रिज़ल्ट्स, मैसेज या कॉल के ज़रिए इन ऐप्स पर भेजा जा सकता है, जिनमें आपके अकाउंट में मदद करने का दावा किया गया हो। ऐप आपसे संवेदनशील जानकारी या परमिशन माँग सकता है जिससे फ्रॉडस्टर्स को आपके डिवाइस या जानकारी तक पहुँच मिल सकती है



ईमेल सिक्योरिटी

ईमेल हमारे रोज़ाना के डिजिटल जीवन का हिस्सा है और इसमें अक्सर व्यक्तिगत संदेश, दस्तावेज़ होते हैं और यह एक मान्य साइनअप/लॉगिन तरीके के रूप में काम करता है।

यही कारण है कि ईमेल सिक्योरिटी ज़रूरी है: अगर किसी को आपके ईमेल का एक्सेस मिल जाता है, तो वे इस जानकारी का गलत इस्तेमाल कर सकते हैं या इसका इस्तेमाल आपके दूसरे अकाउंट्स को एक्सेस करने के लिए कर सकते हैं।



सुरक्षित रहने के तरीके

- अपने ईमेल अकाउंट को सुरक्षित रखने के लिए, हमेशा एक मज़बूत और यूनिक पासवर्ड इस्तेमाल करने की आदत डालें और टू फैक्टर ऑथेंटिकेशन चालू करें।

- जवाब देने से पहले हमेशा भेजने वाले का ईमेल एड्रेस चेक करें। एड्रेस को वैलिडेट करने के लिए किसी भी तरह की विसंगतियों या स्पेलिंग की छोटी गलतियों पर ध्यान दें।

- लिंक्स से सावधान रहें। अनजान लिंक्स पर क्लिक न करें, खासकर वे जो पेमेंट, पासवर्ड रीसेट, रिफंड या संवेदनशील जानकारी माँगते हैं।

- अटैचमेंट्स के साथ सावधान रहें। अनपेक्षित PDF, वर्ड फाइल्स, एक्सेल शीट्स या अन्य अटैचमेंट्स न खोलें, भले ही वे आपके किसी परिचित की ओर से ही क्यों न हों।

- अनपेक्षित अनुरोधों को वेरिफाई करें। यदि कोई ईमेल आपसे भुगतान करने, जानकारी साझा करने या तत्काल कार्रवाई करने के लिए कहता है, तो एक अलग, विश्वसनीय चैनल के माध्यम से इसे वेरिफाई करें।

- ईमेल के ज़रिए निजी ID, फाइनेंशियल डॉक्यूमेंट्स या अन्य निजी जानकारी भेजने से बचें। ऐसा केवल तभी करें जब यह बहुत ज़रूरी हो और केवल भरोसेमंद व्यक्तिगत रूप से जाने-पहचाने ईमेल ID पर ही भेजें।

- अपना इनबॉक्स व्यवस्थित रखें। उन संवेदनशील दस्तावेज़ों और फ़ाइलों को हटा दें जिनकी अब आपको ज़रूरत नहीं है, और पासवर्ड, पिन या बैंकिंग विवरण स्टोर करने के लिए ईमेल का उपयोग न करें।

- स्पैम और जंक ईमेल को मैनेज करें। अगर आप भेजने वाले को नहीं पहचानते हैं या आपको ईमेल की उम्मीद नहीं थी, तो इसे स्पैम के रूप में मार्क करें या डिलीट कर दें।

- अगर आपके डिवाइस में आपका ईमेल डिफ़ॉल्ट रूप से लॉग इन है, तो उसे दूसरों के साथ शेयर न करें। शेयर किए गए डिवाइस के लिए ऐप पासवर्ड का इस्तेमाल करें।

- सर्विस प्रोवाइडर्स द्वारा ऑटो-जेनरेट किए गए अनजान लॉगिन और पासवर्ड-रीसेट रिक्वेस्ट ईमेल की जाँच करें। यह एक इनवैलिड लॉगिन प्रयास का संकेत हो सकता है। संबंधित अकाउंट पासवर्ड रीसेट करें।



कॉमन ईमेल फिशिंग स्कैम्स

फ़िशिंग: यह एक भरोसेमंद व्यक्ति, कंपनी या संगठन होने का नाटक करके लोगों को व्यक्तिगत या वित्तीय जानकारी साझा करने, हानिकारक लिंक पर क्लिक करने, असुरक्षित अटैचमेंट खोलने या भुगतान करने के लिए धोखा देने का तरीका है।

यह उन सबसे आम तरीकों में से एक है जिससे साइबर क्रिमिनल्स लोगों को धोखा देने के लिए ईमेल का इस्तेमाल करते हैं। एक फेक ईमेल ऐसा लग सकता है जैसे वह आपके बैंक, कूरियर कंपनी, सरकारी विभाग या यहाँ तक कि परिवार के किसी सदस्य की ओर से आया हो, और यह आपको बिना जाँच किए कार्रवाई करने के लिए उकसाने हेतु जल्दबाजी पैदा कर सकता है।

फिशिंग के कुछ सामान्य रूप और रोज़मर्रा की स्थितियों में वे कैसे दिखाई दे सकते हैं, वे नीचे दिए गए हैं।



फेक बैंक/अकाउंट ईमेल अपडेट करें

एक फेक ईमेल दावा करता है कि आपके KYC, अकाउंट, क्रेडिट कार्ड या पासवर्ड को अपडेट करने की ज़रूरत है और ऐसा न करने पर अकाउंट ब्लॉक करने की धमकी दे सकता है।

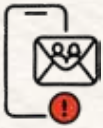
ऐसे लिंक्स पर क्लिक न करें या कोई भी सेंसिटिव डिटेल्स शेयर न करें। अपने बैंक से खुद जाकर चेक करें।



फेक डिलीवरी/ रिफंड ईमेल

एक फेक ईमेल दावा करता है कि आपके पार्सल में देरी हो गई है, कोई रिफंड पेंडिंग है या पेमेंट की ज़रूरत है।

लिंक पर क्लिक न करें या भुगतान न करें; अपने ऑर्डर या रिफंड की जाँच कंपनी के ऑफिशियल ऐप या वेबसाइट के माध्यम से करें।



फेक फैमिली/परिचित व्यक्ति ईमेल

एक ईमेल ऐसा लग सकता है जैसे वह परिवार के किसी सदस्य, दोस्त या आपके किसी परिचित की ओर से आया हो और उसमें पैसे, जानकारी या तत्काल मदद माँगी जा सकती है।

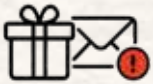
ऐसे अनुरोधों की पुष्टि करने के लिए उन्हें सीधे कॉल करें।



फेक गवर्नमेंट ईमेल

एक फेक ईमेल सरकारी विभाग से होने का दावा कर सकता है और आपसे अपनी निजी डिटेल्स अपडेट करने, जुर्माना/चालान भरने या डॉक्यूमेंट्स जमा करने के लिए कह सकता है।

लिंक्स पर क्लिक न करें या डॉक्यूमेंट्स शेयर न करें; डिपार्टमेंट की ऑफिशियल वेबसाइट के माध्यम से वेरिफाई करें ।



फेक ऑफर्स ईमेल

एक फेक ईमेल आपको इनाम, कैशबैक, गिफ्ट या डिस्काउंट का वादा कर सकता है और आपसे किसी लिंक पर क्लिक करने, डिटेल्स शेयर करने या फीस देने के लिए कह सकता है।

अनपेक्षित ऑफर्स पर कार्रवाई न करें; कंपनी की ऑफिशियल वेबसाइट या ऐप के ज़रिए उनकी पुष्टि करें।





हमेशा याद रखें

एक स्कैमर आपसे संपर्क करने के लिए अलग-अलग तरीकों का इस्तेमाल कर सकता है, लेकिन उनकी चाल अक्सर एक ही होती है; वह व्यक्ति होने का नाटक करना जिस पर आप भरोसा करते हैं और आपको क्लिक करने, जानकारी साझा करने या पेमेंट करने के लिए उकसाना।

फिशिंग

ईमेल के जरिए

"आपका बैंक अकाउंट ब्लॉक कर दिया जाएगा। अपना KYC अभी अपडेट करें।"

स्मीशिंग

SMS/व्हाट्सएप के माध्यम से

"आपका KYC एक्सपायर हो गया है। इसे अपडेट करने के लिए यहाँ क्लिक करें।"

विशिंग

फोन कॉल के जरिए

"मैं आपके बैंक से कॉल कर रहा हूँ। कृपया अपने अकाउंट डिटेल्स वेरिफाई करें।"

क्विशिंग

QR कोड के जरिए

"अपना रिफंड पाने के लिए इस QR कोड को स्कैन करें।"

चैनल बदल सकता है, लेकिन चेतावनी के संकेत वही रहते हैं।



रुकें → **वेरिफाई करें** → **फिरे एक्शन लें**



सोशल मीडिया सेफ्टी

सोशल मीडिया हमें परिवार, सहकर्मियों, दोस्तों और सामुदायिक समूहों के साथ जुड़े रहने में मदद करता है। हम इसका उपयोग उन लोगों से फ़ोटो, मैसेज, वीडियो और जानकारी साझा करने और प्राप्त करने के लिए करते हैं जिन्हें हम जानते हैं और जिन पर भरोसा करते हैं। लेकिन ऑनलाइन कंटेंट हमेशा असली नहीं होता है, और यहाँ तक कि परिचित अकाउंट भी नकली या कॉम्प्रोमाइज्ड हो सकते हैं। हम जो साझा करते हैं वह व्यक्तिगत जानकारी को भी उजागर कर सकता है।

इसीलिए सोशल मीडिया सेफ्टी ज़रूरी है: यह हमें यह जानने में मदद करती है कि किस पर भरोसा करना है, क्या शेयर करना है, क्या फॉरवर्ड करना है और कौन हमारी जानकारी देख सकता है।



सुरक्षित रहने के तरीके

- अपनी प्राइवेसी सेटिंग्स को नियमित रूप से चेक करें और चुनें कि आपकी प्रोफाइल, पोस्ट, फोटो और निजी जानकारी कौन देख सकता है।

- पोस्ट करने से पहले सोचें और जाँच लें कि क्या कोई फोटो या पोस्ट आपके घर का पता, लोकेशन, फोन नंबर, ट्रैवल प्लान, डॉक्यूमेंट या अन्य निजी डिटेल्स को उजागर करती है।

- विश्वास करने या फॉरवर्ड करने से पहले जाँच लें और किसी विश्वसनीय या आधिकारिक स्रोत के माध्यम से चौंकाने वाले दावों को वेरिफाई करें।

- फ्रेंड रिक्वेस्ट सावधानी से स्वीकार करें और केवल उन्हीं लोगों से जुड़ें जिन्हें आप जानते हैं या जिनकी पुष्टि कर सकते हैं।

- अगर आपके जान-पहचान वाले लोग आपसे मदद या पैसों की कोई अजीब माँग करते हैं, तो उन्हें सीधे उनके पुराने नंबर पर कॉल करके इसकी पुष्टि करें।

- इनाम, फ्री गिफ्ट, अविश्वसनीय डिस्काउंट या इन्वेस्टमेंट के अवसरों की पेशकश करने वाले लिंक से सावधान रहें, जब तक कि आपने उनकी पुष्टि न कर ली हो।

- संवेदनशील जानकारी को निजी रखें और सोशल मीडिया के माध्यम से कभी भी OTP, पिन, पासवर्ड, बैंकिंग विवरण, ID या महत्वपूर्ण दस्तावेज़ साझा न करें।

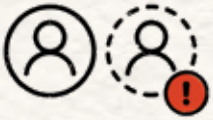
- उन अकाउंट्स से आने वाले डायरेक्ट मैसेजेस से सावधान रहें जो किसी दोस्त के दोस्त, दूर के रिश्तेदार या पारिवारिक मित्र होने का नाटक करते हैं। हमेशा संबंधित मित्र या परिवार के सदस्य से इसकी पुष्टि करें।

- दबाव डालने वाली, धमकी देने वाली या आपको असहज करने वाली बातचीत जारी रखने के बजाय संदिग्ध अकाउंट्स को ब्लॉक और रिपोर्ट करें।

- याद रखें कि सोशल मीडिया शेयरिंग प्राइवेट नहीं है, क्योंकि प्राइवेट मैसेज, फोटो और पोस्ट को सेव या फॉरवर्ड किया जा सकता है।



सोशल मीडिया-से जुड़े फ्रॉड आमतौर पर कैसे होते हैं



फेक फैमिली/फ्रेंड अकाउंट

एक फेक प्रोफाइल पैसे या तुरंत मदद माँगने के लिए परिवार के किसी सदस्य या दोस्त के नाम और फोटोग्राफ का इस्तेमाल कर सकती है। अगर कोई रिक्वेस्ट असामान्य या अर्जेंट लगती है, तो कोई भी कदम उठाने से पहले उस व्यक्ति को सीधे उस नंबर पर कॉल करें जो आपके पास पहले से है।

गलत या भ्रामक जानकारी



कोई पोस्ट, मैसेज या वीडियो किसी सरकारी नियम, स्वास्थ्य सलाह, वित्तीय अवसर या इमरजेंसी के बारे में दावे कर सकता है और लोगों को इसे फॉरवर्ड करने या फीस देने के लिए प्रोत्साहित कर सकता है। किसी चीज़ को सिर्फ इसलिए सच न मानें क्योंकि इसे बहुत ज़्यादा शेयर किया गया है; विश्वास करने या फॉरवर्ड करने से पहले किसी भरोसेमंद या आधिकारिक स्रोत से इसकी जाँच करें।



फेक प्राइज/गिवअवे/ऑफर

कोई पोस्ट, पेज या मैसेज यह दावा कर सकता है कि आपने कोई इनाम जीता है, आपको कोई खास डिस्काउंट मिला है या आपको किसी गिफ्ट के लिए चुना गया है, और फिर आपसे किसी लिंक पर क्लिक करने, फाइनेंशियल जानकारी देने या फीस चुकाने के लिए कह सकता है। जवाब देने से पहले किसी भी अनपेक्षित इनाम या ऑफर की पुष्टि संगठन की ऑफिशियल वेबसाइट या ऐप के ज़रिए ज़रूर करें।



हमेशा याद रखें

स्कैमर्स आपके सोशल मीडिया पोस्ट की जानकारी का इस्तेमाल अपने मैसेज को निजी और भरोसेमंद बनाने के लिए कर सकते हैं। अपनी निजी जानकारी को सार्वजनिक रूप से साझा र करने से बचें।

प्राइवेसी बेस्ट प्रैक्टिसेज़



शायद आपको इसका अहसास न हो, लेकिन हम ऐप्स का इस्तेमाल करते समय, ऑनलाइन शॉपिंग करते समय, पेमेंट करते समय, ट्रैवल बुकिंग करते समय, ग्रुप्स में शामिल होते समय, फॉर्म भरते समय या सर्विसेज के लिए साइन अप करते समय हर दिन अपनी निजी इंफॉर्मेशन शेयर करते हैं। इसमें हमारा नाम, फोन नंबर, एड्रेस, फोटोग्राफ्स, ID, फाइनेंशियल इंफॉर्मेशन और हमारे परिवार के बारे में डिटेल्स शामिल हो सकते हैं। इंफॉर्मेशन शेयर करना अक्सर ज़रूरी होता है, लेकिन ज़रूरत से ज्यादा शेयर करने से दूसरों को ऐसी जानकारी मिल सकती है जिसकी उन्हें ज़रूरत नहीं है।

प्राइवेसी की अच्छी आदतें आपको इस बात पर कंट्रोल रखने में मदद करती हैं कि आप क्या शेयर करते हैं, किसके साथ और क्यों।



जानें कि निजी जानकारी में क्या-क्या आता है

- नाम, फोन नंबर और ईमेल
- घर का पता और जन्म तिथि
- आधार, पैन, पासपोर्ट, वोटर ID और अन्य पहचान दस्तावेज़
- बैंक स्टेटमेंट्स और फाइनेंशियल इन्फॉर्मेशन
- फ़ोटोज़ और वीडियोज़
- लोकेशन इन्फॉर्मेशन
- परिवार की व्यक्तिगत जानकारी (पति/पत्नी, बच्चा, अन्य)



प्राइवेसी बेस्ट प्रैक्टिसेस

ID और ज़रूरी दस्तावेज़ केवल ज़रूरत पड़ने पर ही शेयर करें। जाँच लें कि उन्हें किसकी ज़रूरत है, उन्हें उनकी ज़रूरत क्यों है और उन्हें शेयर करने के लिए किसी भरोसेमंद चैनल का इस्तेमाल करें।

पोस्ट करने या फॉरवर्ड करने से पहले फोटो चेक करें। फोटो में दिखने वाले डॉक्यूमेंट्स, एड्रेस, गाड़ी के नंबर, बिल, लोकेशन या अन्य निजी जानकारी को शेयर न करें या उन्हें मास्क कर दें।

कम्युनिटी ग्रुप्स को शेयर करने लायक जगह मानें। फैमिली, RWA या अन्य ग्रुप्स में शेयर किए गए मैसेज, फोटो और डॉक्यूमेंट्स को कभी भी सेव किया जा सकता है, फॉरवर्ड किया जा सकता है या फेक न्यूज़ फैलाने के लिए इस्तेमाल किया जा सकता है।

- निजी जानकारी साझा करने से पहले रिसीपिएंट को वेरिफाई करें। डॉक्यूमेंट्स या अन्य संवेदनशील जानकारी भेजने से पहले नाम, फोन नंबर या ईमेल एड्रेस चेक करें।

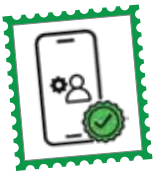
- अपनी निजी जानकारी सार्वजनिक रूप से शेयर करने से बचें। अपना फोन नंबर, घर का पता, जन्म तिथि, परिवार की जानकारी या डेली रूटीन ऑनलाइन पोस्ट न करें।

- दूसरों की प्राइवेसी का सम्मान करें। किसी और की फोटो, इवेंट या निजी डिटेल्स को डिजिटल रूप से पोस्ट या फॉरवर्ड करने से पहले अनुमति माँगें।

- लोकेशन और ट्रैवल की जानकारी को लेकर सावधान रहें। अपनी लाइव लोकेशन, रोज़ाना के रूटीन या ऐसी योजनाओं को सार्वजनिक रूप से शेयर करने से बचें जिनसे यह पता चले कि आप घर से दूर हैं।

- वह व्यक्तिगत जानकारी हटा दें जिसकी अब आपको ज़रूरत नहीं है। अपने फ़ोन, चैट और ईमेल से पुराने दस्तावेज़, स्क्रीनशॉट, डाउनलोड की गई ।D और अनावश्यक फ़ाइलें हटा दें।

- “एग्री” या “एक्सेप्ट” पर क्लिक करने से पहले जाँच लें। समझें कि कौन सी जानकारी, किस उद्देश्य के लिए इकट्ठा की जा रही है, और केवल किसी सर्विस का उपयोग करने के लिए अतिरिक्त जानकारी देने से बचें।



अपनी प्राइवेसी सेटिंग्स चेक करें

आपकी प्राइवेसी सेटिंग्स यह कंट्रोल करती हैं कि आपकी जानकारी कौन देख सकता है और किन ऐप्स के पास आपके अकाउंट का एक्सेस है। इन सेटिंग्स को नियमित रूप से चेक और रिव्यू करें।

सोशल मीडिया के लिए



जहाँ तक संभव हो अपनी प्रोफाइल को प्राइवेट रखें।



अपनी बायो में अपना पूरा पता, फोन नंबर, ईमेल या जन्म तिथि शामिल न करें।



सीमित करें कि आपकी पोस्ट, फोटो और स्टोरीज कौन देख सकता है।



इसकी समीक्षा करें कि कौन आपको फॉलो कर सकता है या आपसे संपर्क कर सकता है और उन लोगों को हटा दें जिन्हें आप नहीं पहचानते।



जब तक आपको वाकई ज़रूरत न हो, लोकेशन शेयरिंग बंद रखें।



रिव्यू करें कि कौन आपको टैग या मेंशन कर सकता है और जहाँ संभव हो टैग्स को अप्रूव करें।

ऐप्स के लिए



अपनी लोकेशन, कॉन्टैक्ट्स, कैमरा, माइक्रोफोन और फोटोज के एक्सेस की जाँच करें।



सिर्फ वही परमिशन्स दें जिनकी किसी ऐप को वाकई ज़रूरत है।



अपने गूगल, एप्पल, ईमेल या सोशल-मीडिया अकाउंट्स से जुड़े ऐप्स का रिव्यू करें।



अपने फोन से उन ऐप्स को हटाने से पहले अकाउंट डिलीट करें जिनका आप अब उपयोग नहीं करते हैं।

क्विक प्राइवेसी

Before you share, post, download
or agree, ask yourself.

- [ ] क्या मैं सिर्फ वही जानकारी शेयर कर रहा हूँ, जो ज़रूरी है?
- [ ] क्या मुझे पता है कि मेरी डिटेल्स कौन माँग रहा है और उन्हें इसकी ज़रूरत क्यों है?
- [ ] क्या मैंने अपनी प्राइवेसी सेटिंग्स चेक की हैं ?
- [ ] क्या मैंने चेक किया कि क्या कोई और ऐप एक्सेस कर सकता है?
- [ ] क्या मैंने शेयर करने से पहले फोटो या डॉक्यूमेंट चेक कर लिया है?
- [ ] क्या मैं इससे सहज महसूस करूँगा/करूँगी अगर इसे सेव या फॉरवर्ड किया जाए?

डिजिटल हाइजीन



डिजिटल हाइजीन का मतलब है अपने डिवाइसेस, अकाउंट्स, पासवर्ड्स और ऑनलाइन एक्टिविटीज को सुरक्षित, व्यवस्थित और मैनेज करने लायक रखने के लिए आसान आदतों को अपनाना।

नियमित डिजिटल चेक-अप आपकी जानकारी को सुरक्षित रखने, सुरक्षा जोखिमों को कम करने और टेक्नोलॉजी का उपयोग करना आसान बनाने में मदद कर सकते हैं।



डिवाइस और अकाउंट हाइजीन

हम बातचीत, मनोरंजन, पेमेंट्स, शॉपिंग और जुड़े रहने के लिए हर दिन अपने फोन का इस्तेमाल करते हैं। समय के साथ, हमारे पास ऐसे अनयूज्ड ऐप्स, पुरानी फाइल्स, भूले हुए अकाउंट्स और सेटिंग्स जमा हो सकते हैं जिन्हें बदलना हमें याद भी नहीं रहता। **समय-समय पर अपने फोन और ऑनलाइन अकाउंट्स को चेक करने से आपकी डिजिटल लाइफ व्यवस्थित, मैनेज करने में आसान और बेहतर बनी रहती है।**

याद रखें

क्या मेरा फोन साफ और व्यवस्थित है?

- **अपने ऐप्स चेक करें:** उन ऐप्स को हटा दें जिनका आप अब उपयोग नहीं करते हैं और केवल उन्हीं को रखें जिनकी आपको ज़रूरत है।
- **अपना स्टोरेज चेक करें:** गैर-ज़रूरी फोटोज, वीडियो, डाउनलोड और फाइल्स को डिलीट करें।
- **अपनी नोटिफिकेशन्स चेक करें:** गैर-ज़रूरी अलर्ट्स को बंद कर दें, ताकि आपका फोन बार-बार आपका ध्यान न भटकाए।
- **अपने अकाउंट्स चेक करें:** उन अकाउंट्स का रिव्यू करें जिनका आप अब इस्तेमाल नहीं करते हैं और जहाँ सही लगे उन्हें क्लोज/डिलीट कर दें।
- **अपने डिवाइसेस चेक करें:** उन फोन्स, टैबलेट्स या कंप्यूटर्स पर अकाउंट्स से साइन आउट करें जिनका आप अब इस्तेमाल नहीं करते हैं।

- **अपनी सेटिंग्स चेक करें:** समय-समय पर फोन और अकाउंट की ज़रूरी सेटिंग्स को रिव्यू करते रहें ताकि आपको पता रहे कि क्या ऑन है।

- **फ्री ट्रायल्स और सब्सक्रिप्शन चेक करें:** ट्रायल शुरू करने से पहले कीमत, रिन्यूअल डेट और कैंसलेशन की शर्तों को चेक करें, और उन सब्सक्रिप्शन को कैंसिल कर दें जिनकी अब आपको ज़रूरत नहीं है।

- **एक डिजिटल क्लीन-अप डे रखें:** हर महीने, अपने फोन, ऐप्स, अकाउंट्स, सेटिंग्स और फाइल्स को रिव्यू करने में कुछ घंटे बिताएं।



याद रखें

जैसे आप अक्सर अपने घर को व्यवस्थित करते हैं, वैसे ही अपनी डिजिटल लाइफ की भी बार-बार सफाई करें।



पासवर्ड हाइजीन

हमारे पास ईमेल, बैंकिंग, शॉपिंग, सोशल मीडिया, ट्रैवल और अन्य सेवाओं के लिए कई अकाउंट्स होते हैं। एक कमज़ोर या दोबारा इस्तेमाल किया गया पासवर्ड एक से अधिक अकाउंट को खतरे में डाल सकता है। **अच्छी अकाउंट सिक्योरिटी का मतलब है मज़बूत पासवर्ड का इस्तेमाल करना और अपनी लॉगिन डिटेल्स को सुरक्षित रखना।**



एक स्ट्रॉन्ग पासवर्ड कैसे बनता है?

एक स्ट्रॉन्ग पासवर्ड लंबा, गेस करने में मुश्किल और हर ज़रूरी अकाउंट के लिए अलग-अलग होना चाहिए।

उदाहरण के लिए:

- ✗ charu123
- ✗ password123
- ✗ ईमेल, बैंकिंग और सोशल मीडिया के लिए एक ही पासवर्ड का उपयोग करना

एक बेहतर तरीका यह है कि आप बिना किसी संबंध वाले शब्दों से बना एक लंबा पासफ्रेज इस्तेमाल करें, जिसमें ज़रूरत के अनुसार नंबर्स या सिम्बल्स भी हों।

- ✓ Mango!River7Window

याद रखें

- महत्वपूर्ण अकाउंट्स के लिए अलग-अलग पासवर्ड्स का इस्तेमाल करें। अपने ईमेल, बैंकिंग और अन्य फाइनेंशियल अकाउंट्स के लिए अलग पासवर्ड्स रखें।
- टू-फैक्टर ऑथेंटिकेशन चालू करें। यह आपके पासवर्ड के अलावा सुरक्षा की एक अतिरिक्त परत जोड़ता है।
- पासवर्ड, OTP या वेरिफिकेशन कोड कभी किसी के भी साथ साझा न करें
- अगर आपको लगता है कि आपका पासवर्ड लीक हो गया है, तो उसे बदल दें। अगर आपने गलती से इसे किसी के साथ शेयर कर दिया है या आपको कोई संदिग्ध गतिविधि दिखाई देती है, तो इसे तुरंत बदलें।
- पुराने अकाउंट्स का रिव्यू करें। जिन अकाउंट्स का आप अब इस्तेमाल नहीं करते हैं उन्हें बंद कर दें, खासकर वे जिनमें निजी या फाइनेंशियल जानकारी हो।
- चेक करें कि आपने कहाँ लॉग इन किया है। उन डिवाइसेस या सेशन्स से साइन आउट करें जिन्हें आप अब नहीं पहचानते या इस्तेमाल नहीं करते।
- पासवर्ड सुरक्षित रूप से स्टोर करें। उन्हें अपने फोन या कंप्यूटर के पास लिखने से बचें; यदि आवश्यक हो, तो एक प्रतिष्ठित पासवर्ड मैनेजर का उपयोग करें।



डिजिटल वेलबीइंग

डिजिटल टेक्नोलॉजी हमें परिवार, दोस्तों और समुदायों से जुड़े रहने में मदद करती है। लेकिन ऑनलाइन बहुत ज़्यादा समय बिताना, लगातार नोटिफिकेशन्स मिलना या हर मैसेज का जवाब देने का दबाव महसूस करना डिजिटल लाइफ को बोझिल बना सकता है। **हेल्दी डिजिटल आदतें आपको अपने फोन को अपने समय, ध्यान या मन की शांति पर हावी होने दिए बिना जुड़े रहने में मदद करती हैं।**

क्या मैं हेल्दी और सहज तरीके से टेक्नोलॉजी का इस्तेमाल कर रहा हूँ?

याद रखें

- तुरंत जवाब देने का दबाव महसूस न करें। अपना समय लें, खासकर तब जब कोई कॉल, मैसेज या रिक्वेस्ट बहुत ज़रूरी लगे।
- अपने फोन से नियमित रूप से ब्रेक लें। भोजन, बातचीत, सैर और सोने से पहले फोन-फ्री समय रखें।
- ऑफ़लाइन भी जुड़े रहें। फोन के समय और परिवार, शौक, सैर-सपाटे तथा अन्य गतिविधियों के बीच संतुलन बनाए रखें।
- अपने मन की शांति बनाए रखें। उन ग्रुप्स और बातचीत को म्यूट करें, छोड़ दें या अनदेखा करें जो तनावपूर्ण या असहज महसूस कराते हों।
- जब पक्का न हो तो मदद माँगें। अगर आपको कोई ऐप, मैसेज, सेटिंग या नोटिफिकेशन समझ नहीं आ रहा है, तो आगे बढ़ने से पहले किसी भरोसेमंद व्यक्ति से पूछें।

साइबरक्राइम रिड्रेसल





अगर आपको साइबरक्राइम का सामना करना पड़े तो क्या करें?

तुरंत कार्रवाई करें (लेकिन शांत रहें)।

घटना की रिपोर्ट करने में इंतज़ार न करें या शर्मिंदगी महसूस न करें।

अपने बैंक या पेमेंट सर्विस को तुरंत सूचित करें।

उनसे प्रभावित अकाउंट, कार्ड, UPI ID या ट्रांजेक्शन को ब्लॉक या सुरक्षित करने के लिए कहें, जैसा भी लागू हो।

सबूत सुरक्षित रखें।

इंसिडेंट से जुड़े स्क्रीनशॉट्स, ट्रांजैक्शन ID, मैसेज, फोन नंबर, ईमेल एड्रेस, लिंक और अन्य डिटेल्स को सेव करें।

प्रभावित अकाउंट्स को सुरक्षित करें।

पासवर्ड बदलें, टू-स्टेप वेरिफिकेशन इनेबल करें और यदि आवश्यक हो तो कार्ड या पेमेंट सर्विसेज को ब्लॉक करें।

संदिग्ध अकाउंट्स या नंबर्स को रिपोर्ट करें।

सबूतों को सेव करने के बाद संबंधित प्लेटफॉर्म या रिपोर्टिंग सर्विस का इस्तेमाल करें और अकाउंट को ब्लॉक कर दें।

अगर ऑनलाइन रिपोर्टिंग मुमकिन नहीं है, तो अपने नज़दीकी पुलिस स्टेशन या साइबरक्राइम पुलिस स्टेशन जाएँ।

अपनी शिकायत/रेफरेंस डिटेल्स अपने पास रखें।

अपनी शिकायत को ट्रैक करते रहें।

एक्नॉलेजमेंट या कंप्लेंट नंबर को सेव करें और फॉलो अप के लिए इसका इस्तेमाल करें।

कहाँ रिपोर्ट करें?



अगर आपके साथ कोई साइबरक्राइम या फाइनेंशियल फ्रॉड हुआ है

फाइनेंशियल फ्रॉड की रिपोर्ट करने के लिए तुरंत **1930 पर कॉल** करें। आप **नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल** के ज़रिए ऑनलाइन साइबर क्राइम की शिकायत दर्ज और ट्रैक भी कर सकते हैं।

पोर्टल: cybercrime.gov.in

हेल्पलाइन: 1930

अगर आपको कोई संदिग्ध कॉल, SMS या मैसेज मिलता है



चक्षु - संचार साथी के माध्यम से संदिग्ध धोखाधड़ी वाले संचार की रिपोर्ट करें। इसमें संदिग्ध धोखाधड़ी वाली कॉल, SMS और व्हाट्सएप मैसेज शामिल हैं, जिनमें किसी और के नाम पर किए गए प्रयास भी शामिल हैं।

www.sancharsaathi.gov.in



अगर आपको एक सीनियर सिटीजन के तौर पर सपोर्ट की ज़रूरत है

सीनियर सिटीजन से जुड़ी चिंताओं के लिए मार्गदर्शन, सहायता और मदद पाने के लिए **एल्डर लाइन - 14567 पर कॉल करें।**



अगर आपको स्थानीय पुलिस की सहायता चाहिए

अपने **नज़दीकी पुलिस स्टेशन या साइबरक्राइम पुलिस स्टेशन** पर जाएँ। इमरजेंसी या साइबरक्राइम के अलावा अन्य अपराधों के लिए, स्थानीय पुलिस से संपर्क करें।

अगर आपका बैंक, कार्ड या UPI शामिल है

अपनी पासबुक, बैंक स्टेटमेंट, आधिकारिक वेबसाइट या ऐप से **कस्टमर-केयर नंबर** लेकर तुरंत अपने बैंक से संपर्क करें।





गोल्डन ऑवर को याद रखें

फाइनेंशियल फ्रॉड होने के पहले एक घंटे के भीतर तुरंत शिकायत दर्ज करें और अपने बैंक से संपर्क करें ताकि पैसे वापस मिलने की संभावना बढ़ सके।



रिपोर्ट करते समय यह जानकारी तैयार रखें

- घटना की तारीख और समय,
- खोई हुई राशि, यदि कोई हो
- ट्रांजैक्शन ID / UTR नंबर
- बैंक या UPI विवरण शामिल हो
- फोन नंबर और ईमेल एड्रेस
- मैसेजेस, प्रोफाइल्स या वेबसाइट्स के स्क्रीनशॉट्स
- संबंधित लिंक्स और अकाउंट डिटेल्स
- पहले से प्राप्त कोई भी शिकायत/रेफरेंस नंबर

OPTIV | DSCI
PROMOTING DATA PROTECTION



दूसरों की सुरक्षा की परवाह करना ही शेयरिंग है।

ऑनलाइन सुरक्षित रहना जागरूकता के साथ शुरू होता है। अपने परिवार, दोस्तों और प्रियजनों के साथ यह गाइड साझा करें ताकि उन्हें आत्मविश्वास के साथ डिजिटल दुनिया का उपयोग करने में मदद मिल सके।

क्या आप गाइड को अपने पास रखना चाहते हैं?
अपनी कॉपी डाउनलोड करने के लिए QR कोड स्कैन करें
और जब भी आपको ज़रूरत हो, बेहतरीन तरीकों को फिर से देखें।



DSCI_Connect | dsci.connect | dsci.connect | dscivideo | data-security-council-of-india

Data Security Council of India (DSCI), 4th Floor,
Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303.