सत्यमेव जयते

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre

साइबर अपराधों से बचाव हेतु मार्गदर्शिका बुकलेट,

साइबर अपराधों से बचाव के लिए ज़रूरी
क्या करें और क्या ना करें

रुको. सोचो. एक्शन लो.

विषय सूची

धोखाधड़ी की चेतावनी

विषय	पृष्ठ संख्या
केवाईसी (KYC) स्कैम	4
ऑनलाइन जॉब स्कैम	5
ऑनलाइन शॉपिंग स्कैम	6
डिजिटल अरेस्ट स्कैम	7
इन्वेस्टमेंट स्कैम	8
ऑनलाइन गेमिंग स्कैम	9
लॉटरी स्कैम	10
फिशिंग	11
विशिंग	12
क्विशिंग	13
सर्च इंजन स्कैम	14
सोशल मीडिया प्रतिरूपण स्कैम	15

विषय सूची

धोखाधड़ी की चेतावनी

विषय	पृष्ठ संख्या
एसएमएस/ ईमेल स्कैम्स	16
डेबिट/क्रेडिट कार्ड स्कैम	17
मोबाइल एप्लिकेशन/ एपीके स्कैम	18
साइबर स्लेवरी	19
सिम स्वैपिंग स्कैम	20
मनी म्यूल्स	21
जूस जैकिंग	22
डीपफेक साइबर स्कैम	23
रिमोट एक्सेस स्कैम	24
असुरक्षित ब्राउज़िंग	25
रैंसमवेयर स्कैम	26
स्मार्टफोन स्कैम	27

केवाईसी (KYC) स्कैम

केवाईसी धोखाधड़ी में साइबर अपराधी गलत पहचान दिखाकर व्यक्तिगत जानकारी चुराते हैं, पहचान की चोरी करते हैं या वित्तीय खातों तक अवैध रूप से पहुंच बनाते हैं। इससे व्यक्तियों, व्यवसायों और वित्तीय संस्थानों को महत्वपूर्ण वित्तीय नुकसान और प्रतिष्ठा संबंधी नुक्सान हो सकता है। आम तौर पर लोगों को धोखा देना, दस्तावेज बनाना और नकली पहचान बनाना शामिल है।

✓ क्या करें

- **अनुरोधों को जाँचें:** किसी भी केवाईसी अपडेट अनुरोध की पुष्टि करने के लिए सीधे अपने बैंक या वित्तीय संस्थान से संपर्क करें।
- **आधिकारिक संपर्कों का उपयोग करें:** कॉन्टैक्ट नंबर या ग्राहक सेवा विवरण केवल आधिकारिक वेबसाइट या विश्वसनीय स्रोतों से प्राप्त करें।
- **स्कैम को रिपोर्ट करें:** यदि आपको किसी साइबर स्कैम का संदेह है तो तुरंत अपने बैंक या वित्तीय संस्थान को सूचित करें।
- **केवाईसी अपडेट के तरीकों की जांच करें:** केवाईसी विवरण अपडेट करने के लिए उपलब्ध तरीकों के बारे में अपने बैंक से सलाह लें।

× क्या ना करें

- **क्रेडेंशियल्स सुरक्षित रखें:** अपने अकाउंट लॉग इन विवरण, कार्ड की जानकारी, पिन, पासवर्ड या ओटीपी कभी भी किसी के साथ या अनधिकृत वेबसाइटों/ऐप्स पर ना डालें।
- **दस्तावेज़ सुरक्षित रखें:** केवाईसी दस्तावेज या उससे जुड़ी जानकारी अज्ञात व्यक्तियों या संगठनों के साथ साझा न करें।
- **संदिग्ध लिंक से बचें:** ईमेल या मैसेज के माध्यम से प्राप्त संदिग्ध लिंक पर क्लिक न करें।

ऑनलाइन जॉब स्कैम

ऑनलाइन नौकरी स्कैम गृहणी, कॉलेज के छात्र, एवं वृद्ध लोगों को धोखा देते हैं। धोखेबाज वेबसाइटों, सोशल मीडिया पर नकली नौकरियां पोस्ट करते हैं, या उची पगार और आसान काम का लालच दे कर ईमेल भेजते हैं। उनका उद्देश्य पीड़ित के पैसे या निजी जानकारी की चोरी करना होता है।

✓ क्या करें

- **विश्वसनीय स्रोतों का उपयोग करें:** प्रामाणिक निजी और सरकारी नौकरी लिस्टिंग के लिए समाचार पत्रों, जॉब पोर्टल्स या सरकारी पोर्टल्स को देखें।
- **कंपनी के बारे में जाँच करें:** अंतर्राष्ट्रीय नौकरी के प्रस्तावों के लिए, कंपनी की जाँच पड़ताल करें और सुनिश्चित करें कि आपके पास सही वर्क वीजा है।
- **प्रश्न पूछें:** ऑनलाइन इंटरव्यू के दौरान, कंपनी और इंटरव्यू लेने वाले के बारे में विस्तृत प्रश्न पूछें।
- **ईमेल की जाँच करें:** ईमेल को अच्छे से देखें जो वास्तविक कंपनियों के ईमेल की नकल करते हैं। उदाहरण के लिए, info@company.com के स्थान पर info@company.net

× क्या ना करें

- **अग्रिम शुल्क से बचें:** कंपनी की वैधता की जाँच किए बिना कोई परामर्श शुल्क न दें।
- **संदेहवादी बनें:** स्पॉन्सर्ड सर्च परिणामों या अनचाही नौकरी के ईमेल पर आँख बंद करके भरोसा न करें।
- **विज्ञापनों की जाँच करें:** सोशल मीडिया प्लेटफॉर्म या ग्रुप पर विशेष रूप से विज्ञापनों की प्रामाणिकता की जाँच किए बिना कभी भी नौकरियों के लिए आवेदन न करें।

ऑनलाइन शॉपिंग स्कैम

ऑनलाइन शॉपिंग स्कैम, स्कैमर आपको नकली ऑफर्स देकर ठगते हैं। वे नकली वेबसाइट बनाते हैं या प्लेटफार्म पर हेरफेर कर के ऐसी डील्स पेश करते हैं जो सच से एकदम परे होती हैं। वह उस वेबसाइट से आपकी व्यक्तिगत और वित्तीय जानकारी चुराते हैं, जिससे वित्तीय नुकसान होता है और ऑनलाइन मार्केटप्लेस में अविश्वास पैदा होता है।

✓ क्या करें

- **कीमतों की तुलना करें:** विभिन्न ई-कॉमर्स वेबसाइटों पर कीमतों की तुलना करें।
- **कैश-ऑन-डिलीवरी का उपयोग करें:** यदि कोई वेबसाइट संदिग्ध लगती है, तो कैश-ऑन-डिलीवरी का विकल्प चुनें।
- **जाँच परख के विक्रेता चुनें:** ई-कॉमर्स वेबसाइटों पर "जाने पहचाने" विक्रेताओं से ही खरीदारी करें।
- **ऑफ़र की जाँच करें:** उन ऑफ़र्स से सतर्क रहें जो अविश्वसनीय रूप से आकर्षक लगते हैं।
- **सुरक्षित लेनदेन:** याद रखें, आपको कभी भी पैसा प्राप्त करने के लिए पिन, पासवर्ड या ओटीपी दर्ज करने की आवश्यकता नहीं होती है।

× क्या ना करें

- **सार्वजनिक नेटवर्क से बचें:** सार्वजनिक कंप्यूटर या नेटवर्क का उपयोग करके ई-शॉपिंग लेनदेन न करें।
- **अपनी जानकारी सुरक्षित रखें:** अविश्वसनीय ई-शॉपिंग वेबसाइटों पर अपने कार्ड विवरण, जन्मतिथि, फोन नंबर आदि को सेव ना करें।
- **विक्रेताओं की जाँच करें:** विक्रेता के क्रेडेंशियल्स की जाँच किए बिना C2C प्लेटफॉर्म जैसे OLX, Quikr आदि पर पहले भुगतान न करें।
- **क्यूआर (QR) कोड से सावधान रहें:** व्हाट्सएप या टेलीग्राम पर किसी अज्ञात व्यक्ति द्वारा 'पैसा प्राप्त करने' हेतु क्यूआर कोड को स्कैन न करें।

डिजिटल अरेस्ट

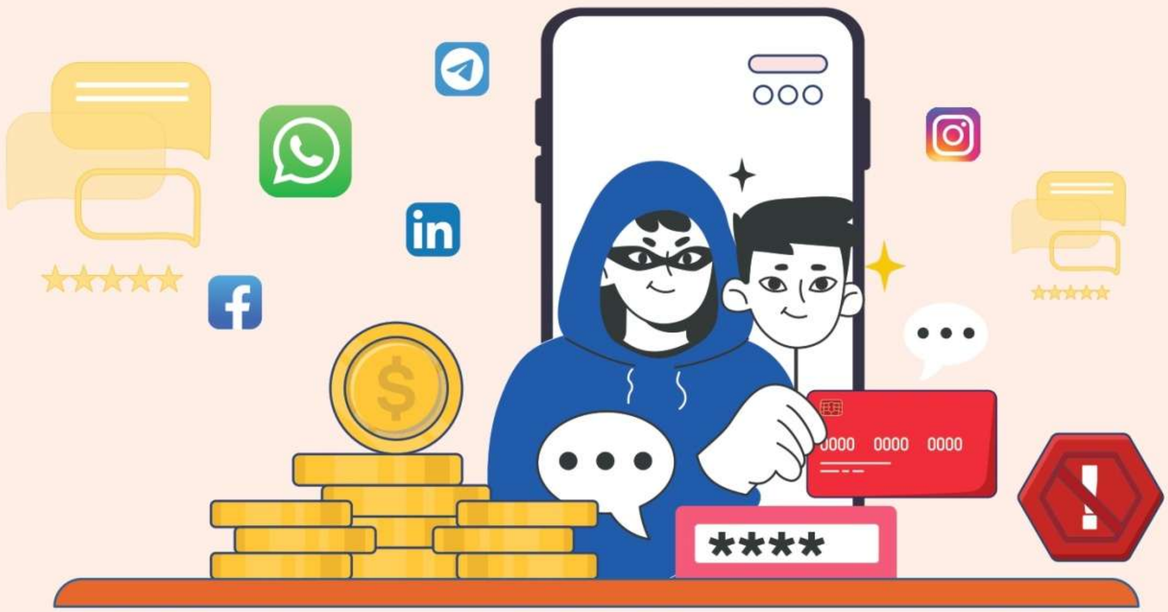
डिजिटल अरेस्ट तब होता है जब किसी को विधियों के बजाय डिजिटल माध्यमों से हिरासत में लिया जाता है या प्रतिबंधित किया जाता है। इसमें अक्सर धोखेबाज सरकारी अधिकारियों के रूप में आपको डरा कर पैसे वसूलते हैं।

✓ क्या करें

- **तथ्य जानें:** पुलिस या सरकारी अधिकारी कभी भी वीडियो कॉल के जरिए पूछताछ नहीं करते हैं।
- **व्यक्तिगत जानकारी बताने से बचें:** कोई भी सरकारी अधिकारी वीडियो कॉल के माध्यम से पैसे या व्यक्तिगत विवरण नहीं मांगेगा।
- **कॉल्स को रिपोर्ट करें:** यदि आपको ऐसे कॉल आते हैं, तो उन्हें तुरंत www.cybercrime.gov.in के "Check & Report" टैब पर रिपोर्ट करें।
- **कानून को समझें:** भारत में "डिजिटल गिरफ्तारी" जैसी कोई चीज नहीं है।

✕ क्या ना करें

- **घबराएं नहीं:** शांत रहें और घोटालों का शिकार होने से बचें।
- **धोखेबाजों को पैसे न दें:** यदि कोई आपको वीडियो कॉल के माध्यम से दबाव डालता है तो भूल से भी पैसे न भेजें।
- **लंबे समय तक व्यस्त न रहें:** संदिग्ध लगने वाले लंबे वीडियो कॉल में फंसने से बचें।
- **अविश्वसनीय कॉल पर भरोसा न करें:** पैसे मांगने वाले सरकारी अधिकारियों के नाम पर आने वाले किसी भी वीडियो कॉल को अनदेखा करें।



इन्वेस्टमेंट स्कैम

निवेश घोटाला या इन्वेस्टमेंट स्कैम में धोखाधड़ी वाली योजनाएँ शामिल होती हैं जो उच्च रिटर्न का वादा करती हैं। यह इन्वेस्टमेंट स्कीम सुन ने में बहुत रोचक लगती है पर होती नहीं है।यह स्कैम नए निवेशकों को निशाना बनाते हैं। इसे पोंजी स्कीम के नाम से भी जाना जाता है।

✓ क्या करें

- **पंजीकृत संस्थाओं के साथ निवेश करें:** केवल सेबी-पंजीकृत संगठनों के साथ निवेश करें।
- **निवेश उत्पादों की जाँच करें:** हमेशा विनियमित वित्तीय संस्थाओं के माध्यम से निवेश करें।
- **सूचित रहें:** विनियमित संस्थाओं और वित्तीय उत्पादों के विश्वसनीय सूचना स्रोतों को फॉलो करें।
- **संदिग्ध गतिविधि की रिपोर्ट करें:** 1930 पर कॉल करें या www.cybercrime.gov.in पर रिपोर्ट करें।

× क्या ना करें

- **घबराएं नहीं:** जल्दबाज़ी ना करते हुए प्रस्ताव की जाँच करें।
- **अविश्वसनीय रिटर्न पर भरोसा न करें:** बिना जोखिम के उच्च रिटर्न का वादा करने वाली योजनाओं से बचें।
- **संदिग्ध ग्रुप में शामिल न हों:** संदिग्ध ट्रेडिंग ऐप्स को बढ़ावा देने वाले सोशल मीडिया ग्रुप्स से ना जुड़ें रहें।
- **खतरे के संकेतों को अनदेखा न करें:** यदि रिटर्न समय के साथ बहुत अधिक लगता है तो सावधान हो जाएँ।

ऑनलाइन गेमिंग

ऑनलाइन गेमिंग साइबर अपराधियों के लिए एक हॉटस्पॉट बन गया है, जिसमें वर्चुअल थेफ़्ट और अकाउंट ब्रीच से लेकर वित्तीय धोखाधड़ी और पहचान की चोरी तक के खतरे हैं। साइबर अपराधी फ़िशिंग घोटालों, मैलवेयर और सोशल इंजीनियरिंग के माध्यम से प्लेटफॉर्म की कमियों का फायदा उठाते हैं और गेमर्स को निशाना बनाते हैं।

✓ क्या करें

- **निगरानी रखें:** यदि आप एक माता-पिता हैं, तो अपनी निगरानी में ही अपने बच्चों को ऑनलाइन गेम खेलने दें।
- **असली पैसे की लेनदेन वाले ऐप्स से सावधान रहें:** कई असली पैसे वाले गेमिंग ऐप्स धोखाधड़ी वाले हो सकते हैं। सतर्क रहें और संदिग्ध लगने वाले ऐप्स से बचें।
- **समझदारी से ऐप को परमिशन दें:** ऐप को संपर्क, कैमरा और स्थान जैसी अनुमतियाँ देने से पहले सावधान रहें।
- **व्यक्तिगत जानकारी सुरक्षित रखें:** अपनी संवेदनशील व्यक्तिगत जानकारी, जैसे कि आपका पूरा नाम, पता, या बैंक खाता विवरण, आदि को सुरक्षित रखें।

✕ क्या ना करें

- **संदिग्ध स्रोतों से बचें:** अविश्वसनीय वेब पेज से गेमिंग ऐप्स डाउनलोड न करें।
- **आश्वस्त रिटर्न से सावधान रहें:** सोशल मीडिया या विज्ञापनों के माध्यम से आश्वस्त रिटर्न का वादा करने वाले गेमिंग ऐप्स इंस्टॉल न करें।
- **जानकारी को निजी रखें:** अज्ञात साथी खिलाड़ियों के साथ गोपनीय जानकारी शेयर ना करें।
- **सोशल मीडिया शेयरिंग को सीमित करें:** उत्पीड़न या साइबर हमले का शिकार बनने से बचने के लिए सोशल मीडिया पर अपनी गेमिंग उपलब्धियों को अधिक शेयर करने से बचें।

लॉटरी फ्रॉड

लॉटरी फ्रॉड लोगों को यह विश्वास दिलाते हैं कि उन्होंने एक पुरस्कार जीता है और उसे प्राप्त करने के लिए उन्हें व्यक्तिगत जानकारी बतानी होगी। यह योजनाएं वित्तीय लाभ की उम्मीद का फायदा उठाती हैं और लोगों को धोखा देते हैं।

✓ क्या करें

- **शुल्क का भुगतान न करें:** धोखेबाज अक्सर नकली पुरस्कारों के लिए शिपिंग शुल्क या हैंडलिंग शुल्क की मांग करते हैं। किसी भी लॉटरी के लिए कभी भी पैसे न भेजें।
- **दावों पर सवाल उठाएं:** अनजान लॉटरी जीतने के संदेशों या कॉलों से सावधान रहें।
- **फ्रॉड को रिपोर्ट करें:** यदि आपको लॉटरी घोटाले का संदेह है तो अधिकारियों को सूचित करें।
- **जागरूक रहें:** याद रखें, कोई भी मुफ्त में बड़ी रकम नहीं देता है।

× क्या ना करें

- **क्रेडेंशियल्स शेयर न करें:** लॉटरी दावों के लिए कभी भी निजी विवरण प्रदान न करें या भुगतान न करें।
- **नकली अधिकारियों से सावधान रहें:** आरबीआई सार्वजनिक खाते नहीं रखता है, जमा राशि की याचना नहीं करता है, या व्यक्तिगत/बैंक विवरण का अनुरोध नहीं करता है।
- **नकली संदेशों को अनदेखा करें:** पुरस्कार राशि, सरकारी सहायता, या पुरस्कारों से जुड़े केवाईसी अपडेट का वादा करने वाले प्रस्तावों का जवाब देने से बचें।

फ़िशिंग

फ़िशिंग एक सामान्य साइबर अपराध रणनीति है जो पीड़ितों को नकली लिंक पर क्लिक करने के लिए उकसाते हैं। ये लिंक विश्वसनीय स्रोतों के ईमेल या वेबसाइटों के रूप में दिखाई देते हैं लेकिन उपयोगकर्ताओं को धोखाधड़ी वाली साइटों पर रीडायरेक्ट करते हैं जो लॉगिन क्रेडेंशियल, व्यक्तिगत जानकारी, या वित्तीय विवरण जैसे संवेदनशील डेटा को चुराने के लिए डिज़ाइन की गई होती हैं। फ़िशिंग आपके डिवाइस पर मालवेयर भी डाल सकता है, जिससे साइबर अपराधियों को अनधिकृत प्रवेश मिल जाता है।

✓ क्या करें

- **जागरूक रहें:** ज्ञात स्रोतों से अप्रत्याशित संदेशों के साथ सावधानी बरतें।
- **यूआरएल जांचें:** असली जगह का पता लगाने और विसंगतियों को देखने के लिए लिंक पर होवर करें।
- **भेजने वालों की जानकारी रखें:** यदि आप किसी संदेश की प्रमाणिकता के बारे में अनिश्चित हैं तो एक विश्वसनीय विधि के माध्यम से भेजने वाले से संपर्क करें।
- **नियमित रूप से अपडेट करें:** सुरक्षा में किसी प्रकार की कमी ना हो उसके लिए अपने सॉफ़्टवेयर और सिस्टम को अप-टू-डेट रखें।
- **फ़िशिंग रिपोर्ट:** यदि आपको फ़िशिंग में कोई फँसा रहा है तो संबंधित अधिकारियों या प्लेटफार्मों को सतर्क करें।

× क्या ना करें

- **लिंक पर क्लिक करने से बचें:** संदिग्ध लिंक पर क्लिक न करें। अज्ञात संदेशों को तुरंत हटा दें।
- **सदस्यता समाप्त करें और ब्लॉक करें:** संदिग्ध लिंक वाले ईमेल से सदस्यता समाप्त करें और भेजने वाले के ईमेल को ब्लॉक करें।
- **आधिकारिक वेबसाइटों पर जाएं:** वित्तीय लेनदेन के लिए हमेशा आधिकारिक वेबसाइट पर जाएं और वेबसाइट सुरक्षा (पैडलॉक के साथ HTTPS) की जाँच करें।

विशिंग

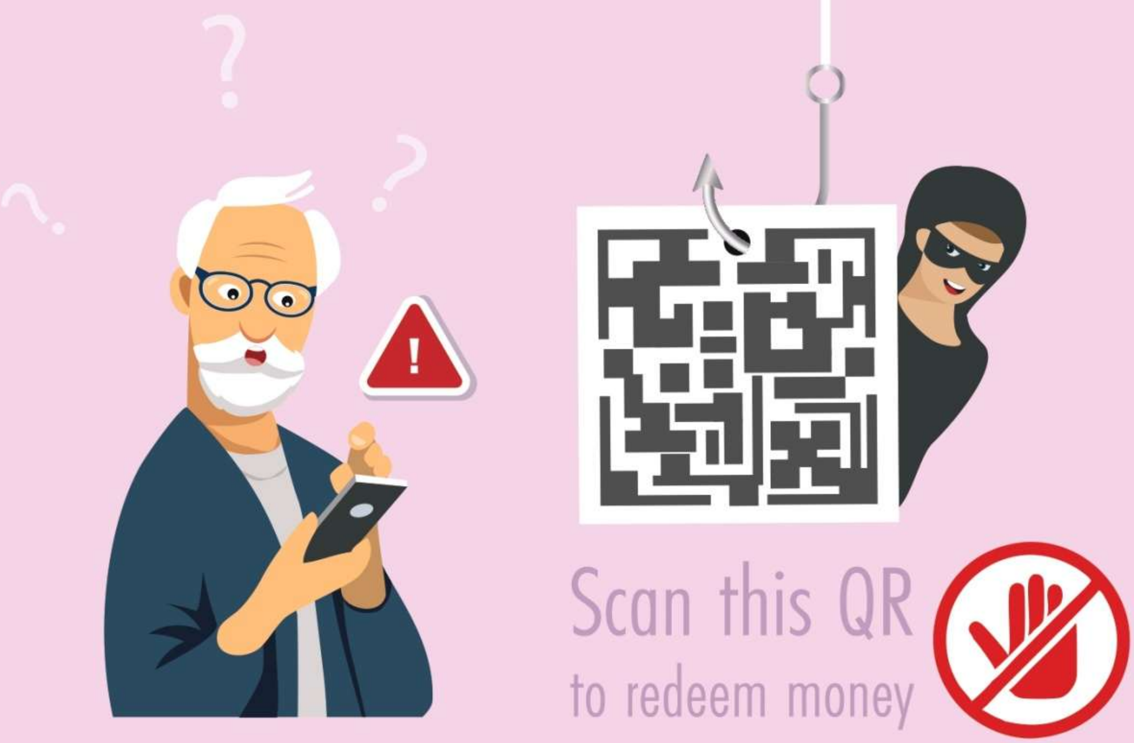
स्पैम/विशिंग कॉल (वॉयस फ़िशिंग) साइबर अपराध का एक दूसरा रूप है। धोखेबाज पीड़ितों को व्यक्तिगत या वित्तीय डेटा जैसी संवेदनशील जानकारी प्रकट करने के लिए सामाजिक इंजीनियरिंग का उपयोग करते हैं। वे अक्सर कॉलर आईडी स्पूफिंग और विश्वास हासिल करने और जानकारी चुराने के लिए तत्कालिकता जैसी रणनीति का उपयोग करके बैंकों या सरकारी एजेंसियों जैसी वैध संस्थाओं का प्रतिरूपण करते हैं।

✓ क्या करें

- **कॉल ब्लॉकर्स का उपयोग करें:** कॉल-ब्लॉकिंग ऐप्स इंस्टॉल करें और स्पैम कॉल को रिपोर्ट करें।
- **सावधान रहें:** अज्ञात नंबरों से आने वाली कॉल का जवाब देते समय सावधानी बरतें।
- **जागरूकता फैलाएं:** दूसरों को सामान्य फोन घोटालों के बारे में शिक्षित करें।
- **सुरक्षा सक्षम करें:** अतिरिक्त सुरक्षा के लिए वॉइसमेल पासवर्ड का उपयोग करें।

× क्या ना करें

- **व्यक्तिगत जानकारी शेयर न करें:** अज्ञात कॉल करने वालों को कभी भी व्यक्तिगत या वित्तीय जानकारी प्रदान न करें।
- **कॉलर आईडी पर भरोसा न करें:** कॉलर आईडी को स्पूफ किया जा सकता है, इसलिए उन पर निर्भर न रहें।
- **अज्ञात नंबरों से बचें:** अपरिचित या अंतर्राष्ट्रीय नंबरों से आने वाली कॉलों पे दुबारा संपर्क न करें।
- **अपने डेटा को सुरक्षित रखें:** वास्तविक संस्थान कभी भी उपयोगकर्ता का नाम, पासवर्ड या ओटीपी जैसी संवेदनशील जानकारी नहीं मांगते हैं। इसे कभी भी शेयर न करें, यहाँ तक कि परिवार के साथ भी नहीं।



क्विशिंग

क्विशिंग घोटाले बढ़ रहे हैं। स्कैमर क्यूआर कोड स्कैन करने के लिए कहकर सौदों या सुविधा का वादा करके पीड़ितों को लुभाते हैं, लेकिन अंतत: अनधिकृत वित्तीय लेनदेन शुरू करते हैं। नकली कोड उपयोगकर्ताओं को फ़िशिंग साइटों पर रीडायरेक्ट कर सकते हैं, लॉगिन क्रेडेंशियल चुरा सकते हैं, या सीधे स्कैमर के खाते में पैसे ट्रांसफर कर सकते हैं।

✓ क्या करें

- **भरोसेमंद स्रोतों को स्कैन करें:** केवल आधिकारिक वेबसाइटों या भरोसेमंद व्यवसायों से क्यूआर कोड स्कैन करें।
- **कुछ भी करने से पहले आश्वस्त हो जाएँ:** स्कैमर अक्सर जल्दबाज़ी पैदा करते हैं। अपना समय लें और जाँच-पड़ताल करें।
- **संदिग्ध कोड की रिपोर्ट करें:** यदि आपको किसी घोटाले का संदेह है, तो कोड की वैध स्रोत और संबंधित अधिकारियों को रिपोर्ट करें।

× क्या ना करें

- **भुगतान के साथ सावधान रहें:** भुगतान ऐप्स के साथ क्यूआर कोड स्कैन करने से बचें, क्योंकि उनमें स्कैमर की अकाउंट डिटेल्स आपको धोखा देने के लिए हो सकती है।
- **पैसे प्राप्त करने के लिए स्कैन न करें:** धन प्राप्त करने के लिए कभी भी क्यूआर कोड स्कैन न करें। वैध लेनदेन के लिए कोड स्कैन करने या एम-पिन या पासवर्ड जैसे बैंकिंग विवरण दर्ज करने की आवश्यकता नहीं होती है।
- **अज्ञात वेबसाइट से सतर्क रहें:** ईमेल, टेक्स्ट या अनजान वेबसाइट से कोड स्कैन न करें।

सर्च इंजन धोखाधड़ी

सर्च इंजन धोखाधड़ी तब होती है जब धोखेबाज वैध संस्थाओं के रूप में प्रदर्शित करने के लिए नकली संपर्क जानकारी प्रदर्शित करने के लिए खोज परिणामों में हेरफेर करते हैं। जो पीड़ित अनजाने में इन नंबरों पर कॉल करते हैं, वे पासवर्ड और खाते के विवरण जैसी संवेदनशील जानकारी प्रकट कर सकते हैं, जिससे वित्तीय नुकसान, पहचान की चोरी और अन्य गंभीर परिणाम हो सकते हैं।

✓ क्या करें

- **आधिकारिक वेबसाइटों पर जाएं:** कॉन्टैक्ट इन्फॉर्मेशन के लिए सर्च रिजल्ट पर निर्भर रहने के बजाय हमेशा आधिकारिक वेबसाइट देखें।
- **संपर्कों की जाँच-पड़ताल करें:** व्यक्तिगत जानकारी बताने से पहले कॉलर आईडी या विश्वसनीय निर्देशिकाओं का उपयोग करके फोन नंबर और वेबसाइटों को दोबारा जांचें।
- **खतरे के संकेतों पर ध्यान दें:** तात्कालिकता, डराने वाली रणनीति या संदिग्ध प्रस्तावों से सावधान रहें। वैध कंपनियां तत्काल कार्रवाई के लिए दबाव नहीं डालती हैं।

× क्या ना करें

- **खोज परिणामों पर भरोसा न करें:** सर्च इंजन रिजल्ट में सूचीबद्ध नंबरों पर कभी कॉल न करें। धोखेबाज अक्सर खुद को अवैध संस्था के रूप में दिखाते हैं।
- **बिना मांगे जानकारी साझा न करें:** फोन पर व्यक्तिगत विवरण तभी बताएं जब आपने संपर्क शुरू किया हो।

सोशल मीडिया प्रतिरूपण

सोशल मीडिया प्रतिरूपण तब होता है जब कोई व्यक्ति किसी वास्तविक व्यक्ति या संगठन की नकल करते हुए एक नकली अकाउंट बनाता है। इन धोखाधड़ी वाले अकाउंट का उपयोग दूसरों को धोखा देने के लिए किया जाता है, जिससे अक्सर पहचान की चोरी, वित्तीय घोटाले, प्रतिष्ठा को नुकसान और गलत जानकारी का प्रसार होता है।

✓ क्या करें

- **खातों की जाँच-परख करें:** प्रमाणिकता की पुष्टि के लिए नीले चेकमार्क, यूज़रनेम और परिचित प्रोफ़ाइल चित्र देखें।
- **प्रतिरूपण की रिपोर्ट करें:** प्लेटफ़ॉर्म और वास्तविक व्यक्ति या संगठन को सूचित करें जिसका प्रतिरूपण किया जा रहा है।
- **धन अनुरोधों की पुष्टि करें:** फोन कॉल या सामने से दोस्तों या रिश्तेदारों से पैसों के अनुरोधों की पुष्टि करें।

× क्या ना करें

- **भुगतान न करें:** अज्ञात व्यक्तियों को ऑनलाइन भुगतान करने से बचें।
- **जानकारी को निजी रखें:** सोशल मीडिया पर कभी भी व्यक्तिगत या गोपनीय विवरण साझा न करें।
- **सावधान रहें:** अनचाहे संदेशों से बचें और कभी भी संदिग्ध लिंक पर क्लिक न करें।

एसएमएस/ ईमेल स्कैम

धोखेबाज़ पीड़ितों को नकली स्कीम से धोखा देने के लिए एसएमएस, ईमेल और कॉल का उपयोग करते हैं। वे अपने लोगों और नकली आईडी का उपयोग करके एनबीएफसी के नाम पर भरोसा हासिल करते हैं। स्कैमर नकली पत्र या चेक भेज कर अग्रिम भुगतान मांगते हैं। एक बार भुगतान हो जाने के बाद, धोखेबाज़ पैसे लेकर गायब हो जाते हैं।

✓ क्या करें

- **प्रमाणिकता की जाँच करें**: हमेशा ईमेल के विवरण को क्रॉस-चेक करें और सीधे आधिकारिक स्रोतों से संपर्क करें।
- **संदिग्ध संदेशों की रिपोर्ट करें:** किसी भी नकली संदेश को आधिकारिक रिपोर्टिंग चैनलों पर भेजें और दूसरों को चेतावनी दें।

× क्या ना करें

- **अनजान प्रस्तावों पर भरोसा न करें:** बिना जानकारी के फोन, ईमेल या टेक्स्ट के माध्यम से ऋण प्रस्तावों पर कभी भरोसा न करें।
- **संवेदनशील जानकारी की पड़ताल करें:** प्रस्ताव की वैधता की पुष्टि किए बिना व्यक्तिगत या वित्तीय विवरण देने से बचें।
- **संदिग्ध ईमेल न खोलें:** अज्ञात स्रोतों से अटैचमेंट या लिंक पर क्लिक न करें या ईमेल न खोलें।
- **अग्रिम शुल्क का भुगतान न करें:** वास्तविक लेंडर्स को लोन प्रोसेस करने के लिए अग्रिम भुगतान की आवश्यकता नहीं होती है।

डेबिट/क्रेडिट कार्ड फ्रॉड

डेबिट और क्रेडिट कार्ड धोखाधड़ी तब होती है जब आपकी सहमति के बिना आपके कार्ड विवरण का उपयोग अनाधिकृत लेनदेन के लिए किया जाता है। अपराधी आपके फिज़िकल कार्ड को चुरा सकते हैं, आपके विवरण को स्किम कर सकते हैं, या फ़िशिंग घोटालों के माध्यम से आपको संवेदनशील जानकारी साझा करने के लिए धोखा दे सकते हैं।

✓ क्या करें

- **अनावश्यक फीचर को बंद रखें:** ऑनलाइन, अंतर्राष्ट्रीय या एनएफसी लेनदेन की आवश्यकता न होने पर उन्हें बंद कर दें।
- **भुगतान करने से पहले जाँच लें:** अपना पिन दर्ज करने से पहले स्क्रीन पर राशि की जाँच करें और स्किमिंग डिवाइस के लिए पीओएस मशीन की जाँच करें।
- **अपने कार्ड को नज़र में रखें**: लेनदेन के दौरान हमेशा अपने कार्ड पर नज़र रखें।
- **अपने पिन को सुरक्षित रखें:** एटीएम या पीओएस मशीनों पर अपना पिन दर्ज करते समय कीपैड को कवर करें।

✗ क्या ना करें

- **विवरण साझा न करें:** कभी भी किसी के साथ कार्ड की जानकारी या पिन शेयर न करें।
- **पिन को स्टोर न करें:** अपने पिन को आसान पहुंच वाली जगहों पर लिखने या सहेजने से बचें।
- **सार्वजनिक वाई-फाई से बचें:** असुरक्षित नेटवर्क पर अपने कार्ड का उपयोग न करें।
- **अलर्ट को अनदेखा न करें:** संदिग्ध लेनदेन होने पर अपने बैंक को तुरंत रिपोर्ट करें।

मोबाइल एप्लीकेशन/ एपीके स्कैम

साइबर अपराधी वैध लोगों के समान चिन्ह और इंटरफेस का उपयोग करके नकली मोबाइल बैंकिंग ऐप बनाते हैं। यह ऐप थर्ड पार्टी के ऐप स्टोर या फ़िशिंग लिंक जैसे अनऑफिशिअल चैनलों के माध्यम से वितरित किए जाते हैं। एक बार इंस्टॉल हो जाने पर, वे आपके बैंकिंग क्रेडेंशियल और व्यक्तिगत डेटा चुरा लेते हैं, जिससे वित्तीय धोखाधड़ी और पहचान की चोरी होती है।

✓ क्या करें

- **आधिकारिक स्टोर से डाउनलोड करें:** हमेशा गूगल प्ले स्टोर या एप्पल एप स्टोर या बैंक वेबसाइटों जैसे विश्वसनीय स्रोतों से बैंकिंग ऐप डाउनलोड करें।
- **ऐप प्रामाणिकता की जाँच करें:** किसी भी बैंकिंग ऐप को इंस्टॉल करने से पहले डेवलपर विवरण की जाँच करें और टर्म्स पढ़ें।
- **सॉफ्टवेयर अपडेट रखें:** सुनिश्चित करें कि आपके फोन का ओएस और सुरक्षा सॉफ्टवेयर हमेशा अपडेटेड हो।
- **दो-कारक प्रमाणीकरण (2 Factor Authentication) सक्षम करें:** अपने खातों में सुरक्षा की एक अतिरिक्त परत जोड़ें।
- **नियमित रूप से बैंक खातों की निगरानी करें:** किसी भी अनाधिकृत लेनदेन के लिए नियमित रूप से अपने बैंक खाते के विवरण की जाँच करें।

× क्या ना करें

- **अनजान लिंक से डाउनलोड न करें:** संदिग्ध ईमेल या वेबसाइटों से लिंक पर क्लिक करने या ऐप डाउनलोड करने से बचें।
- **अज्ञात ऐप्स में संवेदनशील जानकारी दर्ज न करें:** अपरिचित ऐप्स या साइटों में कभी भी बैंकिंग विवरण साझा न करें।
- **अपने डिवाइस को जेलब्रेक न करें:** अपने डिवाइस को रूट करने से यह मैलवेयर और हमलों के प्रति संवेदनशील हो जाता है।
- **क्रेडेंशियल साझा न करें:** कभी भी अपना बैंकिंग पिन या ओटीपी किसी के साथ साझा न करें, भले ही वे सहायता कर्मचारी होने का दावा करें।

साइबर स्लेवरी

साइबर स्लेवरी में डिजिटल प्लेटफार्मों के माध्यम से व्यक्तियों का शोषण होता है, जहाँ उन्हें उचित मुआवज़ा दिए बिना काम करने के लिए मज़बूर या हेरफेर किया जाता है। यह मानव तस्करी और जबरन श्रम के साथ ओवरलैप होता है लेकिन विशेष रूप से शोषण के लिए इंटरनेट और डिजिटल उपकरणों का उपयोग करता है।

✓ क्या करें

- **जानकार एजेंटों के माध्यम से आवेदन करें:** केवल अधिकृत सरकारी एजेंसियों के माध्यम से ही नौकरियों के लिए आवेदन करें।
- **नौकरी के प्रस्तावों की पड़ताल करें:** स्वीकार करने से पहले नौकरी के प्रस्तावों की वैधता को ध्यान से जाँचे।
- **अविश्वसनीय रूप से आकर्षक नौकरियों से सावधान रहें:** ऐसे ऑनलाइन अवसरों से बचें जो कम प्रयास में अधिक वेतन का वादा करते हैं।
- **कंपनी के बारे में जाँचे:** नौकरी की पेशकश करने वाली कंपनी या प्लेटफॉर्म की हमेशा जाँच करें।
- **संदिग्ध गतिविधि को रिपोर्ट करें:** यदि आपको किसी धोखाधड़ी या शोषण का संदेह है, तो तुरंत www.cybercrime.gov.in के "Check and Report" टैब पर रिपोर्ट करें।

× क्या ना करें

- **जल्द पैसे के वादों से बचें:** कम मेहनत में ज़्यादा पैसा देने वाले अवसरों पर भरोसा न करें।
- **पर्यटक वीजा पर काम न करें:** किसी भी देश में नौकरी के लिए सही वीजा लें।
- **सोशल मीडिया के अज्ञात विज्ञापनों पर भरोसा न करें:** अनजान लोगों या ग्रुप के नौकरी प्रस्तावों से सावधान रहें।

सिम स्वैपिंग

सिम स्वैपिंग एक साइबर अपराध है जिसमें धोखेबाज आपका फोन नंबर अपने सिम कार्ड में ट्रांसफर कर लेते हैं। इससे वे आपके कॉल, मैसेज और ओटीपी तक पहुंच बना सकते हैं, जिससे बैंकिंग स्कैम और पहचान चोरी हो सकती है।

✓ क्या करें

- **2-फैक्टर ऑथेंटिकेशन ऑन करें:** अपने ऑनलाइन खातों में अतिरिक्त सुरक्षा जोड़ें।
- **मजबूत पिन सेट करें:** सिम और बैंक खातों के लिए अनुमान लगाने में कठिन पासकोड और पिन रखें।
- **नियमित अपडेट करें:** अपने फोन के सॉफ्टवेयर और ऐप्स को नियमित रूप से अपडेट करते रहें।
- **संदिग्ध गतिविधि की रिपोर्ट करें:** यदि आपको कोई असामान्य गतिविधि दिखाई देती है तो तुरंत अपने नेटवर्क प्रोवाइडर से संपर्क करें।
- **सिम खोने की सूचना तुरंत दें:** अगर आपका सिम बंद हो जाए या खो जाए तो फौरन नेटवर्क प्रोवाइडर को बताएं।

× क्या ना करें

- **ओटीपी या पर्सनल डिटेल्स शेयर न करें:** अनजान लोगों के साथ कोई संवेदनशील जानकारी साझा न करें।
- **आसानी से अनुमान लगाने योग्य पिन का उपयोग न करें:** अपने खातों के लिए आसानी से अनुमान लगाने योग्य पिन न लगाएं।
- **गतिविधि की निगरानी करें:** असामान्य मोबाइल गतिविधि या नेटवर्क पहुंच में लंबे समय तक नुकसान होने पर ध्यान दें और तुरंत कार्यवाही करें।
- **क्रेडेंशियल्स सुरक्षित करें:** अपने सिम कार्ड से जुड़े पहचान विवरण कभी भी शेयर न करें।

मनी म्यूल्स

मनी म्यूल्स वे लोग होते हैं जो जानबूझकर या अनजाने में अवैध धन को इधर-उधर करने में मदद करते हैं। धोखेबाज़ उन्हें कमीशन का लालच देकर चोरी किए गए पैसे को अपने खाते में लेने और आगे भेजने के लिए राजी कर लेते हैं। यह पैसा कई खातों में भेजा जाता है ताकि असली धोखेबाज की पहचान छुपी रहे। ऐसी गतिविधियों में शामिल होना गैरकानूनी है, चाहे अनजाने में ही क्यों न हो, और इसके गंभीर कानूनी परिणाम हो सकते हैं।

✓ क्या करें

- **नौकरी के प्रस्तावों की जाँच करें:** पैसे के लेन-देन से जुड़ी संदिग्ध नौकरियों से सावधान रहें। किसी भी कंपनी या व्यक्ति की वैधता की अच्छी तरह से जाँच करें।
- **वित्तीय जानकारी को सुरक्षित रखें:** कभी भी अज्ञात पार्टियों के साथ बैंक खाते का विवरण या व्यक्तिगत जानकारी शेयर न करें।
- **संदिग्ध गतिविधि की रिपोर्ट करें:** यदि आपको मनी म्यूल योजना का संदेह है तो अधिकारियों से संपर्क करें।

× क्या ना करें

- **खाते शेयर न करें:** कभी भी दूसरों को धन प्राप्त करने या लेन-देन करने के लिए अपने खाते का उपयोग न करने दें।
- **कमीशन लेने से मना करें:** शुल्क के लिए अनधिकृत धन को संभालने के प्रस्तावों को अस्वीकार करें।
- **जोखिमों को जानें:** अवैध धन का लेन-देन करने पर गंभीर कानूनी कार्रवाई हो सकती है।

जूस जैकिंग

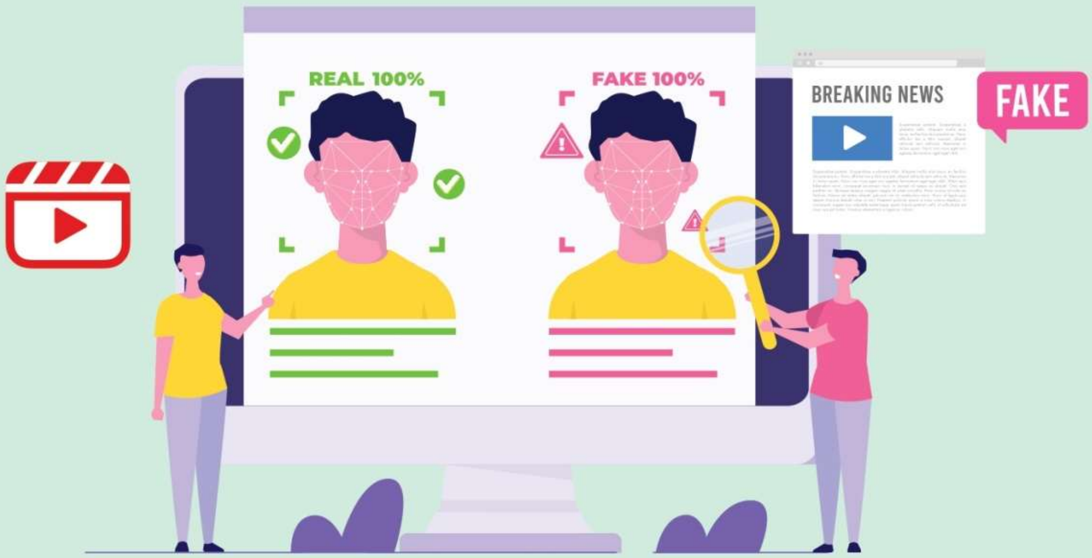
जूस जैकिंग सार्वजनिक USB चार्जिंग स्टेशनों से जुड़ा होता है। हैकर्स ऐसे USB पोर्ट का उपयोग करके मैलवेयर इंस्टॉल कर सकते हैं या संवेदनशील जानकारी चुरा सकते हैं। हालांकि अब तक कोई पुष्ट मामला सामने नहीं आया है, लेकिन सतर्क रहना जरूरी है।

✓ क्या करें

- **अपना चार्जर साथ रखें:** संभावित रूप से छेड़छाड़ किए गए सार्वजनिक पोर्ट से बचने के लिए अपने स्वयं के चार्जर और केबल का उपयोग करें।
- **प्रॉम्प्ट को वेरिफाई करें:** "इस डिवाइस पर भरोसा करें" प्रॉम्प्ट के बारे में सतर्क रहें और केवल विश्वसनीय स्रोत ही स्वीकार करें।
- **AC आउटलेट चुनें:** जब भी संभव हो स्टैण्डर्ड इलेक्ट्रिकल आउटलेट चुनें।

× क्या ना करें

- **सार्वजनिक पोर्ट से बचें:** अज्ञात या सार्वजनिक USB पोर्ट या केबल का उपयोग न करें।



डीपफेक साइबर अपराध

साइबर अपराधी वास्तविक फुटेज या रिकॉर्डिंग में हेरफेर करके नकली वीडियो या ऑडियो क्लिप बनाने के लिए AI का उपयोग करते हैं। इन नकली मीडिया को सोशल मीडिया, मैसेजिंग ऐप और ईमेल के माध्यम से फैलाया जाता है, जो अक्सर सार्वजनिक हस्तियों, मशहूर हस्तियों या अधिकार में मौजूद लोगों को टारगेट करते हैं। इसका लक्ष्य दर्शकों को धोखा देना, राय में हेरफेर करना या गलत जानकारी फैलाना है। अपराधी डीपफेक को वास्तविक दिखाने के लिए सोशल इंजीनियरिंग तकनीकों का उपयोग कर सकते हैं, जिससे व्यक्ति और संगठन जोखिम में आ सकते हैं।

✓ क्या करें

- **सूचित रहें:** डीपफेक तकनीक और इसके जोखिमों के बारे में जानें।
- **कॉन्टेंट को वेरिफाई करें:** शेयर करने या विश्वास करने से पहले हमेशा मीडिया की प्रामाणिकता की जांच करें।
- **विश्वसनीय स्रोतों का उपयोग करें:** समाचार और अपडेट के लिए प्रतिष्ठित प्लेटफार्मों पर निर्भर रहें।
- **संदिग्ध कॉन्टेंट की रिपोर्ट करें:** यदि आपको संभावित डीपफेक मिलते हैं तो अधिकारियों या प्लेटफार्मों को सतर्क करें।

× क्या ना करें

- **अनवेरिफाइड मीडिया को शेयर न करें:** किसी भी कॉन्टेंट की सच्चाई की जाँच किए बिना उस को शेयर करने से बचें।
- **संदिग्ध स्रोतों पर भरोसा न करें:** अविश्वसनीय स्रोतों से दूर रहें जो डीपफेक शेयर कर सकते हैं।
- **आँख बंद करके भरोसा न करें:** जरूरत से ज्यादा भावनात्मक या बढ़ा-चढ़ाकर दिखाए गए कंटेंट से सतर्क रहें।
- **प्राइवेसी को अनदेखा न करें:** प्राइवसी सेटिंग्स की समीक्षा करें और अपनी व्यक्तिगत जानकारी को ऑनलाइन शेयर करने की सीमा तय करें।

रिमोट एक्सेस फ्रॉड

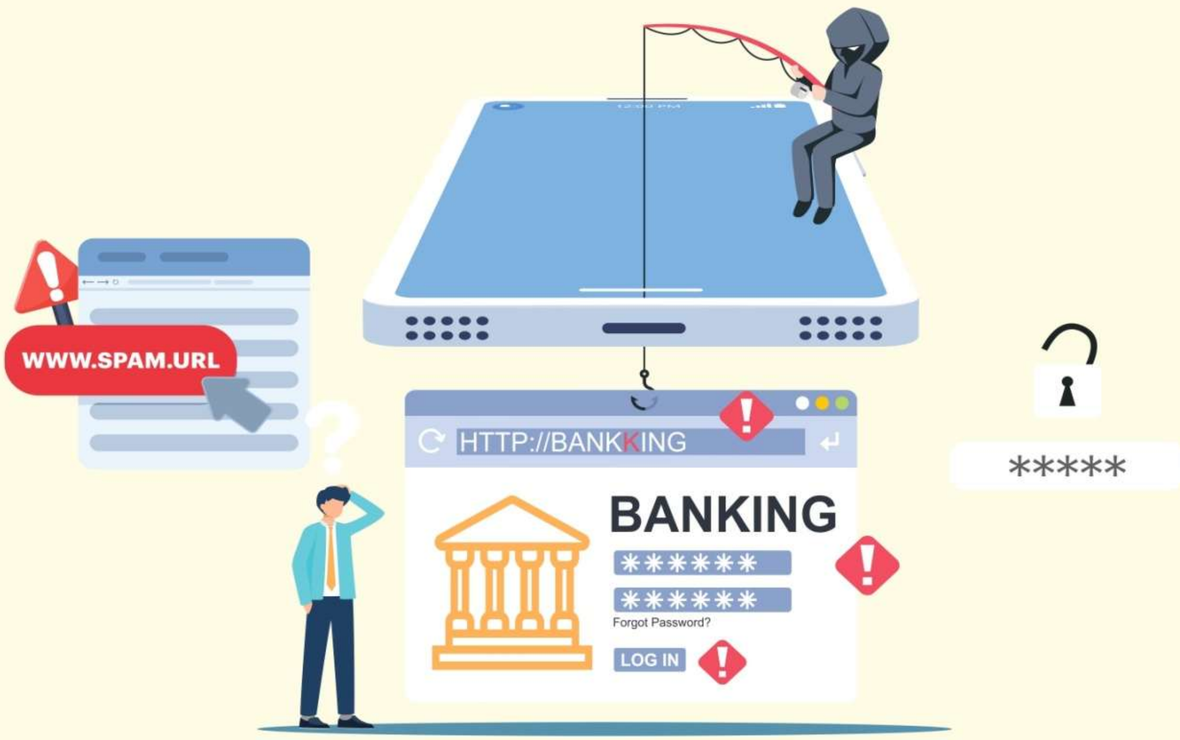
रिमोट एक्सेस फ्रॉड तब होता है जब साइबर अपराधी खुद को विश्वसनीय संस्था बताकर लोगों को धोखा देते हैं। वे स्क्रीन-शेयरिंग ऐप का उपयोग करके पीड़ित के डिवाइस तक अनधिकृत पहुँच बना सकते हैं। एक बार एक्सेस मिलने के बाद, वे संवेदनशील जानकारी चुरा सकते हैं, खातों पर कब्ज़ा कर सकते हैं और धोखाधड़ी वाले लेनदेन कर सकते हैं।

✓ क्या करें

- **सावधानी से भरोसा करें:** कभी भी किसी ऐसे व्यक्ति को रिमोट एक्सेस न दें जिसे आप नहीं जानते और जिस पर आपको भरोसा नहीं है।
- **पहचान वेरिफाई करें:** कॉलर की पहचान सीधे अपने आप वेरिफाई करें (उनके द्वारा दिए गए नंबरों के माध्यम से नही)।
- **अज्ञात सॉफ्टवेयर से बचें:** किसी के अनुरोध पर सॉफ्टवेयर डाउनलोड न करें जब तक कि आप निश्चित न हों।
- **सतर्क रहें:** अवांछित कॉल, संदेशों या ईमेल के बारे में सतर्क रहें।
- **सुरक्षा बढ़ाएं:** मजबूत पासवर्ड का उपयोग करें और मल्टी-फैक्टर ऑथेंटिकेशन सक्षम करें।

× क्या ना करें

- **सुरक्षित रूप से डाउनलोड करें:** स्क्रीन-शेयरिंग ऐप्स अनाधिकारिक स्रोतों से न करें।
- **भुगतान ऐप्स को सुरक्षित करें:** कोई भी स्क्रीन-शेयरिंग सॉफ़्टवेयर डाउनलोड करते वक़्त किसी भी भुगतान संबंधी एप में लॉगिन न रहें।
- **उपयोग के बाद एप हटाएं:** कार्य पूरा होने के बाद स्क्रीन-शेयरिंग ऐप को फ़ोन में न रखें।
- **अपने डेटा की सुरक्षा करें:** कभी भी व्यक्तिगत या वित्तीय जानकारी को शेयर न करें और स्क्रीन एक्सेस वाले व्यक्ति के दौरान क्रेडेंशियल दर्ज करने से बचें।



असुरक्षित ब्राउज़िंग

असुरक्षित ब्राउज़िंग का मतलब है हानिकारक या असुरक्षित वेबसाइटों का उपयोग करना, खतरनाक फ़ाइलें डाउनलोड करना, या अविश्वसनीय प्लेटफ़ॉर्म पर संवेदनशील जानकारी साझा करना। यह उपयोगकर्ताओं के लिए मैलवेयर, फ़िशिंग, पहचान की चोरी (इमपर्सनेशन), और डेटा लीक जैसे खतरे पैदा करता है।

✓ क्या करें

- **सुरक्षित ब्राउज़र का उपयोग करें:** हमेशा अपडेट किए गए, सुरक्षित ब्राउज़र से ब्राउज़ करें और सुनिश्चित करें कि वेबसाइट HTTPS का उपयोग करती हैं।
- **एंटीवायरस इंस्टॉल करें:** विश्वसनीय एंटीवायरस सॉफ़्टवेयर से अपने डिवाइस को सुरक्षित रखें।
- **URL वेरिफाई करें:** संवेदनशील जानकारी दर्ज करने से पहले वेबसाइट लिंक की जांच करें।
- **फ़ायरवॉल सक्षम करें:** सुरक्षा की एक अतिरिक्त परत के लिए फ़ायरवॉल का उपयोग करें।

✕ क्या ना करें

- **अज्ञात लिंक पर क्लिक करने से बचें:** अनवेरिफाइड या संदिग्ध लिंक से दूर रहें।
- **सार्वजनिक Wi-Fi पर सतर्क रहें:** सुरक्षा के बिना असुरक्षित सार्वजनिक Wi-Fi का उपयोग न करें।
- **सार्वजनिक उपकरणों पर पासवर्ड न रखें:** शेयर्ड या सार्वजनिक कंप्यूटरों पर लॉगिन क्रेडेंशियल सेव करने से बचें।
- **असुरक्षित साइटों का उपयोग:** ब्राउज़र चेतावनियों को अनदेखा न करें और फ़्लैग की गई या असुरक्षित वेबसाइटों पर जाने से बचें।

रैंसमवेयर

रैंसमवेयर एक खतरनाक सॉफ़्टवेयर है जो पीड़ित की फ़ाइलों को लॉक कर देता है, जिससे वे इस्तेमाल नहीं की जा सकतीं। स्कैमर उन्हें अनलॉक करने के बदले फिरौती मांगते हैं। यह फ़िशिंग ईमेल, संक्रमित सॉफ़्टवेयर डाउनलोड और सुरक्षा खामियों के जरिए फैल सकता है। रैंसमवेयर से महत्वपूर्ण डेटा खो सकता है और बड़ा आर्थिक नुकसान हो सकता है।

✓ क्या करें

- **डेटा का बैकअप लें:** नुकसान को रोकने के लिए नियमित रूप से अपने डेटा का बैकअप लें।
- **कॉन्टेंट स्कैनिंग का उपयोग करें:** हानिकारक फ़ाइलों की पहचान करने के लिए समय पर कॉन्टेंट स्कैनिंग और फ़िल्टरिंग लागू करें।
- **सिस्टम अपडेट करें:** सुरक्षा खामियों को ठीक करने के लिए अपने सिस्टम और सॉफ्टवेयर को अप-टू-डेट रखें।
- **कर्मचारी प्रशिक्षण:** कर्मचारियों को फ़िशिंग और अन्य साइबर धोखाधड़ी की पहचान करने और उनसे बचने के तरीके सिखाएं।

× क्या ना करें

- **फिरौती का भुगतान न करें:** इससे डेटा वापस मिलने की कोई गारंटी नहीं होती और यह साइबर अपराधियों को और हमले करने के लिए बढ़ावा देता है।
- **व्यक्तिगत जानकारी की सुरक्षा करें:** अपरिचित स्रोतों को व्यक्तिगत जानकारी प्रदान न करें।
- **हमले को रोकें:** हमले को फैलने न दें। प्रभावित सिस्टम को सर्वर से तुरंत अलग करें।
- **हमले के दौरान बैकअप न चलाएं:** हमले के दौरान बैकअप न चलाएं, क्योंकि वे भी लॉक हो सकते हैं।

स्मार्टफोन स्कैम

स्मार्टफोन स्कैम बढ़ रहे हैं, जहाँ धोखेबाज नकली कॉल, खतरनाक ऐप्स और SIM से जुड़ी धोखाधड़ी के ज़रिये डेटा और पैसा चुराते हैं। वे खुद को किसी प्रतिष्ठित एजेंसी का प्रतिनिधि बताकर निजी जानकारी चुराने की कोशिश करते हैं। सतर्क रहें और सुरक्षित उपाय अपनाएँ।

✓ क्या करें

- **चुराए गए फोन की रिपोर्ट करें:** चोरी हुए फोन की तुरंत पुलिस और संचार साथी पोर्टल https://sancharsaathi.gov.in पर रिपोर्ट करें।
- **SIM पंजीकरण जाँचे:** अपने नाम पर पंजीकृत SIM की संख्या को नियमित रूप से जाँचे।
- **स्पैम कॉल की रिपोर्ट करें:** स्पूफिंग कॉल की रिपोर्ट करें और स्पैम कॉल को ब्लॉक करने के लिए DND सेवा का उपयोग करें।
- **केवल वेरिफाइड स्टोर का उपयोग करें:** Play Store या App Store जैसे आधिकारिक स्टोर से ही ऐप्स डाउनलोड करें।
- **IMEI नंबर का रिकॉर्ड रखें:** संचार साथी पोर्टल का उपयोग कर के अपने IMEI नंबर का रिकॉर्ड रखें।

× क्या ना करें

- **अज्ञात स्रोतों से बचें:** सोशल मीडिया ग्रुप्स या अनवेरिफाइड स्रोतों पर मिले ऐप्स डाउनलोड करने से बचें।
- **SIM सीमा जांचें:** सुनिश्चित करें कि आप अनुमत 9 SIM की सीमा से अधिक नहीं हैं (जम्मू और कश्मीर, असम, नार्थ ईस्ट के लिए 6)।
- **स्पैम कॉल को अनदेखा करें:** कभी भी स्पैम कॉल में भाग न लें या उनसे जुड़ें नहीं। उन्हें तुरंत ब्लॉक करें।
- **अनावश्यक SIM कनेक्शन हटाएं:** अपने नाम पर अनावश्यक SIM कनेक्शन न रखें।
- **WhatsApp सेटिंग बदलें:** स्कैम कॉल से बचने के लिए WhatsApp पर "साइलेंस अननोन कॉलर" का उपयोग करें।

साइबर अपराधों की शिकायत के लिए
www.cybercrime.gov.in
या **1930** पर कॉल करें

लेटेस्ट साइबर अपराधों की जानकारी के लिए
CyberDost को फॉलो करें