SAFER INTERNET INDIA

उपयोगकर्ता सुरक्षा पुस्तिका

उपयोगकर्ता सुरक्षा

फरवरी 2025

स्वीकृतियाँ

अतीश नंदी, बर्जेस मालू, ललनतिका अरविन्द, समृद्धि कुमार, सिवा भार्गवी नोरी, सृष्टि जोशी

लेखक की ओर से गठबंधन के सदस्यों को समर्थन एवं इनपुट प्रदान करने के लिए धन्यवाद।

अंदर क्या है

सामान्य स्कैम और फ्रॉड

हम सतर्क रहने और जागरूक रहने में मदद करने के लिए स्कैम करने वालों की विभिन्न रणनीतियों का विश्लेषण करते हैं।

सुरक्षित सर्फिंग के सुझाव

आज के इंटरनेट के दौर में सुरक्षित रहने के लिए क्या करें और क्या न करें

विश्वास और सुरक्षा के मूलभूत स्तंभ

हम ऑनलाइन भरोसा और सुरक्षा कायम करने के लिए चार मूलभूत स्तंभों पर चर्चा करते हैं।

उद्योग के सर्वोत्तम अभ्यास

हम ऐसी अग्रणी प्रौद्योगिकी कंपनियों के साथ सर्वोत्तम अभ्यास पर चर्चा करते हैं, जो इंटरनेट को हम सभी के लिए थोड़ा सुरक्षित बनाती हैं।

विषय-सूची

प्रिय पाठक

सेफ़र इंटरनेट इंडिया (SII) भारत की डिजिटल अर्थव्यवस्था के विभिन्न क्षेत्रों में फैली समान विचारधारा वाली कंपनियों का एक गठबंधन है।

SII ऑनलाइन फ़्रॉड, साइबर खतरों और डेटा उल्लंघनों के बढ़ते ख़तरों से निपटने के लिए एक तात्कालिक सामाजिक आवश्यकता को पूरा करने की दिशा में काम करता है। हम ऑनलाइन जाने वाले उपयोगकर्ताओं के भरोसे और सुरक्षा को मजबूत करने के लिए बहु-विषयक आवाज़ को एक ही मंच पर लाते हैं।

हमने यह पुस्तिका इसलिए लिखी है ताकि आप जैसे इंटरनेट उपयोगकर्ता अपने आप को ऑनलाइन फ़्रॉड और स्कैम से सुरक्षित कर सकें।

यह पुस्तिका इंटरनेट पर होने वाले सामान्य फ़्रॉड और स्कैम का विवरण प्रदान करती है। साथ ही, यह बताती है कि इंटरनेट पर उपयोगकर्ताओं को सुरक्षित रूप से काम करने एवं सुरक्षित तथा विश्वसनीय तरीके से डिजिटल व्यवसायों के साथ जुड़ने के लिए क्या करना चाहिए और क्या नहीं करना चाहिए। यह ऑनलाइन स्पेस को सुरक्षित बनाने के लिए व्यवसायों और नीति निर्माताओं द्वारा उठाए गए कदमों को भी मान्यता देती है।

पढ़ने के लिए धन्यवाद

सेफ़र इंटरनेट इंडिया

परिचय

डिजिटल क्षेत्र हमारे जीवन के हर पहलू को छूते हैं। भारत के 900 मिलियन+ इंटरनेट उपयोगकर्ता नियमित रूप से काम करने, सीखने और घरेलू आवश्यकताओं से लेकर लक्जरी सामान, मनोरंजन के लिए सब्सक्रिप्शन और यहां तक कि वित्तीय सेवाएँ भी खरीदने के लिए ऑनलाइन जाते हैं।

हालांकि, उपयोगकर्ताओं को इसे लेकर सावधान रहना चाहिए कि वे किसके साथ बातचीत करते हैं, और वे कहाँ से ऑनलाइन खरीदारी करते हैं। ऑनलाइन दुनिया में आपको ऐसे अनगिनत प्रस्ताव और डील्स मिलेंगी, जो सुनने में बहुत अच्छी लगती हैं। लेकिन क्या आपको पता है, भारतीयों ने 2024 के पहले नौ महीनों में ऑनलाइन स्कैम में लगभग ₹ 11,333 करोड़ रुपये गँवाए हैं!

दुर्भाग्य से, ऑनलाइन स्कैम्स बढ़ते जा रहे हैं, जबकि दूसरी तरफ़ कई भारतीयों में बुनियादी डिजिटल कौशल की कमी है। फ़्रॉड और स्कैमर अत्यधिक प्रतिकूल, अवसरवादी और अनुकूली हैं। भारत सरकार (GOI) की ओर से 2022-23 में हुए सर्वेक्षण से पता चलता है कि भारत के लगभग आधे इंटरनेट उपयोगकर्ताओं को यह नहीं पता होता कि ईमेल कैसे भेजना है, जबकि केवल 38 प्रतिशत लोग ऑनलाइन बैंकिंग लेनदेन कर सकते हैं। डिजिटल कौशल की बात करें तो ग्रामीण भारत शहरों से काफ़ी पीछे है। इसके अलावा, लैंगिक रूप से भी डिजीटल कौशल को लेकर काफ़ी असमानताए हैं। कुल मिला कर, स्कैम संपूर्ण समाज के लिए एक चुनौती हैं। कई भारतीयों पर ठगे जाने का ख़तरा बना रहता है और उन्हें खुद को ऑनलाइन सुरक्षित रखने के लिए कौशल और जागरूकता के साथ सशक्त बनने की ज़रूरत है।

भारत सरकार भारतीय इंटरनेट उपयोगकर्ताओं को ऑनलाइन स्कैम के खतरे से बचाने की आवश्यकता को पहचानती है। गृह मंत्रालय और इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय एक साथ भारतीय साइबर अपराध समन्वय केंद्र (I4C)) और भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-in) जैसे विशेष निकायों के साथ मिलकर फ़्रॉड और स्कैम की जांच और रोकथाम तथा संबंधित ऑनलाइन सुरक्षा मुद्दों को हल करने के लिए चौबीसों घंटे काम करते हैं। भारतीय रिजर्व बैंक (RBI) और भारतीय दूरसंचार नियामक प्राधिकरण (TRAI) जैसे नियामक भी भारतीयों की सुरक्षा के लिए प्रौद्योगिकी का इस्तेमाल कर रहे हैं, चाहे वह मनी लॉन्ड्रिंग में इस्तेमाल किए जाने वाले मूल अकाउंट का पता लगाने के लिए AI (आर्टफिशल इन्टेलिजन्स) प्रणाली हो या स्पैम/अप्रिय कॉलों को सीमित करने के लिए टेलीमार्केटर्स का वितरित खाता प्रौद्योगिकी (DLT) आधारित पंजीकरण हो, इसके अलावा वे अपने डोमेन में नए नियम भी पेश कर रहे हैं।

लेकिन ऑनलाइन सुरक्षा की समस्या को बड़े स्तर पर सुलझाने के लिए हम सभी को एक साथ आना होगा। उपयोगकर्ताओं को ऑनलाइन सुरक्षित रखने के लिए सभी को एक साथ मिल कर काम करना होगा। व्यवसाय भारत की समृद्ध डिजिटल अर्थव्यवस्था में प्रमुख भूमिका निभाते हैं और SII गठबंधन उपयोगकर्ताओं की सुरक्षा और डिजिटल सेवाओं में उनका विश्वास बनाने की अपनी ज़िम्मेदारी को पहचानता है।

मूल बातें

ऑनलाइन सुरक्षित रहना पहले से कहीं ज़्यादा ज़रूरी है। इस खंड में हम आपको कुछ बुनियादी शब्दों और अवधारणाओं से परिचित कराएँगे, ताकि आप डिजिटल स्पेस में बेहतर तरीके से नेविगेट कर सकें।

व्यक्तिगत जानकारी

व्यक्तिगत जानकारी वह विवरण है, जो यह बताता है कि आप कौन हैं। इसमें आपका नाम, पता, फोन नंबर, ईमेल, जन्म तिथि या बैंक विवरण जैसी चीजें शामिल हैं। स्कैमर अक्सर इसे चुराने की कोशिश करते हैं ताकि वे आप बन कर आपके खातों तक पहुंच प्राप्त कर सकें।

संवेदनशील व्यक्तिगत जानकारी

संवेदनशील व्यक्तिगत जानकारी के लिए अत्यधिक सुरक्षा की आवश्यकता होती है, क्योंकि यदि यह गलत हाथों में जाती है तो इसका दुरुपयोग किया जा सकता है। इसमें आपके पासवर्ड, बैंक खाता संख्या, क्रेडिट कार्ड विवरण, मेडिकल रिकॉर्ड, या सरकारी आईडी नंबर (जैसे आधार या पैन) जैसी चीजें शामिल हैं। अपनी पहचान और वित्त को सुरक्षित रखने के लिए इस जानकारी को सुरक्षित रखना बहुत महत्वपूर्ण है। इस तरह की जानकारी साझा करने को लेकर बहुत सावधान रहें।

फ़्रॉड

ऑनलाइन फ़्रॉड तब होता है जब कोई व्यक्ति इंटरनेट के माध्यम से अवैध रूप से पैसे या संवेदनशील जानकारी चुराने के लिए झूठ या धोखे का उपयोग करता है। इसमें अकाउंट्स को हैक करना, भुगतान विवरण चुराना या लोगों को ठगने के लिए नकली वेबसाइट बनाना जैसी चीजें शामिल हैं।

स्कैम

ऑनलाइन स्कैम तब होता है जब कोई व्यक्ति आपके पैसे, व्यक्तिगत जानकारी या संवेदनशील डेटा चुराने के इरादे से इंटरनेट पर आपके साथ ठगी करता है। स्कैम करने वाले अक्सर भरोसेमंद होने का दिखावा करते हैं, नकली सौदों की पेशकश करते हैं, ख़ुद को अधिकारियों के रूप में प्रस्तुत करते हैं या आपके साथ फ़्रॉड करने के लिए वास्तविक दिखने वाले संदेश भेजते हैं।

ऑनलाइन स्कैम एक प्रकार का ऑनलाइन फ्रॉड है, लेकिन सभी फ्रॉड स्कैम नहीं होते। स्कैम में अक्सर लोगों को स्वेच्छा से पैसा या जानकारी देने के लिए राज़ी किया जाता है (जैसे, नकली पुरस्कार या नौकरी प्रस्ताव)। दूसरी ओर, ऑनलाइन फ्रॉड में पहचान की चोरी या हैकिंग जैसी क्रियाएँ शामिल हो सकती हैं, जिसमें पीड़ित को एहसास भी नहीं होता कि उनका नुकसान हो चुका है।

संक्षेप में, स्कैम करने वाले लोगों के साथ ठगी करते हैं जबकि फ्रॉड करने वाले व्यापक तरीकों का इस्तेमाल करते हैं, जैसे जानकारी चोरी करना या जानकारी का दुरुपयोग करना। इसलिए, उपयोगकर्ताओं को न केवल उस समय सतर्क रहना चाहिए जब वे लोगों के साथ ऑनलाइन बातचीत करते हैं, बल्कि तब भी सतर्क रहना चाहिए जब वे वेबसाइटों पर जाते हैं या ऐप्स डाउनलोड करते हैं।

हैक

हैकिंग उसे कहा जाता है, जब कोई व्यक्ति जानकारी चुराने के लिए अनुमति के बिना कंप्यूटर, खाते या नेटवर्क में घुसता है, नुकसान का कारण बनता है या उसे अपने नियंत्रण में ले लेता है। हैकर अक्सर कमजोरियाँ खोजने और ऐक्सेस प्राप्त करने के लिए विशेष उपकरण या तकनीकों का उपयोग करते हैं।

फिशिंग

फिशिंग वो तकनीक है जिसका उपयोग स्कैमर आपकी व्यक्तिगत जानकारी को चुराने के लिए करते हैं, जैसे पासवर्ड, बैंक विवरण या क्रेडिट कार्ड नंबर। वे आमतौर पर ऐसे किसी व्यक्ति का रूप लेते हैं जिस पर आप भरोसा करते हैं, जैसे कि आपका बैंक, कोई कंपनी या सरकारी एजेंसी, जो आपको नकली लिंक पर क्लिक करने या संवेदनशील जानकारी साझा करने के लिए कहती है।

फिशिंग हमले विभिन्न तरीकों से हो सकते हैं। SMS / मैसेजिंग ऐप्स के जरिए किए गए हमलों को स्मिशिंग हमला कहा जाता है, जबकि जो हमले फोन कॉल्स के जरिए किए जाते हैं उन्हें विशिंग (वॉइस-फिशिंग) हमला कहा जाता है।

उदाहरण:

आपको एक ईमेल मिलता है जो कहता है:

"आपका बैंक खाता बंद कर दिया गया है। अपनी पहचान सत्यापित करने और अपना खाता अनलॉक करने के लिए यहां क्लिक करें।

यह लिंक आपको एक नकली वेबसाइट पर ले जाता है, जो आपके बैंक की साइट की तरह दिखती है। लेकिन जब आप इस पर अपना विवरण दर्ज करते हैं, तो यह विवरण सीधे स्कैमर्स तक पहुंच जाता है।

फिशिंग ईमेल का एक और उदाहरण यह है कि स्कैमर किसी व्यक्ति की कंपनी में उसका सहकर्मी होने का दिखावा करता है और एक ईमेल भेजता है जिसमें पैसे की मांग की जाती है। ऐसे मामलों में, कृपया बिल्कुल भी पैसा न भेजें और सहकर्मी की पहचान सत्यापित करने के लिए उसे (चाहे वह आपका बॉस ही क्यों न हो) कॉल करें। एक और महत्वपूर्ण टिप यह है कि उसका ईमेल सत्यापित किया जाए। आमतौर पर, यह ईमेल आपकी कंपनी के नाम पर नहीं होती है या यह आपके सहकर्मी के आधिकारिक ईमेल से मेल नहीं खाती होगी।

मालवेयर

मालवेयर हानिकारक सॉफ़्टवेयर है जो आपकी अनुमति के बिना आपके कंप्यूटर, फोन या अन्य उपकरणों को नुकसान पहुँचाने, चोरी करने या नियंत्रण करने के लिए डिज़ाइन किया गया है। इसे नकली ऐप्स, ईमेल अटैचमेंट (ईमेल के साथ होने वाली फाइल) या वेबसाइट में छिपाया जा सकता है। यह आपकी जानकारी चोरी करने या आपके डिवाइस को धीमा करने जैसी समस्याओं का कारण बन सकता है।

आर्टीफ़ीशियल इन्टेलिजेंस

आर्टीफ़ीशियल इन्टेलिजेंस एक ऐसी तकनीक है जो डेटा का विश्लेषण कर सकती है, मानव व्यवहार की नकल कर सकती है और वास्तविक सामग्री बना सकती है, जैसे मैसेज या आवाजें। स्कैमर्स आर्टीफ़ीशियल इन्टेलिजन्स का उपयोग अपनी चालों को और अधिक विश्वासनीय बनाने के लिए कर सकते हैं, जैसे कि नकली मैसेज बनाना जो वास्तविक लगते हैं, किसी की आवाज की नकल करना, या लोगों को पैसे या व्यक्तिगत जानकारी साझा करने के लिए धोखा देने के लिए व्यक्तिगत ईमेल भेजना। आर्टफिशल इन्टेलिजन्स स्कैमर्स को पीड़ितको अधिक प्रभावी तरीके से लक्षित करने में मदद करता है और उनके स्कैम्स को पहचानना अधिक कठिन बना देता है।

स्पैम

स्पैम अवांछित या जंक संचार है। यह आमतौर पर फोन कॉल, ईमेल, टेक्स्ट, सोशल मीडिया के माध्यम से भेजा जाता है। इसका अक्सर चीजों का विज्ञापन करने के लिए उपयोग किया जाता है, लेकिन कभी-कभी इसका उपयोग आपकी जानकारी या पैसे चुराने के लिए भी किया जा सकता है।

उदाहरण:

"बधाई हो! आपने $1,000 का उपहार कार्ड जीता है! अपना पुरस्कार क्लेम करने के लिए यहाँ क्लिक करें।"

यह ईमेल आमतौर पर नकली होता है, और लिंक पर क्लिक करने से आपके साथ स्कैम हो सकता है या यह आपके डिवाइस को हानिकारक सॉफ़्टवेयर के साथ संक्रमित कर सकता है।

स्पैम अधिक प्रचलित होता जा रहा है और यह ऐसे संचार से मिलता-जुलता हो सकता है जो आपके व्यवसाय, पेशे या वोकेशन के लिए प्रासंगिक हो सकता है।

निम्नलिखित आपके पेशे के अनुरूप प्रचलित स्पैम का एक उदाहरण हो सकता है:

यह ईमेल पेशेवर और आपके काम के लिए प्रासंगिक नज़र आता है, लेकिन यह लिंक किसी फ़िशिंग साइट पर ले जा सकती है और अटैचमेंट में मालवेयर हो सकता है। इस तरह का स्पैम संदेश वैध और व्यक्तिगत लगता है, लेकिन इसे पेशेवरों को गुमराह करने के लिए डिज़ाइन किया जाता है।

सामान्य फ्रॉड और स्कैम

स्कैम # 1 आर्टिफिशियल इंटेलिजेंस स्कैम

यह क्या होता है?

एआई वॉयस स्कैम में स्कैमर आपको गुमराह करने के लिए आपके किसी परिचित, जैसे कि परिवार के कोई सदस्य या बॉस की आवाज़ को कॉपी करने के लिए आर्टिफिशियल इंटेलिजेंस का उपयोग करते हैं। वे आपको कॉल कर के पैसे मांग सकते हैं, या किसी आपातकालीन स्थिति में होने का नाटक कर सकते हैं, या जानकारी चुराने के लिए नकली निर्देश दे सकते हैं। चूंकि आवाज़ बहुत वास्तविक लगती है, इसलिए वह आपको गुमराह कर सकते हैं और उन्हें पहचानना मुश्किल हो सकता है।

यह कैसे काम करता है?

स्कैमर सोशल मीडिया, वीडियो या वॉयसमेल से लोगों की आवाज़ की रिकॉर्डिंग ढूंढते हैं। फिर वे एआइ टूल का उपयोग करके उस व्यक्ति की आवाज़ की नकल करते हैं ताकि वह असली और प्राकृतिक लगे।

स्कैमर नकली आवाज़ का उपयोग करके आपको कॉल करते हैं और कोई ऐसा व्यक्ति होने का दिखावा करते हैं जिसे आप एक दोस्त, परिवार के सदस्य या बॉस की तरह जानते हैं। वे तनाव पैदा करते हैं और ऐसा दिखाते हैं जैसे वे किसी आपात स्थिति में हैं और पैसे, उपहार कार्ड या संवेदनशील जानकारी की माँग करते हैं।

यदि आप उनके झांसे में आते हैं तो वे इसका उपयोग आपके पैसे या व्यक्तिगत जानकारी चुराने के लिए करते हैं।

- **तात्कालिकता से सावधान रहें:** स्कैमर अक्सर आपके ऊपर जल्दी करने का दबाव डालते हैं। कुछ भी करने से पहले कुछ समय के लिए सोचें और उनकी बात को सत्यापित करें।
- **कॉल करने वाले को सत्यापित करें:** यदि कोई पैसे या संवेदनशील व्यक्तिगत जानकारी मांगता है, तो उनकी पहचान सत्यापित करने के लिए उनके नंबर पर कॉल-बैक करें।
- **व्यक्तिगत प्रश्न पूछें:** कुछ सवाल केवल असली व्यक्ति को पता होंगे, जो स्कैमर को पकड़ने में आपकी मदद करेगा।
- **कोई सुरक्षित शब्द या कोड बनाएँ:** आपात स्थितियों के लिए, परिवार या कार्यस्थल पर एक "सुरक्षित शब्द" सेट करें, जिसके बारे में केवल विश्वसनीय लोगों को पता होगा।

स्कैम # 2 डेटिंग एप स्कैम

यह क्या होता है?

यह स्कैम तब होता है जब किसी डेटिंग ऐप पर किसी व्यक्ति का मैच होता है और उसे एक रेस्तरां या कैफे में मिलने के लिए आमंत्रित किया जाता है, जो स्कैम का एक हिस्सा होता है। यह स्कैमर महंगी चीज़ें ऑर्डर करता है, कभी-कभी ऐसी चीज़ें भी ऑर्डर करता है, जो मेनू पर भी नहीं होती हैं, फिर वहाँ से निकलने का बहाना बनाता है। वह पीड़ित को एक बड़े बिल के साथ छोड़ जाता है। फिर रेस्तरां का स्टाफ़ या बाउंसर उसे भुगतान करने के लिए मजबूर करते हैं।

यह कैसे काम करता है?

डेट प्लान करना: स्कैमर डेट प्लान करता है और पीड़ित को किसी विशेष कैफे में मिलने के लिए कहता है। कभी-कभी स्कैमर किसी इलाके का प्रस्ताव दे सकता है और पीड़ित से मेट्रो स्टेशन पर मिलने के लिए कह सकता है। वह कहेगा कि वे पास के किसी कैफे में चलेंगे।

कैफे में: अंदर जाते ही, स्कैमर भोजन या ड्रिंक ऑर्डर करेगा, कभी-कभी ऐसी चीज भी जो मेनू पर नहीं होंगी। वो एक आपातकालीन स्थिति का बहाना बना कर वहाँ से निकल सकता है।

एक बड़ा बिल: बिल उम्मीद से बहुत अधिक होता है - अक्सर सामान्य से कई गुना ज़्यादा कीमत होती है। अगर पीड़ित मना करता है, तो कैफे का स्टाफ या बाउंसर उसे धमकी देते हैं, जिससे उसे भुगतान करने के लिए मजबूर होना पड़ता है।

स्कैम का ऑपरेशन: इस स्कैम में एक समूह शामिल होता है। इसमें कैफे का मालिक, स्टाफ जिसमें मैनेजर्स या बाउंसर भी शामिल होते हैं, और वह व्यक्ति शामिल होता है जो डेटिंग ऐप पर पीड़ित से मिलता है। प्रत्येक व्यक्ति को उस बिल में से एक हिस्सा मिलता है।

अधिकांश पीड़ित इस स्कैम की रिपोर्ट नहीं करते क्योंकि उन्हें बेइज़्ज़ती का डर होता है या वे अपने परिवार को यह बताने से डरते हैं कि वे एक डेटिंग ऐप का उपयोग कर रहे थे।

अगर यह आपके साथ होता है, तो कृपया इसे अपने स्थानीय पुलिस स्टेशन में रिपोर्ट करें या www.cybercrime.gov.in पर जाएँ।

- **मीटिंग स्थल को लेकर सतर्क रहें:** जब तक आप क्षेत्र से परिचित न हों, तब तक दूसरे व्यक्ति द्वारा चुने गए स्थानों पर मीटिंग से बचें।
- **दूसरे व्यक्ति द्वारा सुझाए गए कैफे पर शोध करें:** कैफे को ऑनलाइन देखें और रीव्यू की जांच करके पता लगाएँ कि क्या यह एक वैध स्थान है। कई स्रोतों से रीव्यू क्रॉस-वेरिफ़ाई करें। कभी-कभी स्कैमर्स उसे वैध बनाने के लिए किसी जगह पर नकली रीव्यू भी डालते हैं।
- **अपनी प्रवृत्ति पर भरोसा करें:** यदि कुछ अजीब महसूस होता है - जैसे कि व्यक्ति किसी स्थान को लेकर अत्यधिक आग्रह करता है या आपके रेस्तरां में बैठने के बात अचानक से शांत और दूर हो जाता है - तो सावधान रहें।
- **संदिग्ध व्यवहार की रिपोर्ट करें:** अगर आपको फाउल प्ले का संदेह है, तो दूसरों को स्कैम से बचाने के लिए पुलिस या डेटिंग ऐप को सूचित करें।

स्कैम # 3 डिजिटल अरेस्ट

यह क्या होता है?

डिजिटल अरेस्ट स्कैम में स्कैमर पुलिस, सरकारी अधिकारी जैसे सीमा शुल्क अधिकारी के ऑनलाइन या फोन पर होने का दिखावा करते हैं। वे दावा करते हैं कि आप कानूनी परेशानी में हैं और "गिरफ्तारी से बचने" के लिए तुरंत पैसे देने की मांग करते हैं। वे अक्सर पीड़ित से तुरंत भुगतान हासिल करने के लिए डर और तात्कालिकता का उपयोग करते हैं।

यह कैसे काम करता है?

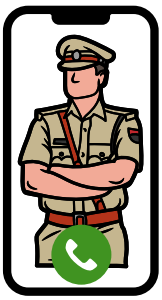
नकली कॉल या मैसेज: आपको कॉल, ईमेल या संदेश प्राप्त होता है जिसमें यह दावा किया जाता है कि आपने कानून तोड़ा है और आपको जुर्माना भरना होगा या गिरफ्तारी का सामना करना पड़ेगा। उदाहरण के लिए, एक पीड़ित को एक अंतरराष्ट्रीय नंबर से कॉल प्राप्त हुई, जिसमें यह कहा गया कि एक पार्सल की निर्धारित डिलीवरी रद्द कर दी गई है।

धमकी और दबाव: स्कैमर कहता है कि यदि आप तुरंत भुगतान नहीं करते हैं, तो आपको जेल जैसे गंभीर परिणामों का सामना करना पड़ सकता है। उपरोक्त उदाहरण में, कॉलर ने पीड़ित से कहा कि वे सपोर्ट हासिल करने के लिए "0" दबाए। ऐसा करते ही, ग्राहक सहायता प्रतिनिधि के रूप में प्रस्तुत होने वाला कोई व्यक्ति कॉल पर आया और दावा किया कि उनके नाम से जुड़े एक पैकेज में अवैध पदार्थ थे और चीन भेजा गया था। प्रतिनिधि ने आगे दावा किया कि उसके खिलाफ एक गिरफ्तारी वारंट जारी किया गया था। फिर नकली पुलिस अधिकारी और जांचकर्ता वीडियो कॉल में शामिल हो गए।

स्कैमर्स आपको यह समझाने के लिए तमाम कोशिशें करेंगे कि वे असली पुलिस हैं। वे आपको नकली लेटरहेड और आईडी कार्ड दिखाएंगे। यहां तक कि वे नकली पुलिस स्टेशन भी बनाते हैं और वीडियो कॉल करते समय पुलिस की तरह कपड़े पहनते हैं।

अलगाव और तात्कालिकता: स्कैमर्स कोशिश करेंगे कि वे आपको खुद को अलग-थलग करने के लिए मना लें। वे आपको एक दूरस्थ स्थान की यात्रा करने या अपने आप को एक कमरे में लॉक करने और पदचिह्न हटाने के लिए कहेंगे। वे आपको अन्य कॉल लेने से बचने के लिए भी कहेंगे।

निरंतर भुगतान की माँग: वे आमतौर पर कई खातों में लगातार पैसे की मांग करते हैं, ताकि पैसा ट्रेस न किया जा सके।



उदाहरण:

आपको एक कॉल आएगी जिसमें कहा जाएगा: **"साइबर क्राइम यूनिट से अधिकारी एक्स बात कर रहा है। हमने आपके खाते से जुड़ी अवैध गतिविधियों का पता लगाया है। आपको गिरफ्तारी से बचने के लिए अभी ₹10,000 का भुगतान करना होगा। इसका पालन करने में विफल रहने पर आपको गिरफ्तार किया जाएगा।"**

- **शांत रहें:** पुलिस भारत में फोन कॉल या वीडियो कॉल पर गिरफ्तारी नहीं कर सकती है। भले ही स्कैमर आपके पते, नाम आदि के बारे में व्यक्तिगत विवरण जानने का दावा करता है, फिर भी कॉल को तुरंत डिस्कनेक्ट कर दें और संवाद को बंद कर दें।

- **उसका दावा सत्यापित करें:** अपने आधिकारिक फोन नंबर या वेबसाइट का उपयोग करके सीधे संबंधित संगठन से संपर्क करें, चाहे वह पुलिस हो या अन्य सरकारी अधिकारी अथवा संगठन जिनके ग्राहक सेवा प्रतिनिधि ने आपको कॉल किया हो।

- **अलगाव को मना करें:** कभी भी खुद को अलग न होने दें, चाहे वो कितनी भी कोशिश करे। दोस्तों या परिवार की कॉल उठाएँ। कॉल काटें और किसी ऐसे व्यक्ति से बात करें जिस पर आप बेहद भरोसा करते हैं।

- **भुगतान न करें:** वास्तविक कानूनी अधिकारी कभी फोन पर पैसे नहीं मांगेंगे। ऐसी सभी मांगों को अस्वीकार करें।

- **अजीब चीज़ें तलाशें:** अंतरराष्ट्रीय या घरेलू नंबरों से कॉल जिनसे आप परिचित नहीं हैं। अपने नाम, बैंक खाते या आईडी जैसे व्यक्तिगत विवरणों को "सत्यापित" करने के लिए कहना।

- **सावधान रहें:** अज्ञात या संदेहास्पद नंबरों से फोन कॉल का जवाब देते समय सतर्क रहें, जैसे कि विदेशों से आने वाली कॉल्स।

स्कैम # 4 नकली निवेश/ट्रेडिंग ऐप स्कैम

यह क्या होता है?

नकली ट्रेडिंग ऐप स्कैम में निवेशकों को ठगने के लिए डिज़ाइन किए गए फ्रॉड ट्रेडिंग ऐप्लिकेशन का निर्माण और प्रचार शामिल है। ये एप्स अक्सर उच्च रिटर्न और कम जोखिम का वादा करते हैं। यह आपको अपने पैसे निवेश करने के लिए लुभाते हैं। हालाँकि, जब आप इन नकली ऐप में पैसा जमा करते हैं, तो आप कई तरह के ठगी भरे अभ्यासों का सामना कर सकते हैं।

यह कैसे काम करता है?

नकली निवेश ऐप्स के लिए विज्ञापन और प्रचार: स्कैमर भ्रामक विज्ञापनों का उपयोग करते हैं ताकि पीड़ितों को असामान्य रूप से उच्च वित्तीय लाभ का वादा करके आकर्षित किया जा सके। अक्सर, पीड़ितों को व्हाट्सएप ग्रुप्स में भी जोड़ा जाता है, जिनके नाम वैध लगते हैं जैसे "ICICI IR टीम", जिससे पीड़ित को यह लगता है कि वे लाइसेंस प्राप्त वित्तीय संस्थाओं से जुड़े हैं। स्कैमर इन ग्रुप्स का उपयोग आमतौर पर सफलता की फ़र्जी कहानियाँ साझा करने के लिए करते हैं, ताकि पीड़ित का विश्वास जीता जा सके।

नकली ऐप्स डाउनलोड करने और निवेश करने के निर्देश: पीड़ित को फर्जी ऐप्स डाउनलोड करने के लिए कहा जाता है जो वास्तविक निवेश अवसरों की पेशकश करने का दावा करते हैं। ये ऐप्स, जैसे 'IC ORGAN MAX' और 'Techstars.shop', प्रसिद्ध स्टॉक्स और वित्तीय उपकरणों के नाम दिखाते हैं, ताकि उपयोगकर्ताओं को यह विश्वास दिलाया जा सके कि वे वैध हैं।
ऐप को वास्तविक दिखाने के लिए डिज़ाइन किया जाता है, जिसमें नकली चार्ट्स, खाते का बैलेंस और मुनाफे के बैंक स्टेटमेंट होते हैं, जो यह दर्शाते हैं कि आपकी निवेश राशि बढ़ रही है।

उच्च मुनाफे का झूठा प्रदर्शन: जब पीड़ित नकली ऐप्स इंस्टॉल करते हैं और अपना पैसा निवेश करते हैं, तो वे पहले अपने डैशबोर्ड पर अच्छा मुनाफ़ा देखकर उत्साहित होते हैं, जो उन्हें अधिक निवेश करने के लिए प्रेरित करता है। हालांकि, ये मुनाफे नकली आंकड़े होते हैं। जब पीड़ित अपना पैसा निकालने की कोशिश करते हैं, तो उनसे अतिरिक्त शुल्क जैसे वैधानिक कर या ब्रोकर फीस अदा करने के लिए कहा जाता है, ताकि स्कैमर उनसे और भी पैसे निकाल सकें।

भ्रामक अभ्यास

लॉक किए गए फंड्स: आप अपना पैसा नहीं निकाल पाते हैं।

फीस की मांग: ऐप आपको अपनी राशि ऐक्सेस करने से पहले अतिरिक्त "फीस" या "कर" का भुगतान करने के लिए कहता है।

गायब होना: स्कैमर्स ऐप को पूरी तरह से बंद कर के आपका पैसा लेकर गायब हो सकते हैं।

फ़र्जी कस्टमर सपोर्ट: मदद के लिए संपर्क करने पर आपको फ़र्जी कस्टमर सपोर्ट मिल सकता है, जो आप पर अधिक धन जमा करने के लिए दबाव डालता है या आपको टाल देता है।

गायब होने वाले स्कैमर्स: जब स्कैम का खुलासा हो जाता है, तो ऐप हटा दिया जाता है और स्कैमर्स गायब हो जाते हैं, जिससे पीड़ित के पास अपना पैसा वापस प्राप्त करने का कोई रास्ता नहीं बचता।

- अवांछित/अप्रत्याशित मैसेजों से सावधान रहें, जिन से आपकी ऑनलाइन निवेश के माध्यम से त्वरित धन की पेशकश करने को लेकर कोई बात नहीं हुई है।
- अवास्तविक रिटर्न का वादा करने वाले निवेश अवसरों से बचें।
- आधिकारिक वेबसाइटों या ऐप्स के माध्यम से निवेश प्लेटफार्म की वैधता को सत्यापित करें। उदाहरण के लिए, यदि वे कहते हैं कि वे किसी ख़ास बैंक से संबद्ध हैं, जैसे कि ICICI, तो ICICI के ग्राहक सहायता को कॉल करें या आधिकारिक वेबसाइट पर जाँचें कि यह सच है।
- विशेष रूप से मैसेजिंग ऐप पर, लॉगिन क्रेडेंशियल्स, व्यक्तिगत या वित्तीय जानकारी को अजनबियों के साथ साझा न करें।
- अपरिचित संपर्क के अनुरोध पर अज्ञात ऐप या फ़ाइलों को डाउनलोड करने से बचें।

स्कैम # 5 नकली नौकरी प्रस्ताव स्कैम

यह क्या होता है?

नकली नौकरी का प्रस्ताव स्कैम तब होता है, जब स्कैमर आपको नौकरी देने का दिखावा करते हैं ताकि वे आपसे पैसा या व्यक्तिगत जानकारी प्राप्त कर सकें। ये स्कैमर अक्सर नौकरियों की खोज करने वाले लोगों को लक्षित करते हैं, उच्च वेतन, आसान काम या लाभ का वादा करके उन्हें फ़ुसलाते हैं।

यह कैसे काम करता है?

आकर्षक नौकरी पोस्ट: यह स्कैमर वेबसाइट, सोशल मीडिया पर या ईमेल/मैसेज के जरिए नकली नौकरी के विज्ञापन बनाते हैं। कभी-कभी, स्कैमर खुद को कंसल्टेंसी के रूप में पेश करते हैं, जो आपको एक प्रतिष्ठित कंपनी में नौकरी की गारंटी देते हैं।

तेज चयन प्रक्रिया: वे बताते हैं कि आप नौकरी के लिए "चयनित" हो गए हैं। वे अक्सर बिना साक्षात्कार या स्क्रीनिंग के आपका चयन कर लेते हैं।

भुगतान या व्यक्तिगत जानकारी की मांग: आपसे प्रशिक्षण, पंजीकरण, काम के सामग्री या वीजा प्रोसेसिंग (यदि यह अंतरराष्ट्रीय नौकरी है) के लिए फीस देने को कहा जाता है।

नकली दस्तावेज़ या लिंक: वे नकली ऑफर लेटर, अनुबंध भेज सकते हैं या आपको फर्जी वेबसाइटों पर ले जाकर वैध दिखाने की कोशिश कर सकते हैं।

गायब होना: जब वे पैसे या आपकी व्यक्तिगत जानकारी इकट्ठा कर लेते हैं, तो स्कैमर गायब हो जाते हैं और नौकरी भी नहीं मिलती है।

नकली नौकरी स्कैम के उदाहरण

नकली नौकरी वाले स्कैम कई प्रकार के होते हैं

- **वर्क फ्रॉम होम नौकरी स्कैम**
- **नौकरी प्लेसमेंट सेवा स्कैम**
- **नैनी, केयरगिवर, और वर्चुअल पर्सनल असिस्टेंट नौकरी स्कैम्स**

वर्क फ्रॉम होम नौकरी स्कैम

स्कैमर ऐसे काम ऑफर करते हैं, जहाँ आप बिना ज्यादा समय और मेहनत के घर से काम करके महीनों में लाखों रुपये कमा सकते हैं।

वर्क फ्रॉम होम नौकरी के सामान्य स्कैम में री-शिपिंग स्कैम्स और मर्चेंडाइज री-सैलिंग स्कैम्स शामिल हैं।

री-शिपिंग स्कैम:
स्कैमर नकली नौकरियों जैसे गुणवत्ता नियंत्रण प्रबंधक या वर्चुअल असिस्टेंट का विज्ञापन डालते हैं। "हायर" करने के बाद, आपका काम महंगे सामानों को प्राप्त करना, फिर से पैक करना और भेजना होता है, जो अक्सर चुराए गए क्रेडिट कार्ड से खरीदे जाते हैं। वेतन कभी नहीं मिलता और कंपनी भी गायब हो जाती है, जिससे आप अपराध में शामिल हो जाते हैं। अगर आपने "भुगतान" के लिए व्यक्तिगत विवरण दिए हैं, तो आपकी पहचान की चोरी भी हो सकती है।

मर्चेंडाइज री-सैलिंग स्कैम्स:
स्कैमर्स एक नौकरी का वादा करते हैं जिसमें आप लग्जरी प्रोडक्ट्स को मुनाफे में रीसैल करते हैं। जब आप सामानों के लिए भुगतान करते हैं, तो पैकेज कभी नहीं आता या उसमें बेकार सामान होता है।

नैनी, केयरगिवर, और वर्चुअल पर्सनल असिस्टेंट नौकरी स्कैम्स

स्कैमर नौकरी साइट्स पर नैनी, केयरगिवर, और वर्चुअल असिस्टेंट के लिए नकली नौकरी के विज्ञापन पोस्ट करते हैं। या वे आपको ऐसे ईमेल भेज सकते हैं जो इस तरह दिखते हैं जैसे वे आपकी कम्यूनिटी से किसी व्यक्ति द्वारा भेजे गए हों। यह मैसेज आपके कॉलेज या विश्वविद्यालय जैसे किसी संगठन से भी आ सकता है जिसे आप जानते हैं।

यदि आप आवेदन करते हैं, तो आपको नियुक्त करने वाला व्यक्ति आपको एक चेक भेज सकता है। वे आपको कहेंगे कि आप चेक जमा करें, अपनी सेवाओं के लिए पैसा रखें और बाकी को किसी और को भेज दें।

यह एक स्कैम है। एक वैध नियोक्ता कभी भी आपसे ऐसा नहीं कहेगा। चेक नकली है और वह बाउंस हो जाएगा और बैंक आपसे नकली चेक की पूरी राशि वापस लेने को कहेगा, जबकि स्कैमर आपके द्वारा भेजी गई असली राशि को रख लेगा।

नौकरी प्लेसमेंट सेवा स्कैम

स्कैमर एक ऐसी कंसल्टेंसी के रूप में आपसे संपर्क करेंगे जो आपको एक बड़ी कंपनी में नौकरी पाने में मदद कर सकती है। वे आपको साक्षात्कार के लिए बुलाएंगे। जब आप वहां पहुंचेंगे, तो प्रवेश द्वार पर कुछ मोटे-तगड़े आदमी खड़े मिल सकते हैं। स्कैमर कंसल्टेंट के रूप में पेश आएंगे और आपकी योग्यताओं के बारे में कुछ सामान्य सवाल पूछेंगे। वे आपको पहले बड़े मल्टी-नेशनल कंपनियों में रखे गए लोगों की नकली तस्वीरें भी दिखा सकते हैं। इसके बाद, वे आपसे पैसे की मांग करेंगे और मोटे-तगड़े आदमी आपको भुगतान करने के लिए मजबूर कर सकते हैं।

- कोई भी संगठन/कंपनी कभी भी उनके साथ काम करने के लिए आपसे पैसे नहीं मांगती।
- स्पैम/जंक ईमेल्स या मैसेजों से भेजे गए नौकरी के प्रस्तावों को अनदेखा करें।
- यदि आपको ऐसा प्रस्ताव मिलता है जिसमें चेक जमा करने और फिर कुछ पैसे किसी कारण से उपयोग करने को कहा जाए, तो यह एक स्कैम है। इससे दूर रहें।
- प्लेसमेंट फर्म उम्मीदवारों से फीस नहीं मांगतीं। कंपनियां उन्हें नौकरी के लायक उम्मीदवार खोजने के लिए फीस देती हैं। अगर कोई प्लेसमेंट फर्म आप से फीस मांगती है — खासकर अग्रिम भुगतान करने के लिए — तो इससे दूर रहें। आप शायद स्कैम का सामना कर रहे हैं।
- यदि कोई आपको नौकरी का प्रस्ताव देता है और कहता है कि आप कम समय में कम मेहनत के साथ बहुत पैसा कमा सकते हैं, तो यह लगभग निश्चित रूप से एक स्कैम है।
- कंपनी की वेबसाइट, समीक्षाएँ और आधिकारिक संपर्क विवरण जांचें।
- उन कंपनियों के प्रस्तावों से बचें जिनकी ऑनलाइन उपस्थिति नहीं है या जिनके विवरण संदिग्ध हैं।
- संवेदनशील जानकारी जैसे आपका बैंक खाता, आधार या पैन कंपनी को सत्यापित किए बिना साझा न करें।

स्कैम # 6 नकली लिंक / QR कोड स्कैम

यह क्या होता है?

नकली लिंक / QR कोड स्कैम आपको एक हानिकारक लिंक पर क्लिक करने या फर्जी QR कोड को स्कैन करने के लिए कहते हैं। ये स्कैम व्यक्तिगत जानकारी, भुगतान विवरण चुराने या आपके डिवाइस पर हानिकारक सॉफ़्टवेयर इंस्टॉल करने के लिए डिज़ाइन किए गए होते हैं।

यह कैसे काम करता है?

नकली लिंक: स्कैमर ईमेल, मैसेज या सोशल मीडिया के माध्यम से लिंक भेजते हैं, जिसमें वे कुछ आकर्षक ऑफर (जैसे छूट, पुरस्कार, या तात्कालिक अपडेट्स) का दावा करते हैं। लिंक पर क्लिक करने से आपको एक नकली वेबसाइट पर ले जाया जाता है, जो वैध दिखती है लेकिन आपकी जानकारी चुराने के लिए डिज़ाइन की गई होती है।

फर्जी QR कोड: स्कैमर ऐसे QR कोड बनाते हैं जो फिशिंग वेबसाइट्स पर ले जाते हैं या हानिकारक क्रियाएँ शुरू करते हैं (जैसे मालवेयर इंस्टॉल करना)। ये कोड डिजिटल रूप से भेजे जा सकते हैं या भौतिक पोस्टर या विज्ञापनों पर लगाए जा सकते हैं।

कभी-कभी, स्कैमर्स एक वैध विज्ञापन लेते हैं और QR कोड को नकली कोड से बदल देते हैं, ताकि लोग यह सोचें कि वे वैध हैं।

नकली लिंक / QR कोड स्कैम के उदाहरण

- एक टेक्स्ट मैसेज आता है जिसमें कहा जाता है कि आपकी पैकेज डिलीवरी में देरी हो गई है; लिंक आपको भुगतान विवरण मांगने वाली साइट पर भेजता है।
- स्कैमर नकली वेबसाइट के लिंक भेजते हैं, जो वैध संस्थाओं जैसे बैंकों की साइट्स की नकल करती हैं और आपसे अपनी KYC विवरण अपडेट करने के लिए कहती हैं।
- स्कैमर्स नकली भुगतान लिंक या QR कोड भी प्रसारित कर सकते हैं, ताकि वे आपको अपने क्रेडिट कार्ड विवरण या UPI पिन भरने के लिए कह सकें।
- एक पोस्टर पर एक QR कोड छूट का प्रस्ताव देता है, लेकिन यह एक फिशिंग साइट पर ले जाता है।

- यदि आप किसी अप्रत्याशित स्थान पर QR कोड देखते हैं, तो उसे खोलने से पहले URL की जांच करें। यदि यह URL आप पहचानते हैं, तो सुनिश्चित करें कि कहीं वे नकली तो नहीं है — गलत वर्तनी या बदला हुआ अक्षर देखें।
- कभी भी उस ईमेल या टेक्स्ट मैसेज में दिए गए QR कोड को स्कैन न करें, जिसे आपके पास नहीं आना था। यदि वह आपसे तुरंत क्रिया करने के लिए कह रहा हो तो अवश्यक रूप से ध्यान दें। अगर आपको लगता है मैसेज वैध है, तो कंपनी से संपर्क करने के लिए उस फोन नंबर या वेबसाइट का उपयोग करें, जो वाकई में असली है और आपने सत्यापित की है।
- अनजान स्रोतों से भुगतान लिंक पर क्लिक न करें।
- QR कोड पर भुगतान करते समय हमेशा इच्छित प्राप्तकर्ता का नाम सत्यापित करें।
- जब आपको KYC के लिए पूछा जाए, तो KYC का उद्देश्य और जानकारी मांगने वाले व्यक्ति की पहचान सत्यापित करें।

स्कैम # 7 नकली लोन ऐप स्कैम

यह क्या होता है?

एक नकली लोन ऐप स्कैम में स्कैमर्स फर्जी ऐप्स बनाते हैं जो कम दस्तावेज़ीकरण के साथ त्वरित और आसान लोन का वादा करते हैं। ये ऐप्स अक्सर उन व्यक्तियों को लक्षित करते हैं जिन्हें पैसों की तत्काल आवश्यकता होती है, और उन्हें शुल्क भुगतान करने या व्यक्तिगत जानकारी साझा करने के लिए धोखा देते हैं। इन ऐप्स में अक्सर छिपे हुए शुल्क और बहुत उच्च ब्याज दरें होती हैं।

यह कैसे काम करता है?

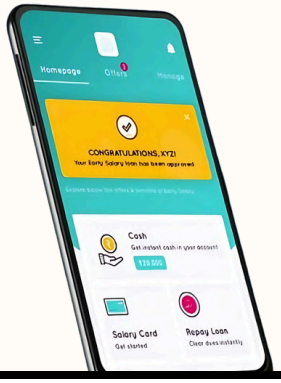
आकर्षक ऑफर: ऐप बिना क्रेडिट चेक, तुरंत अप्रूवल या बहुत कम ब्याज दरों के साथ लोन का विज्ञापन करता है, ताकि आपको उनकी सेवाओं का उपयोग करने के लिए आकर्षित किया जा सके। स्कैमर्स अक्सर प्रतिष्ठित वित्तीय संस्थानों जैसे बैंकों के समान नाम चुनते हैं ताकि वे आपको यह सोचने पर मजबूर करें कि वे वैध हैं।

अग्रिम शुल्क: जब आप आवेदन करते हैं, तो ऐप लोन जारी करने से पहले प्रोसेसिंग शुल्क, सेवा शुल्क या अन्य भुगतान की मांग करता है।

डेटा चोरी और मालवेयर हमले: ऐप आपकी संवेदनशील व्यक्तिगत जानकारी जैसे आपके बैंक खाता नंबर, आईडी प्रमाण, और फोन संपर्क एकत्र करता है। कभी-कभी इन ऐप्स में मालवेयर इंस्टॉल होता है जो डाउनलोड करने के बाद आपके फोन में लोड हो जाता है।

हिंसक व्यवहार: यदि आप भुगतान करने में असफल रहते हैं, तो स्कैमर चुराई गई जानकारी का उपयोग करके आपको, आपके परिवार को या आपके संपर्कों को धमकियां देकर या उनका सार्वजनिक रूप से अपमान करके परेशान करेंगे। उदाहरण के तौर पर, वे वीडियो-KYC करने का बहाना बनाकर आपकी तस्वीरें ऐक्सेस कर सकते हैं और उसके आधार पर आपको ब्लैकमेल कर सकते हैं।

लोन जारी नहीं किया गया: अक्सर, शुल्क चुकाने के बाद भी कोई लोन नहीं दिया जाता और ऐप गायब हो जाता है या जवाब देना बंद कर देता है।



- **स्रोत की पुष्टि करें:** लोन ऐप्स कभी भी लोन खुद नहीं जारी करते; इसके बजाय, वे RBI-नियंत्रित बैंकों या नॉन-बैंकिंग वित्तीय कंपनियों (NBFCs) के साथ साझेदारी करते हैं।

  जांचें कि क्या वे लोन ऐप जो ऐसी साझेदारी का दावा कर रहे हैं, वास्तव में बैंक और NBFCs के साथ साझेदारी में हैं। यदि आपको वेबसाइट पर कुछ नहीं मिलता, तो बैंक/NBFC के ग्राहक सेवा नंबर पर कॉल करके आगे की पुष्टि करें।

- **अनुमतियों के साथ सतर्क रहें:** ऐसे ऐप्स से बचें जो संपर्क, तस्वीरों या मैसेजों तक अनावश्यक ऐक्सेस की मांग करते हैं।

- **विश्वसनीय स्रोतों का उपयोग करें:** ऐप की वैधता और समीक्षाओं की पुष्टि करें। इसका उपयोग करने से पहले विभिन्न स्रोतों से समीक्षाओं की जांच करें। जैसा कि पहले कहा गया था, स्कैमर अक्सर अपनी वैधता का दिखावा करने के लिए नकली समीक्षाएं डालते हैं।

- **अग्रिम शुल्क:** वैध उधारदाता आम तौर पर अग्रिम शुल्क नहीं मांगते। ऐसे उधारदाताओं से बचें जो लोन जारी करने से पहले भुगतान की मांग करते हैं।

- **रेड फ़्लैग:** तुरंत लोन देने वाले ऑफर्स से सतर्क रहें, विशेष रूप से यदि वे बिना क्रेडिट चेक के गारंटीकृत स्वीकृति का वादा करते हैं।

- **ब्याज दरें:** ब्याज दरों और शर्तों की सावधानी से जांच करें। यदि वे बहुत अच्छी लग रही हैं, तो वे शायद सच नहीं हैं।

- **संपर्क जानकारी:** उधारदाता के संपर्क विवरण और भौतिक पते की पुष्टि करें। स्कैमर अक्सर नकली जानकारी का उपयोग करते हैं।

- **अगर फ़्रॉड का संशय है, तो रिपोर्ट करें:** यदि आप संभावित साइबर लोन शार्क का सामना करते हैं या आपको लगता है कि आपके साथ फ्रॉड हुआ है, तो तुरंत संबंधित अधिकारियों से इसकी रिपोर्ट करें।

स्कैम # 8 नकली मोबाइल रिचार्ज स्कैम

यह क्या होता है?

नकली मोबाइल रिचार्ज स्कैम आपको फोन रिचार्ज या ऑफ़र्स के लिए पैसे देने के लिए कहता है जो असली नहीं होते। स्कैमर्स नकली वेबसाइट्स, ऐप्स, या मैसेजों का इस्तेमाल करते हैं जो डिस्काउंट, कैशबैक, या मुफ्त रिचार्ज देने का दावा करते हैं।

यह कैसे काम करता है?

नकली ऑफ़र्स: स्कैमर्स मैसेज, सोशल मीडिया या नकली ऐप्स के माध्यम से अवास्तविक डील्स का विज्ञापन करते हैं, जैसे कि भारी डिस्काउंट्स या "मुफ्त रिचार्ज़।" कभी-कभी स्कैमर्स ख़ुद को TRAI का अधिकारी बताते हैं, ताकि आप उन पर विश्वास करें।

रिचार्ज के लिए भुगतान: पीड़ित नकली प्लेटफ़ॉर्म के माध्यम से रिचार्ज के लिए भुगतान करता है, लेकिन असल में कोई रिचार्ज नहीं किया जाता।

जानकारी चुराना: नकली रिचार्ज प्लेटफॉर्म अक्सर प्रक्रिया के दौरान व्यक्तिगत जानकारी, भुगतान विवरण, या बैंक/क्रेडिट कार्ड जानकारी एकत्र करते हैं।

फिशिंग लिंक: स्कैमर्स SMS या ईमेल के माध्यम से लिंक भेजते हैं, जो आपको नकली वेबसाइट्स पर ले जाते हैं जो वास्तविक टेलीकॉम रिचार्ज सेवाओं की नकल करती हैं।

- **विश्वसनीय प्लेटफॉर्म का उपयोग करें:** केवल अपने मोबाइल सेवा प्रदाता के ऐप या उस ऐप का उपयोग करें जो आपके UPI से जुड़ा हुआ हो।
- **अवास्तविक ऑफ़र्स से सावधान रहें:** ऐसी डील्स को नजरअंदाज करें जो असली से ज्यादा अच्छी लगती हैं, जैसे भारी डिस्काउंट या मुफ्त रिचार्ज।
- **वेबसाइट्स और ऐप्स की पुष्टि करें:** URL में नकली या गलत स्पेलिंग की जांच करें और केवल आधिकारिक ऐप स्टोर्स से ऐप्स डाउनलोड करें।
- **अप्रमाणित लिंक पर क्लिक न करें:** SMS, WhatsApp या ईमेल के माध्यम से भेजे गए रिचार्ज लिंक पर क्लिक करने से बचें, जो अज्ञात स्रोतों से आते हैं।
- **भुगतान विवरण सुरक्षित रखें:** कभी भी अपनी भुगतान जानकारी उन थर्ड-पार्टी प्लेटफ़ॉर्म के साथ साझा न करें जो प्रमाणित नहीं हैं।
- **संदिग्ध गतिविधि की रिपोर्ट करें:** यदि आप किसी स्कैम का सामना करते हैं तो अपने टेलीकॉम प्रदाता या स्थानीय साइबर क्राइम हेल्पलाइन को सूचित करें।

स्कैम # 9 पार्सल डिलीवरी स्कैम

यह क्या होता है?

पार्सल डिलीवरी स्कैम आपको यह सोचने पर मजबूर करते हैं कि आपका एक पैकेज डिलीवरी का इंतजार कर रहा है। स्कैमर नकली मैसेज या ईमेल भेजते हैं, जिसमें पैकेज को जारी करने के लिए भुगतान या व्यक्तिगत जानकारी मांगी जाती है।

यह कैसे काम करता है?

नकली सूचनाएँ: आपको एक टेक्स्ट, ईमेल या कॉल प्राप्त होती है जिसमें दावा किया जाता है कि आपका पैकेज आ गया है, लेकिन पते की अधूरी जानकारी या बकाया भुगतान के कारण इसे डिलीवर नहीं किया जा सकता है। यह मैसेज एक विश्वसनीय कूरियर कंपनी जैसे FedEx, DHL, या इंडिया पोस्ट से आता प्रतीत हो सकता है।

फिशिंग लिंक: मैसेज में एक लिंक शामिल होता है जिसमें आपको अपना पता अपडेट करने को कहा जाता है। ऐसा अक्सर सीमित समय के भीतर, जैसे 12 घंटों में करने के लिए कहा जाता है। मैसेज में "डिलीवरी की पुष्टि करने" या शुल्क का भुगतान करने का लिंक भी हो सकता है। लिंक पर क्लिक करने से आपको एक नकली वेबसाइट पर ले जाया जाता है, जहां स्कैमर आपकी भुगतान जानकारी या व्यक्तिगत जानकारी चुराते हैं।

फॉलो-अप कॉल: आमतौर पर, SMS या ईमेल के साथ कूरियर कंपनी के प्रतिनिधि के रूप में किसी व्यक्ति का फोन कॉल आता है। वह कहता है कि आपका पार्सल डिलीवर नहीं किया जा सकता क्योंकि आपका पता अधूरा है या कुछ भुगतान बकाया है और आपको लिंक पर जाकर औपचारिकता पूरी करने के लिए प्रेरित करता है।

तत्कालिता और दबाव: कॉल करने वाला पीड़ित पर दबाव डालता है और धमकी देता है कि अगर पता अपडेट नहीं किया गया या भुगतान नहीं किया गया तो ऑर्डर रद्द कर दिया जाएगा या पार्सल नष्ट कर दिया जाएगा।

भुगतान का जाल: आपको फिर से डिलीवरी के लिए एक छोटी सी फीस भुगतान करने के लिए कहा जाता है। वेबसाइट केवल डेबिट या क्रेडिट कार्ड के जरिए भुगतान स्वीकार करती है, जिसमें UPI या कैश ऑन डिलीवरी का कोई विकल्प नहीं होता।

कोई डिलीवरी नहीं: जब आप भुगतान कर देते हैं या विवरण प्रदान कर देते हैं, तो स्कैमर गायब हो जाते हैं, जिससे आपको कोई पैकेज नहीं मिलता और आपकी जानकारी चोरी हो सकती है।

- **याद करें कि क्या आपने ऑर्डर दिया है:** यह याद करने की कोशिश करें कि क्या वास्तव में आपका कोई पैकेज रास्ते में है या क्या आपने कोई ऑर्डर दिया है जो अभी तक डिलीवर नहीं हुआ है।
- **मैसेज की पुष्टि करें:** कूरियर कंपनी से सीधे उनके आधिकारिक वेबसाइट या फोन नंबर के माध्यम से संपर्क करें ताकि डिलीवरी की पुष्टि हो सके।
- **अज्ञात लिंक पर क्लिक करने से बचें:** मैसेज में आए लिंक पर क्लिक न करें, खासकर अगर वह पैकेज के बारे में हो और भेजने वाला अज्ञात हो।
- **रेड फ़्लैग देखें:** खराब व्याकरण, सामान्य अभिवादन या संदिग्ध ईमेल पतों से सावधान रहें।
- **अपनी जानकारी सुरक्षित रखें:** व्यक्तिगत या भुगतान जानकारी कभी भी न दें जब तक कि आपको स्रोत की वैधता का पूरा यकीन न हो।

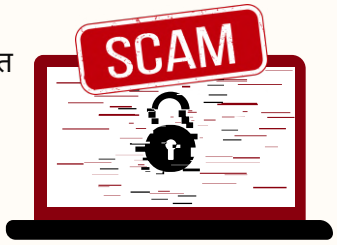
स्कैम # 10 अप्रकट मालवेयर स्कैम

यह क्या होता है?

एक अप्रकट मालवेयर स्कैम आपको हानिकारक लिंक पर क्लिक करने के लिए प्रेरित करता है, जिसका उद्देश्य मालवेयर फैलाना या व्यक्तिगत जानकारी चुराना होता है। ये लिंक अक्सर वैध दिखते हैं, लेकिन इन पर क्लिक करने से आपका डिवाइस संक्रमित हो सकता है या ये आपको हानिकारक साइट्स पर ले जा सकते हैं।

यह कैसे काम करता है?

वेबसाइटों पर लिंक का स्थान: स्कैम करने वाले यह लिंक विभिन्न तरीकों से वेबसाइटों पर विज्ञापनों के माध्यम से रखते हैं।



क्लिक करके संक्रमित होना: जब आप लिंक पर क्लिक करते हैं, तो यह निम्नलिखित कर सकता है:

- आपके डिवाइस पर मालवेयर इंस्टॉल करना,
- आपको फ़िशिंग वेबसाइट्स पर रीडायरेक्ट करना, या
- आपको फेक सॉफ़्टवेयर या अपडेट डाउनलोड करने पर मजबूर करना।

किसी प्रतिक्रिया की आवश्यकता नहीं है: कुछ हानिकारक लिंक के लिए क्लिक करने की भी आवश्यकता नहीं होती—वे सिर्फ कुछ वेबसाइट्स पर दिखाई देने से ही आपके डिवाइस को संक्रमित कर सकते हैं (मेलीशियस कोड के माध्यम से)।

- **संदेहास्पद लिंक से बचें:** ऐसे लिंक पर क्लिक न करें जो अविश्वसनीय डील्स, मुफ्त सॉफ़्टवेयर, या तात्कालिक चेतावनियाँ प्रदान करते हैं।
- **सॉफ़्टवेयर को अपडेट रखें:** यह सुनिश्चित करें कि आपका ब्राउज़र और सुरक्षा सॉफ़्टवेयर अद्यतित हैं ताकि हानिकारक विज्ञापनों को ब्लॉक किया जा सके।
- **सुरक्षा फीचर्स सक्षम करें:** एंटीवायरस सॉफ़्टवेयर और ब्राउज़र सुरक्षा सेटिंग्स का उपयोग करें ताकि खतरों का पता चल सके और उन्हें ब्लॉक किया जा सके। यदि आप गलती से किसी धोखेबाज वेबसाइट पर चले जाते हैं, तो कुछ एंटीवायरस सॉफ़्टवेयर में मालवेयर सुरक्षा होती है, जो खतरों को ब्लॉक करती है। सुनिश्चित करें कि आप ऐसे फीचर्स वाले एंटीवायरस सॉफ़्टवेयर का उपयोग करें। इसके अलावा, यह सुनिश्चित करें कि आपके ब्राउज़र की रिस्क मॉनिटरिंग सेटिंग्स चालू हों।
- **विश्वसनीय वेबसाइट्स पर ही रहें:** संदिग्ध या ग़ैर- वेरिफ़ाइड वेबसाइट्स पर न जाएं और न ही उनसे इंटरएक्ट करें। विश्वसनीय और प्रसिद्ध वेब ब्राउज़र का उपयोग करें जो आपको ऐसी वेबसाइट्स खोलने पर चेतावनी देता है और बताता है कि इनमें हानिकारक सामग्री, मालवेयर, या सुरक्षा प्रमाणपत्रों की कमी हो सकती है।

स्कैम # 11 टेक सपोर्ट स्कैम के संकेत

यह क्या होता है?

टेक सपोर्ट स्कैम आपको यह विश्वास दिलाता है कि आपके कंप्यूटर या डिवाइस में कोई समस्या है। स्कैमर खुद को माइक्रोसॉफ्ट या एप्पल जैसी वास्तविक कंपनियों से बताते हैं और नकली "सपोर्ट" प्रदान करने का दावा करते हैं ताकि वे काल्पनिक समस्याओं को ठीक करने के नाम पर आपका पैसा या व्यक्तिगत जानकारी चुरा सकें।

यह कैसे काम करता है?

फर्जी चेतावनी मैसेज: आपको अपने कंप्यूटर या फोन पर एक पॉप-अप दिखाई देता है, जिसमें यह दावा किया जाता है कि आपका डिवाइस वायरस से संक्रमित है या इसमें कोई गंभीर त्रुटि है। इसमें अक्सर एक फर्जी ग्राहक सहायता नंबर भी होता है।

स्पैम कॉल्स: स्कैमर कॉल करके यह दावा करते हैं कि उन्हें आपके डिवाइस में समस्याएं नज़र आई है और वे तकनीकी सहायता प्रदान करने के लिए फोन करते हैं।

स्क्रीन मिररिंग सॉफ़्टवेयर: स्कैमर्स आपको रिमोट डेस्कटॉप सॉफ़्टवेयर या स्क्रीन-शेयरिंग ऐप डाउनलोड करने के लिए कहते हैं, ताकि वे आपके कंप्यूटर की त्रुटि को ठीक कर सकें। वे आपको एक पिन शेयर करने के लिए कहते हैं, जिससे वे किसी भी स्थान से आपके डिवाइस तक पहुंच सकते हैं। स्कैमर इसके बाद आपकी फाइलों को देख सकते हैं, डेटा ट्रांसफर कर सकते हैं, वायरस इंस्टॉल कर सकते हैं और आपके डिवाइस को नियंत्रित कर सकते हैं।

भुगतान की मांग: वे समस्या ठीक करने का दावा करते हैं और फर्जी सेवाओं के लिए भुगतान की मांग करते हैं, जो अक्सर क्रेडिट कार्ड या गिफ्ट कार्ड के माध्यम से होता है।

डेटा चोरी: जब वे आपके डिवाइस तक पहुंचते हैं, तो वे संवेदनशील जानकारी जैसे पासवर्ड या बैंकिंग विवरण चुरा सकते हैं।

- **अनचाही कॉल पर विश्वास न करें:** वैध कंपनियां आपको उन समस्याओं के बारे में कॉल नहीं करतीं, जिन्हें आपने रिपोर्ट नहीं किया है।
- **पॉप-अप की अनदेखी करें:** किसी भी संदिग्ध पॉप-अप को बंद कर दें और प्रदर्शित नंबरों पर कॉल न करें। इसके बजाय, अपने डिवाइस को स्कैन करने के लिए एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
- **रिमोट एक्सेस कभी न दें:** किसी को भी आपके डिवाइस को रिमोटली नियंत्रित करने की अनुमति न दें, जब तक कि आपने एक विश्वसनीय, सत्यापित सहायता सेवा से संपर्क न किया हो।
- **सहायता दावों की सत्यता जांचें:** वेबसाइट पर दिए गए आधिकारिक संपर्क विवरणों का उपयोग करके कंपनी से सीधे संपर्क करें, न कि स्कैमर द्वारा दिए गए नंबर से।
- **एंटीवायरस सॉफ़्टवेयर का उपयोग करें:** अपने उपकरणों को अपडेट और सुरक्षित रखें और विश्वसनीय एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
- **फ्रॉड की रिपोर्ट करें:** अगर आपको तकनीकी सहायता फ्रॉड का सामना करना पड़े, तो इसे स्थानीय अधिकारियों या जिस कंपनी का नाम लेकर ऐसा किया जा रहा है, उस से रिपोर्ट करें।

स्कैम # 12 OTP स्कैम

यह क्या होता है?

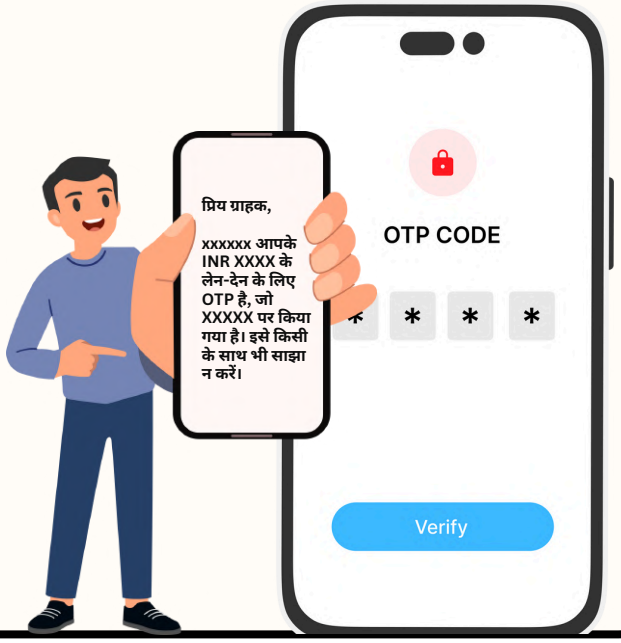
वन टाइम पासवर्ड (OTP) स्कैम में आपको फ़्रॉड लोगों को अपना OTP बताने के लिए गुमराह किया जाता है। OTP सामान्यत: आपकी पहचान की पुष्टि करने या ऑनलाइन लेन-देन अथवा वेबसाइट्स में लॉगिन के लिए अनुमति की पुष्टि करने के लिए उपयोग किए जाते हैं। ये कोड सामान्यत: SMS या ईमेल के माध्यम से भेजे जाते हैं और इन्हें केवल एक बार उपयोग के लिए निर्धारित किया जाता है।

यह कैसे काम करता है?

अधिकार का दुरुपयोग: स्कैमर कॉल्स या ईमेल्स के माध्यम से बैंकों, ई-कॉमर्स वेबसाइट्स, पार्सल डिलीवरी सेवाओं या अन्य सेवा प्रदाताओं की वास्तविक सेवाओं की नकल करते हैं।

झूठी आपात स्थिति का आभास: स्कैमर झूठी आपात स्थिति का आभास पैदा करते हैं, जिससे आप गुमराह हो जाते हैं और वे बिना यह सत्यापित किए कि प्राप्तकर्ता कौन है, आपके ऊपर OTP शेयर करने का दबाव डालते हैं।

पैसों या व्यक्तिगत जानकारी की चोरी: धोखेबाज OTP का उपयोग करके संवेदनशील जानकारी जैसे बैंकिंग विवरण या व्यक्तिगत जानकारी प्राप्त करते हैं, जिसका उपयोग वे पहचान की चोरी के लिए करते हैं।



- **शांत रहें:** उत्पन्न की गई आपात स्थिति के झांसे में न आएँ, शांत रहें और अपने लेन-देन का इतिहास ट्रेस करें, प्रेषक की पहचान सत्यापित करें और उचित सतर्कता बरतें।
- **अज्ञात कॉल्स और ईमेल्स से सतर्क रहें:** कभी भी किसी ऐसे व्यक्ति के साथ व्यक्तिगत जानकारी या OTP साझा न करें जो अचानक आपसे संपर्क करता है। सामान्यत:, केवल तब संवेदनशील जानकारी की आवश्यकता हो सकती है, जब आप बैंकों या अन्य सेवाओं से संपर्क करते हैं और वे CVV और अन्य संवेदनशील व्यक्तिगत या वित्तीय जानकारी मांगते हैं।
- **प्रेषक की पहचान सत्यापित करें:** ईमेल या लिंक पर क्लिक करने से पहले, प्रेषक की पहचान सत्यापित करें।
- **उचित सतर्कता बरतें:** कॉल करने वाले से OTP के उद्देश्य के बारे में जानकारी मांगें और यह सुनिश्चित करें कि आपने कोई ऐसी लेन-देन की है या नहीं, और क्या वे आपको फोन या लिंक पर OTP साझा करने के लिए कह सकते हैं।

स्कैम # 13 पुरस्कार स्कैम

यह क्या होता है?

पुरस्कार स्कैम में, आपको एक पुरस्कार का लालच देकर आपकी संवेदनशील जानकारी हासिल करने का प्रयास किया जाता है।

यह कैसे काम करता है?

पुरस्कार संचार साझा करना: स्कैमर आपको एक ईमेल या SMS भेजते हैं, जिसमें आपको बड़ी नकद राशि या क्रेडिट कार्ड पॉइंट्स जीतने की बधाई दी जाती है। यह आपको किसी वेबसाइट या फ्रॉड ऐप पर जाने के लिए लिंक पर क्लिक करने का निर्देश देता है।

यह ऐसा दिख सकता है: "प्रिय मान्य ग्राहक, आपके SBI नेटबैंकिंग रिवॉर्ड पॉइंट्स (Rs 9980) आज समाप्त हो जाएंगे! अब SBI रिवॉर्ड ऐप इंस्टॉल करें और अपने खाते में नकद जमा करके अपना पुरस्कार क्लेम करें।"

झूठी वेबसाइटें: वेबसाइट वैध प्रतीत हो सकती है और आपसे आपकी व्यक्तिगत या बैंकिंग जानकारी दर्ज करने को कह सकती है। हालांकि, डेटा को स्कैमर्स द्वारा एक्सेस किया जाता है।

झूठे ऐप्स: स्कैमर्स आपको ऐसे ऐप्स डाउनलोड करने के लिए निर्देशित कर सकते हैं जो दिखने में वैध होते हैं जैसे 'SBI रिवॉर्ड्स', ताकि आप पुरस्कार क्लेम कर सकें। हालांकि, यह एक मेलीशियस ऐप होता है और कैमरा, माइक्रोफ़ोन, संपर्क सूची, फ़ोटो, मैसेज आदि जैसे संवेदनशील ऐप्स को एक्सेस कर सकता है।

दुर्भावनापूर्ण पुरस्कार: इसके अलावा, स्कैमर यह भी दावा कर सकते हैं कि आपने नया फोन, टैबलेट या लैपटॉप जीता है। हालांकि, ये उपकरण पहले से इंस्टॉल किए गए दुर्भावनापूर्ण ऐप्स या वायरस से भरे होते हैं जो आपकी संवेदनशील व्यक्तिगत जानकारी, जिसमें बैंकिंग डेटा भी शामिल है, चुरा सकते हैं।

- **सावधान रहें:** पुरस्कार और प्राइज़ का दावा करने के लिए लिंक पर क्लिक करने से पहले मैसेज की सामग्री को ध्यान से पढ़ें।
- **सत्यापन करें:** यह जांचें कि क्या ऐसा कोई रिवॉर्ड प्रोग्राम लाइव है, जैसे कि बैंक या अन्य सेवाओं से पुष्टि प्राप्त करें। उदाहरण के लिए, जो बड़ी कंपनियां रिवॉर्ड प्रोग्राम चलाती हैं, वे इसे अपनी आधिकारिक वेबसाइटों पर प्रचारित करती हैं।
- **फैक्ट्री रीसेट करें:** जो भी उपकरण आपको उपहार या पुरस्कार के रूप में प्राप्त होते हैं, उसमें व्यक्तिगत जानकारी डालने से पहले फैक्ट्री रीसेट करें। यह ऐसे किसी रीसेल उपकरण के लिए भी एक अच्छा अभ्यास है जिसे आप खरीदते हैं।

स्कैम # 14 SIM स्वैपिंग / SIM क्लोनिंग स्कैम

यह क्या होता है?

SIM स्वैपिंग, जिसे SIM क्लोनिंग भी कहा जाता है, तब होता है जब स्कैमर आपका SIM कार्ड डुप्लिकेट कर लेते हैं ताकि वे आपके फोन नंबर को कंट्रोल कर सकें। जब वे इसमें प्रवेश कर लेते हैं, तो वे OTP-आधारित सुरक्षा जांच को बायपास कर सकते हैं और आपके बैंक अकाउंट से पैसे चुरा सकते हैं।

यह कैसे काम करता है?

टेलीकॉम प्रोवाइडर को नंबर पोर्ट करने के लिए मनाना: स्कैमर्स फ़िशिंग ईमेल्स, मालवेयर अटैक्स या डेटा लीक के जरिए व्यक्तिगत जानकारी इकट्ठा करते हैं। इसके बाद वे आपके मोबाइल नेटवर्क प्रोवाइडर से संपर्क करते हैं और खुद को आपकी पहचान बताकर, नकली ID प्रूफ प्रदान करते हैं और एक नया SIM कार्ड मांगते हैं। वह ये दावा करते हैं कि पुराना खो गया है या क्षतिग्रस्त है।

SIM स्वैप के लिए मनाना: कभी-कभी स्कैमर्स आपको SIM स्वैप को सक्रिय करने के लिए मनाने की कोशिश करते हैं। इस तरीके में, स्कैमर आपको एक नकली कॉल करता है और खुद को आपके टेलीकॉम प्रोवाइडर का एक एग्जीक्यूटिव बताता है। स्कैमर एक बेहतर मोबाइल सब्सक्रिप्शन पैकेज का ऑफर देता है और आपको आपका 20 अंकों वाला SIM नंबर साझा करने और “1” दबाने के लिए मनाता है, ताकि आप ऑफर को सक्रिय कर सकें। हालांकि, जब आप "1" दबाते हैं, तो आप अपने नंबर पर SIM स्वैप को प्रमाणित कर देते हैं और स्कैमर को नियंत्रण दे देते हैं।

नियंत्रण प्राप्त करना: जब प्रोवाइडर नया SIM जारी करता है या SIM स्वैप पूरा कर देता है, तो आपका मूल SIM निष्क्रिय हो जाता है। स्कैमर को आपके कॉल्स, मैसेजेस और OTP तक पहुंच मिल जाती है।

वित्तीय फ्रॉड और पहचान की चोरी: स्कैमर्स OTP का उपयोग करके पैसे ट्रांसफर करते हैं, पासवर्ड रीसेट करते हैं और आपके वित्तीय और सोशल मीडिया अकाउंट्स पर कब्जा कर लेते हैं।

- **SIM लॉक सक्षम करें:** अपने डिवाइस की सेटिंग्स में जाएं और अपने SIM को लॉक करने के लिए SIM PIN सेट करें। स्कैमर्स आपके SIM PIN के बिना आपके SIM को स्वैप या निष्क्रिय नहीं कर पाएंगे।
- **नेटवर्क समस्याओं के लिए सतर्क रहें:** यदि आपके फोन का अचानक नेटवर्क चला जाता है, जबकि अन्य लोगों के सिग्नल आ रहे हैं, तो तुरंत अपने प्रोवाइडर से संपर्क करें।
- **अपने डिजिटल फुटप्रिंट के बारे में सतर्क रहें:** गूगल, मेटा जैसी लोकप्रिय सेवाओं पर अपने प्राइवेसी सेटिंग्स की समीक्षा करने के लिए समय निकालें। आप जान सकते हैं कि आपकी व्यक्तिगत जानकारी कितनी थर्ड पार्टी के साथ साझा की जाती है।

स्कैम # 15 ग़लत पहचान स्कैम

यह क्या होता है?

स्कैमर हैकिंग, चुराए गए पासवर्ड और फ़िशिंग तकनीकों का उपयोग करके आपके दोस्त, रिश्तेदार या सहकर्मी का रूप धारण करते हैं और फिर आपको पैसे भेजने के लिए गुमराह करते हैं। यह मैसेज एक परिचित व्यक्ति से आते हुए प्रतीत होते हैं, इसलिए पीड़ित अक्सर इस फ्रॉड के शिकार हो जाते हैं।

यह कैसे काम करता है?

स्कैमर किसी का सोशल मीडिया अकाउंट हैक कर लेते हैं और उनके संपर्कों को एक आपात स्थिति में होने का मैसेज भेजते हैं।

मैसेज ऐसा दिख सकते हैं: **"नमस्ते, मैं दिल्ली में फंसा हुआ हूं। मैं यहाँ छुट्टियों पर आया था और मुझे किसी ने लूट लिया है। मुझे तुरंत 5000 रुपये की आवश्यकता है, लेकिन जितना हो सके मुझे भेज दें, आपका बहुत आभार होगा और मैं वापस आने पर आपको जल्द ही पैसे लौटा दूंगा। कृपया मदद करें।"**

कभी-कभी स्कैमर एक ऐसा ईमेल बनाते हैं जो आपके सहकर्मी या बॉस के ईमेल आईडी जैसा लगता है। वे औपचारिक लहजे में ईमेल लिखते हैं और आपसे एक ज़रूरी टास्क पूरा करने के लिए पैसे माँगते हैं।
जब आप स्कैमर को हैक किए गए अकाउंट या नकली ईमेल पर जवाब देते हैं, तो वे आपको एक विशिष्ट खाते या यूपीआई हैंडल पर पैसे ट्रांसफर करने के लिए कहते हैं। पैसे भेजने के बाद स्कैमर गायब हो जाते हैं और पीड़ित को ब्लॉक कर देते हैं।

- **आपातकालीन मैसेजों से सावधान रहें:** स्कैमर घबराहट पैदा करते हैं, ताकि आप जल्दबाज़ी में कोई काम करें। ऐसे मैसेज से सतर्क रहें जो मैसेजिंग ऐप्स, सोशल मीडिया या ईमेल पर अचानक पैसों के लिए आपातकालीन अनुरोध भेजते हैं।
- **अनुरोधों की पुष्टि करें:** आपातकालीन रूप से पैसे के अनुरोध को मानने से पहले सुनिश्चित करें कि आप उस व्यक्ति से सीधे संपर्क करें या एक सामान्य दोस्त/रिश्तेदार से बात करें।
- **रेड फ़्लैग जाँचें:** क्या मैसेज उसी लहजे में लिखा गया है जिसमें भेजने वाला आमतौर पर बात करता है? असामान्य अनुरोध, अजीब व्याकरण और फॉर्मेटिंग का ध्यान रखें और नए/अज्ञात बैंक खातों में पैसे ट्रांसफर करने के अनुरोध देखें।

स्कैम # 16 स्किमिंग मशीन फ्रॉड

यह क्या होता है?

स्किमिंग के तहत स्कैमर एटीएम या हैंडहेल्ड कार्ड पेमेंट मशीनों में एक उपकरण छिपाते हैं, जिससे आपके कार्य की महत्वपूर्ण जानकारी जैसे कार्ड नंबर, समाप्ति तिथि और तीन अंकों वाला कार्ड सत्यापन मूल्य (सीवीवी) को चुराया जाता है।

ये उपकरण अक्सर मशीन के सामान्य हिस्से लगते हैं। जब कार्ड विवरण कैप्चर हो जाता है, तो धोखेबाज डुप्लिकेट कार्ड बनाकर आपके खाते से लेन-देन करते हैं।

यह कैसे काम करता है?

स्किमर लगाना: स्कैमर एटीएम या स्वाइप मशीन के कार्ड रीडर पर एक उपकरण जोड़ते हैं।

कार्ड डेटा कैप्चर करना: जब आप अपना कार्ड डालते हैं, तो स्किमर आपके कार्ड की जानकारी पढ़ता है।

पिन रिकॉर्ड करना: एक छोटा कैमरा या नकली कीपैड एटीएम पर आपका पिन रिकॉर्ड करता है।

क्लोनिंग और फ्रॉड लेन-देन: धोखेबाज चुराई गई जानकारी का उपयोग करके डुप्लिकेट कार्ड बनाते हैं और पैसे निकालते हैं।

- **एटीएम का निरीक्षण करें:** एटीएम पर ढीले कार्ड स्लॉट, झूलते कीपैड या अतिरिक्त कैमरों की जांच करें।
- **सावधान रहें:** कार्ड स्वाइप मशीन का हमेशा अपने सामने इस्तेमाल करने के लिए कहें और संदिग्ध स्थानों या मशीनों पर कार्ड स्वाइप करने में सतर्क रहें।
- **बैंक स्टेटमेंट की निगरानी करें:** अपनी बैंक स्टेटमेंट और एसएमएस को नियमित रूप से चेक करें ताकि अवैध डेबिट लेन-देन का पता चल सके।
- **बैंक को तुरंत अवैध लेन-देन की रिपोर्ट करें:** अगर आप बैंक को जल्दी सूचित करते हैं तो आप नुकसान को सीमित कर सकते हैं।

स्कैम # 17 फर्जी कल्याणकारी योजना स्कैम

यह क्या होता है?

स्कैमर फर्जी पोर्टल्स बनाते हैं जो पीएम किसान योजना, पीएम आवास योजना जैसी सामान्य योजनाओं की वेबसाइट्स के समान दिखते हैं। स्कैमर इसके तहत पीड़ित को अपनी बैंक खाता जानकारी, मोबाइल नंबर, और आधार विवरण दर्ज करने के लिए कहते हैं।

यह कैसे काम करता है?

स्कैमर आपको कॉल करते हैं और बताते हैं कि आप एक सामाजिक कल्याण योजना के तहत फंड प्राप्त करने के योग्य हैं, लेकिन आपको पहले अपना बैंक विवरण 'सत्यापित' या 'अपडेट' करना होगा, ताकि राशि आपके पास भेजी जा सके।

फिर स्कैमर आपको अपनी बैंक खाता जानकारी और डेबिट कार्ड विवरण साझा करने के लिए कहते हैं ताकि 'सत्यापन' प्रक्रिया पूरी हो सके। वे अंत में सत्यापन पूरा करने के लिए आपसे OTP मांगते हैं।

लेकिन स्कैमर आपके बैंक और डेबिट कार्ड विवरण का उपयोग करके आपके खाते पर भुगतान सेट करते हैं और डेबिट लेनदेन को अधिकृत करने के लिए OTP का उपयोग करते हैं। OTP साझा करने के बाद पीड़ित को समझ आता है कि स्कैमर ने उनके खाते से पैसे निकाल लिए हैं।

- **फ्रीबीज़ के बारे में सावधान रहें:** धोखेबाज अक्सर फ्रीबीज़, टैक्स छूट, या अन्य प्रोत्साहन का वादा करते हैं ताकि आप अपनी व्यक्तिगत और वित्तीय जानकारी साझा करें।
- **सरकारी वेबसाइटों की पुष्टि करें:** कल्याण योजनाओं के लिए आधिकारिक पोर्टल का उपयोग करें। सरकारी वेबसाइटों का आमतौर पर अंत में ".gov.in" या ".nic.in" एक्सटेंशन होता है।
- **योजना विवरण की पुष्टि करें:** किसी भी सरकारी योजना के विवरण की पुष्टि अपनी ग्राम पंचायत या तहसीलदार कार्यालय से करें।
- **सावधानी बरतें:** OTP वाली मैसेज को ध्यान से पढ़ें। जांचें कि क्या यह वैध लग रहा है है या यह कुछ और है। हमारे प्रो-टिप्स पेज 38 पर देखें।

क्या करें और क्या न करें

सुरक्षित रूप से सर्फिंग करने की टिप्स

- नियमित रूप से अपने ब्राउज़र और ऐप्स की गोपनीयता सेटिंग्स की समीक्षा करें, जैसे मैसेजिंग, सोशल मीडिया, और मैप्स, ताकि आप ऑनलाइन अपने बारे में जो जानकारी साझा करते हैं, उसे सीमित कर सकें।
- सुनिश्चित करें कि थर्ड-पार्टी और सोशल मीडिया ऐप्स की आपके डिवाइस के डेटा, जैसे फ़ोटो, फ़ाइलें, और डिवाइस के स्थान तक सीमित पहुंच हो।
- पासवर्ड याद रखें या उन्हें कहीं सुरक्षित रूप से लिखकर रखें। अपने पासवर्ड को नियमित रूप से बदलें और अलग-अलग वेबसाइट्स और ऐप्स पर पासवर्ड को दोहराने से बचें।
- यदि आप किसी फिशिंग स्कैम के पीड़ित हैं और आपकी बैंक या कार्ड की जानकारी स्कैमर के हाथों में पड़ गई है, तो तुरंत अपने बैंक से संपर्क करें और इसकी रिपोर्ट करें।
- जब तक जरूरी न हो, अपने डिवाइस पर लोकेशन सेवाओं को बंद रखें।
- यदि निवेश योजना / नौकरी का प्रस्ताव कुछ ज़्यादा ही अच्छा लग रहा है, तो शायद यह सच नहीं है।

ऐसा बिल्कुल न करें

- अज्ञात स्रोतों से एसएमएस / ईमेल या मैसेजिंग ऐप्स पर दिए गए किसी भी लिंक पर क्लिक करने से पहले ध्यान से पढ़ें।
- ओटीपी, एटीएम या यूपीआई पिन और पासवर्ड कॉल्स, एसएमएस, ऑनलाइन फॉर्म और ईमेल्स पर साझा न करें।
- मैसेजिंग ऐप्स पर अज्ञात नंबर से शादी के निमंत्रण जैसे फ़ाइलें डाउनलोड न करें।
- सोशल मीडिया पर अजनबियों से दोस्ती के अनुरोध और मैसेज अनुरोध स्वीकार न करें।
- सॉफ़्टवेयर और मीडिया की पायरेटेड कॉपी डाउनलोड और इंस्टॉल न करें, इनमें मालवेयर हो सकता है।
- असुरक्षित वेबसाइट्स पर लेन-देन करते समय सावधान रहें (सुनिश्चित करें कि वेब पता “https://” से शुरू होता है, “http://” से नहीं)।
- ऑनलाइन लेन-देन के लिए सीवीवी दर्ज करते समय सावधान रहें।

विशेष सुझाव

1 पासवर्ड सुरक्षा

- कम से कम 16 वर्णों का पासवर्ड बनाएँ, जिसमें अपरकेस, लोअरकेस, संख्याएँ और प्रतीक हों।
- ऐसे पैटर्न में पासवर्ड न लिखें जिसका पूर्वानुमान लगाया जा सके। इसके अलावा, व्यक्तिगत जानकारी या अनुक्रमिक वर्णों से बचें।
- जहां संभव हो, पासकीज़ सक्षम करें। पासकीज़ पारंपरिक पासवर्ड के बजाय बायोमेट्रिक्स जैसे फिंगरप्रिंट, फेस आईडी या वॉयस रिकग्निशन का उपयोग करती हैं।
- अतिरिक्त सुरक्षा के लिए जहां भी उपलब्ध हो, मल्टी फैक्टर ऑथेंटिकेशन सेट करें।

कमजोर पासवर्ड

साधारण: Aditi1995 (नाम + जन्म वर्ष)
क्रमिक: abcdxyz123
अनुमान योग्य: SalmanBhaiFan

मजबूत पासवर्ड

व्यक्तिगत: Maachbhaat&Dal92

यादृच्छिक शब्द और कई पात्र: C@rr0tcake&MnMs!

2 SMS कोड्स को समझना

फर्जी SMS मैसेज वास्तविक मैसेजों की नकल करके बनाए जाते हैं, जो अक्सर आपके ऊपर तुरंत एक्शन लेने के लिए दबाव डालते हैं। यहां बताया गया है कि आप ऐसे स्कैमर्स से कैसे पहचाना जा सकता है और खुद को सुरक्षित रखा जा सकता है:

- जाली मैसेज अक्सर व्यक्तिगत मोबाइल नंबरों या सामान्य संख्यात्मक आईडी जैसे 567678 या 909090 से भेजे जाते हैं।
- वास्तविक SMS का प्रारूप [XY-ABCDEF] होता है।
  - X वह टेलीकॉम सेवा प्रदाता का नाम होता है (जैसे Jio के लिए J, Airtel के लिए A और Vodafone के लिए V)।
  - Y सेवा क्षेत्र का नाम होता है (जैसे दिल्ली के लिए D, मुंबई के लिए M और कर्नाटका के लिए X)।
  - ABCDEF वह कोड है जो भेजने वाले को सौंपा जाता है (जैसे SPICEJ Spice Jet के लिए)।

.. जारी

- **चित्रण:**
    - SMS कोड 'AD-SHPRKT' का मतलब है कि भेजने वाला Ship Rocket है, कैरियर Airtel है और मैसेज दिल्ली से भेजा गया है।
    - SMS कोड 'VM-SBIUPI' का मतलब है कि भेजने वाला State Bank of India है, कैरियर Vodafone है और मैसेज मुंबई से भेजा गया है।
- TRAI एक विस्तृत सूची बनाए रखता है जिसमें सेवा प्रदाता कोड, टेलीकॉम सेवा क्षेत्र कोड और व्यवसायों के लिए आवंटित हेडर शामिल हैं। खासकर भुगतान के लिए किसी लिंक पर क्लिक करने से पहले SMS की प्रामाणिकता की पुष्टि करें।

#3 स्कैमर और धोखेबाजों से निपटना

- **कॉल काटें और नंबर ब्लॉक करें:** अज्ञात कॉल करने वालों द्वारा अपनाई गई आपातकाल वाली या डराने वाली चालों का जवाब न दें, चाहे वे ख़ुद को बैंक या सरकारी प्रतिनिधि ही क्यों न कहें।
- **रिपोर्ट करें:** 'संचार साथी' पोर्टल (www.sancharsaathi.gov.in) पर 'चक्षु' को रिपोर्ट करके स्कैमर का नंबर निष्क्रिय करवाएं।
- **अगर आप अपना पैसा खो चुके हैं:** तुरंत अपने बैंक से संपर्क करें और लेन-देन की रिपोर्ट करें। इसके अलावा राष्ट्रीय साइबरक्राइम रिपोर्टिंग पोर्टल (डायल 1930 या www.cybercrime.gov.in पर जाएं) पर भी घटना की रिपोर्ट करें।
- **स्पैम को फ़िल्टर करें:** अपने टेलीकॉम प्रोवाइडर द्वारा TRAI दिशानिर्देशों के अनुसार स्पैम ब्लॉकिंग सुविधा के लिए 1909 डायल करें और रजिस्टर करें।
- **सतर्कता बनाए रखें:** नवीनतम जानकारी के लिए I4C को सोशल मीडिया पर फॉलो करें: (X (ट्विटर) पर @CyberDost; फेसबुक पर CyberDostI4C या इंस्टाग्राम पर @cyberdosti4c देखें।
- **अपना डिजिटल फुटप्रिंट जाँचें:** अपने डिजिटल फुटप्रिंट के आकार को लेकर सतर्क रहें। समीक्षा करें कि आपने कितनी कंपनियों को अपना डेटा दिया है। आवश्यकता होने पर उनसे आपका डेटा हटाने के लिए कहें। साथ ही, यह पता लगाने के लिए 'www.haveibeenpwned.com' जैसे फ्री टूल्स का उपयोग करें कि आपका डेटा किसी डेटा ब्रीच का हिस्सा तो नहीं रहा है।

उपयोगकर्ता सुरक्षा के लिए उद्योग के सर्वोत्तम अभ्यास

उपयोगकर्ता की सुरक्षा सुनिश्चित करना एक निरंतर प्रक्रिया है। जैसे-जैसे डिजिटल स्पेस और अधिक आकर्षक होते जा रहे हैं, व्यवसायों को अपनी प्रथाओं को विकसित करना होगा ताकि वे उपयोगकर्ताओं को सूचित, सशक्त और सुरक्षित रख सकें।

उपयोगकर्ता सुरक्षा के चार बुनियादी सिद्धांत हैं:

💪 **इंटरनेट उपयोगकर्ताओं को ऑनलाइन इंटरएक्शन पर नियंत्रण प्राप्त करने के लिए सशक्त बनाना**

🔐 **ऐसे उत्पाद बनाना जो डिज़ाइन द्वारा सुरक्षित हों**

🤝 **तुरंत और प्रभावी शिकायत निवारण सुनिश्चित करना**

🤖 **उपयोगकर्ताओं को सुरक्षित और सक्षम बनाने के लिए एआई टूल्स का उपयोग करना**

💪 इंटरनेट उपयोगकर्ताओं को सशक्त बनाने के लिए अलर्ट्स और टूल्स

व्यवसाय अपनी ऐप्स और डिजिटल सेवाओं में डिजाइन फीचर्स को एकीकृत करते हैं, जो आपको अपने डेटा पर नज़र रखने, गोपनीयता और सुरक्षा सेटिंग्स को समायोजित करने और सूचित रहने में मदद करते हैं।

इससे आपको यह जांचने और नियंत्रित करने में मदद मिलती है कि आपकी जानकारी तीसरे पक्ष के साथ कैसे साझा की जा रही है, आप यह तय कर सकते हैं कि कौन सी जानकारी साझा की जाए और कौन सी निजी रखी जाए और संदिग्ध गतिविधि के बारे में सूचित किया जा सकता है, जैसे कि कोई आपके खाते तक पहुंचने का प्रयास कर रहा हो।

भारतीय प्राधिकरणों की सुनें

- **आवर्ती भुगतानों के लिए लेन-देन सूचनाएँ:** भारतीय रिजर्व बैंक (RBI) ने बैंकों को आवर्ती भुगतानों जैसे कि सब्सक्रिप्शन या व्यवस्थित निवेश योजनाओं (SIP) की प्रक्रिया करने से कम से कम 24 घंटे पहले सूचनाएँ भेजने का आदेश दिया है।
- **विस्तृत गोपनीयता सूचनाएँ:** इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) व्यवसायों से यह अपेक्षा करता है कि वे स्पष्ट रूप से बताएं कि वे आपसे कौन सा व्यक्तिगत डेटा एकत्र कर रहे हैं और उस डेटा के संग्रह का उद्देश्य क्या है।

.. जारी

- **स्पैम/पेस्की कॉल्स से निपटने के लिए TRAI के नियम:** TRAI ने कंपनियों को बल्क में ऐप्स और वेबसाइटों के लिंक वाले टेक्स्ट मैसेज भेजने की अनुमति दी है, बशर्ते कि वे अपनी सामग्री को टेलीकॉम सेवा प्रदाताओं के साथ पंजीकरण करवाएं। इससे यह सुनिश्चित होता है कि केवल सत्यापित और व्हाइटलिस्टेड लिंक और अटैचमेंट्स सार्वजनिक रूप से प्रचार मैसेजों में वितरित किए जाएं।
- **डार्क पैटर्न्स से सुरक्षा:** उपभोक्ता मामलों के विभाग (DoCA) के अनुसार, व्यवसायों द्वारा उपयोग किए गए गुमराह करने वाले डिज़ाइन पैटर्न को अनुचित व्यापार अभ्यास के रूप में देखा जा सकता है।
    - गुमराह करने वाले डिज़ाइनों के उदाहरण हैं: ऐसे ऐप्स जिनमें जटिल यूज़र इंटरफेस (UI) होता है, जिससे आवर्ती लेन-देन को रद्द करना कठिन हो जाता है या ऐसे ऐप्स जो चेकआउट से पहले छिपा हुआ शुल्क और अतिरिक्त शुल्क जोड़ लेते हैं।
    - अगर आप ऐसे फ्रॉड डिज़ाइन देखे, तो आप 1915 पर कॉल करके या INGRAM पोर्टल (www.consumerhelpline.gov.in/user/) पर जाकर DoCA में शिकायत कर सकते हैं।

💪 इंटरनेट उपयोगकर्ताओं को सशक्त बनाने के उपकरण

META

प्राइवेसी सेंटर

आप Facebook, Instagram, Messenger और अन्य Meta उत्पादों पर अपनी प्राइवेसी को नियंत्रित और प्रबंधित करने के लिए सेटिंग्स को अनुकूलित कर सकते हैं।

WhatsApp प्राइवेसी कंट्रोल्स

आप WhatsApp पर अपनी प्रोफाइल फोटो, लास्ट सीन विवरण किसे दिखाना है, इसे कस्टमाइज कर सकते हैं। साथ ही, आप चैट्स को लॉक करने की सुविधा का उपयोग कर सकते हैं।

TRUECALLER

स्पैम / फ्रॉडअलर्ट

Truecaller संदिग्ध कॉल्स को "स्पैम" या "फ्रॉड अलर्ट" जैसे लेबल्स के साथ चिन्हित करता है।

व्यावसायिक कॉलर आईडी

Truecaller व्यावसायिक कॉल्स में एक टैम्पर-प्रूफ नाम, हरा बैज और लोगो जोड़ता है, जो कि स्कैमर से बचाता है और आपको असली कॉलर्स और स्कैमर में अंतर करने में मदद करता है।

MICROSOFT

Copilot नियंत्रण

आप अपनी प्राथमिकताएँ सेट कर सकते हैं, डेटा देख सकते हैं, संपादित कर सकते हैं या हटा सकते हैं और Copilot पर बातचीत की हिस्ट्री का प्रबंधन कर सकते हैं।

Skype पर गोपनीयता और रिपोर्टिंग

आप Skype पर हानिकारक मैसेजों की रिपोर्ट कर सकते हैं, संदिग्ध मैसेजों को ब्लॉक या रिपोर्ट कर सकते हैं।

🔐 डिजाइन से सुरक्षा

'डिजाइन से सुरक्षा' का मतलब है तकनीकी उत्पादों को इस तरह से बनाना कि आपको अपने डिवाइस, डेटा और नेटवर्क इन्फ्रास्ट्रक्चर को सुरक्षित करने के लिए अतिरिक्त कदम न उठाने पड़े।

डिजाइन द्वारा उत्पादों को सुरक्षित बनाने के लिए शुरू से ही गोपनीयता, अखंडता और उपलब्धता पर ध्यान देना आवश्यक है।

गोपनीयता

संवेदनशील व्यक्तिगत डेटा जैसे पासवर्ड को निजी रखने के लिए एन्क्रिप्शन उपकरणों का उपयोग करना।

अखंडता

डेटा की सेंधमारी और अनधिकृत पहुंच को रोकने के लिए तकनीकी उपायों का उपयोग।

उपलब्धता

डेटा बैकअप्स की उपलब्धता और सेंधमारी के बाद डेटा पुनर्प्राप्ति योजना का सुनिश्चित करना।

गोपनीयता बढ़ाने वाली तकनीकें (PET) प्रमुख सुरक्षा उपकरण हैं जो आपके डेटा को अनधिकृत पहुँच से बचाते हैं। एन्क्रिप्शन, अनामीकरण और सुरक्षित संगणना जैसी तकनीकें आमतौर पर इस्तेमाल की जाने वाली PET हैं। वे डेटा उपयोगिता की आवश्यकता और गोपनीयता की आवश्यकता के बीच संतुलन बनाने में मदद करते हैं।

यह तकनीकें डेटा की उपयोगिता और गोपनीयता की आवश्यकता के बीच संतुलन बनाए रखने में मदद करती हैं।

भारतीय प्राधिकारियों की सुनें

- **क्लाउड सेवाएँ:** MeitY व्यवसायों को सुरक्षा उपाय लागू करने की अनुशंसा करता है जैसे कि 'फुल डिस्क एन्क्रिप्शन' और 'फॉर्मेट प्रिजर्विंग एन्क्रिप्शन' ताकि जानकारी की सुरक्षा की जा सके, साथ ही डेटा की संरचना (जैसे क्रेडिट कार्ड नंबर) बनी रहे।

- **वित्तीय सेवाएँ:** RBI बैंकों और वित्तीय कंपनियों से अपेक्षाएँ करता है कि वे:
  - डेटा छिपाएँ: संवेदनशील जानकारी के हिस्सों को छिपाएं, जैसे कि केवल कार्ड के आखिरी चार अंक दिखाना।
  - मल्टी-फैक्टर ऑथेंटिकेशन का उपयोग करें ताकि सुरक्षा की एक अतिरिक्त परत जोड़ी जा सके, जैसे कि ऑनलाइन कार्ड भुगतान के लिए CVV + OTP.
  - मजबूत एन्क्रिप्शन अपनाएं: ऐसे उपकरणों का उपयोग करें जो हैकर्स के लिए डेटा को पढ़ना चुनौतीपूर्ण बना दें।

🔐 डिज़ाइन समाधान क्रियान्वयन से सुरक्षा

MICROSOFT

Zero-Trust मॉडल

Microsoft का Zero Trust मॉडल हर डेटा एक्सेस अनुरोध को इस तरह से सत्यापित, प्रमाणीकरण और एन्क्रिप्ट करता है जैसे वह एक असुरक्षित ओपन नेटवर्क से उत्पन्न हुआ हो।

सुरक्षित भविष्य की पहल

Microsoft उत्पादों में सुरक्षा डिफ़ॉल्ट रूप से सक्षम और लागू की जाती है, जिन्हें अतिरिक्त प्रयास की आवश्यकता नहीं होती और ये वैकल्पिक नहीं होते हैं।

AIRTEL

स्पैम फ़िल्टरिंग

Airtel उपयोग पैटर्न, SMS की आवृत्ति, कॉल की अवधि आदि जैसी जानकारी को प्रोसेस करता है ताकि स्पैम कॉल्स और मैसेजों की पहचान की जा सके।

चेहरे का मिलान

Airtel Payments Bank सुरक्षा एल्गोरिदम का उपयोग करता है जो पहचान की चोरी या फ्रॉड का खतरा महसूस होने पर सेल्फी-आधारित चेहरे की पहचान सत्यापन सक्रिय कर देता है।

🤝 उपयोगकर्ताओं के लिए शिकायत निवारण चैनल

स्पष्ट और सरल शिकायत निवारण तंत्र की मदद से डिजिटल सेवाओं के उपयोगकर्ता जैसे कि आप डिजिटल व्यवसायों के साथ जुड़ने के दौरान आने वाली समस्याओं के लिए समय पर समाधान प्राप्त कर सकते हैं। व्यवसाय आपकी ई-कॉमर्स खरीद की डिलीवरी में देरी या कैब की सवारी के भुगतान में समस्याओं जैसे मुद्दों को शिकायत निवारण चैनलों के माध्यम से संबोधित करते हैं।

शिकायत निवारण के लिए तंत्र

- **संचार साथी:** दूरसंचार विभाग (DoT) आपको टेलीकॉम फ्रॉड से निपटने के लिए विभिन्न पहलों की पेशकश करता है। संचार साथी पहल आपको निम्नलिखित की अनुमति देती है:
  - शक के आधार पर फ्रॉडसंचारों की रिपोर्ट करें (www.sancharsaathi.gov.in/sfc/ पर जाएं);
  - आपके नाम पर जारी सभी मोबाइल कनेक्शनों की पहचान और प्रबंधन करें;
  - खोए हुए/चोरी हुए मोबाइल हैंडसेट की रिपोर्ट करें ताकि उन्हें ब्लॉक, ट्रेस और रिकवर किया जा सके।

- **वित्तीय क्षेत्र निगरानी:** भारतीय रिजर्व बैंक (RBI) की एकीकृत ओम्बड्समैन योजना एक केंद्रीय शिकायत निवारण तंत्र प्रदान करती है, जिससे आप बैंक, भुगतान सेवा प्रदाताओं, क्रेडिट ब्यूरो और अन्य वित्तीय संस्थानों के खिलाफ शिकायत कर सकते हैं।

- **उपभोक्ता हेल्पलाइन:** उपभोक्ता मामले मंत्रालय (DoCA) आपको व्यापारों और सेवा प्रदाताओं के खिलाफ शिकायत निवारण के लिए कई चैनल प्रदान करता है: जैसे कि व्हाट्सएप-इंटीग्रेटेड हेल्पलाइन नंबर (8800001915), राष्ट्रीय उपभोक्ता हेल्पलाइन वेब पोर्टल (www.consumerhelpline.gov.in), और UMANG ऐप।

- **मध्यस्थता दिशानिर्देश:** MeitY डिजिटल प्लेटफ़ॉर्म जैसे सोशल मीडिया और गेमिंग कंपनियों से अपेक्षा रखता है कि वे शिकायत निवारण तंत्र स्थापित करें और उपभोक्ता शिकायतों का समयबद्ध तरीके से समाधान करें। यदि आप कंपनी के शिकायत निवारण प्रक्रिया से संतुष्ट नहीं हैं, तो आप सरकार द्वारा नियुक्त शिकायत अपीलीय समिति (GAC) में एक ई-शिकायत दर्ज कर सकते हैं।

🤝 शिकायत निवारण चैनल्स का कार्यान्वयन

VODAFONE IDEA (VI)

विशेषीकृत हेल्पलाइन
Vi आपके विभिन्न आवश्यकताओं के आधार पर विशेषीकृत हेल्पलाइन्स प्रदान करता है, जैसे कि मोबाइल नंबर पोर्टेबिलिटी, डेटा सक्रियण, आदि।

My VI ऐप
MyVi ऐप आपको विभिन्न उत्पाद और सुरक्षा विकल्पों तक पहुंच प्रदान करता है। आप डू-नॉट-डिस्टर्ब (DND) सुविधा का चयन कर सकते हैं, टेलीमार्केटर्स के खिलाफ शिकायत कर सकते हैं और ग्राहक सेवा अधिकारियों से सेवा अनुरोध और शिकायतें कर सकते हैं।

AIRTEL

Airtel थैंक्स ऐप
Airtel थैंक्स ऐप आपको अवांछित नंबरों को प्रबंधित/ब्लॉक करने, हानिकारक गतिविधि की रिपोर्ट करने और विपणन मैसेजों से बचने के लिए डू-नॉट-डिस्टर्ब (DND) सेवा का चयन करने की अनुमति देता है।

दो-स्तरीय अपीलीय प्राधिकरण
यदि आपको समाधान से असंतोष होता है, तो आप 30 दिनों के भीतर सेवा क्षेत्र आधारित अपीलीय प्राधिकरण के पास अपील कर सकते हैं।

🤖 उपयोगकर्ताओं की सुरक्षा और सशक्तिकरण के लिए AI का उपयोग

AI (आर्टिफिशियल इंटेलिजेंस) एक एल्गोरिदम-आधारित निर्णय लेने वाली प्रणाली है। यह ऐसे कार्य कर सकता है जिनके लिए आमतौर पर मानव बुद्धि की आवश्यकता होती है। उदाहरण के लिए, प्राकृतिक भाषा-आधारित प्रसंस्करण एल्गोरिदम हेरफेर की गई सामग्री का पता लगाने और असामान्य गतिविधियों या लेनदेन को चिह्नित करने के लिए टेक्स्ट, छवि और वीडियो सामग्री का विश्लेषण करते हैं।

भारतीय अधिकारियों की सुनें

- **स्पैम फ़िल्टरिंग:** TRAI सभी दूरसंचार प्रदाताओं (जैसे Airtel और Vodafone) को AI का उपयोग करके स्पैम/परेशान करने वाली कॉल्स को फ़िल्टर करना अनिवार्य करता है।
- **म्यूल खाता निगरानी:** RBI बैंकों से यह अनुरोध करता है कि वे अपने सहायक संगठन RBI इनोवेशन हब (RBIH) द्वारा बनाए गए AI मॉडल के साथ सहयोग करें, जो बैंकों और वित्तीय संस्थाओं को फ्रॉड करने वालों और मनी लॉन्ड्रर्स द्वारा उपयोग किए जा रहे म्यूल खातों का पता लगाने में मदद करता है।

.. जारी

- **अंतर्राष्ट्रीय इनकमिंग स्पूफ कॉल्स की रोकथाम प्रणाली:** DoT ने एक प्रणाली लागू की है जो ऐसी अंतर्राष्ट्रीय स्पैम कॉल का पता लगाती है और उन्हें ब्लॉक करती है, जो भारत से उत्पन्न हुई प्रतीत होती हैं। इसके परिणामस्वरूप, अंतर्राष्ट्रीय स्कैमर जो कॉलर विवरण को इस तरह से संशोधित करते हैं कि भारतीय नंबर "(+91 XXXXX XXXXX)" दिखाई दे, उन्हें स्वचालित रूप से पहचान कर ब्लॉक कर दिया जाता है।

AI समाधान का कार्यान्वयन

AIRTEL

हानिकारक मैसेज की पहचान
Airtel के AI टूल्स एक टेक्स्ट मैसेज के विभिन्न पहलुओं की जांच करते हैं, जैसे कि क्या साझा किया गया लिंक ब्लैकलिस्टेड है या नहीं, ताकि मैसेज को संदिग्ध घोषित किया जा सके।

डायनेमिक फिल्टरिंग
Airtel अपने ग्राहकों को हानिकारक और दुर्भावनापूर्ण वेबसाइटों से बचाने के लिए संबंधित सरकारी एजेंसियों के साथ साझेदारी में काम करता है।

TRUECALLER

SMS फ्रॉड सुरक्षा
Truecaller की AI-संचालित SMS फ्रॉड सुरक्षा सक्रिय रूप से फ्रॉड मैसेजों का पता लगाती है और उन्हें ब्लॉक करती है, संदेहास्पद लिंक को स्वचालित रूप से अक्षम कर देती है।

खोज संदर्भ
खोज संदर्भ वास्तविक समय में संदिग्ध गतिविधियों को चिह्नित करता है, जैसे कि फोन नंबरों के लिए बार-बार नाम बदलना—जो अक्सर फ्रॉड या स्कैम का संकेत होता है, जिससे आपको यह निर्णय लेने में मदद मिलती है कि कौन से कॉल का उत्तर देना है।

META

एंड-टू-एंड एन्क्रिप्शन
WhatsApp यह सुनिश्चित करता है कि केवल प्रेषक और प्राप्तकर्ता ही मैसेजों, कॉल्स, फ़ोटो और वीडियो को एक्सेस कर सकते हैं।

डेटा संग्रहण सीमित करता है
WhatsApp केवल आवश्यक डेटा जैसे फोन नंबरों को स्टोर करता है और डिफ़ॉल्ट रूप से मैसेज सामग्री या स्थान डेटा को स्टोर करने से बचता है।

SAFER INTERNET INDIA

विजिट करे: www.saferinternetindia.com
secretariat@saferinternetindia.com पार हमें लिखें

Safer Internet India
@saferinternetindia
SaferInternetIN
@SaferInternetIndia