SAFER INTERNET INDIA

वापरकर्ता सुरक्षा मार्गदर्शिका

वापरकर्ता सुरक्षा मार्गदर्शिका

फेब्रुवारी 2025

कृतज्ञता

अतिश नंदी, लालांतिका अरविंद, मेघना बल, समृद्धी कुमार, शिवा भार्गवी नोरी, सृष्टी जोशी आणि सेफर इंटरनेट इंडिया आघाडीचे सदस्य

आत काय आहे?

सर्वसाधारण स्कॅम्स आणि घोटाळे

तुम्हाला सतर्क आणि जागरूक ठेवण्यासाठी आम्ही स्कॅमर्सद्वारे वापरल्या जाणाऱ्या विविध युक्त्या उलगडून सांगतो

सुरक्षित इंटरनेट वापरण्याच्या टिप्स

आजच्या डिजिटल युगात सुरक्षित राहण्यासाठी आवश्यक असलेल्या गोष्टींची आणि टाळावयाच्या गोष्टींची यादी आम्ही तयार केली आहे

विश्वास आणि सुरक्षिततेसाठी मूलभूत आधारस्तंभ

आम्ही ऑनलाइन विश्वास आणि सुरक्षितता वाढवण्यासाठी चार मूलभूत आधारस्तंभांवर चर्चा करतो

इंडस्ट्रीतील सर्वोत्तम पद्धती

आम्ही अग्रगण्य तंत्रज्ञान कंपन्यांच्या सर्वोत्तम पद्धतींबद्दल चर्चा करतो ज्यामुळे आपल्या सर्वांसाठी इंटरनेट थोडे सुरक्षित होते

अनुक्रमणिका

परिचय	06
मुलभूतगोष्टी	07
सर्व साधारण फ्रॉड आणि स्कॅम्स	11
AI व्हॉइस स्कॅम	11
डेटिंग ॲप स्कॅम	12
डिजिटल अरेस्ट स्कॅम	14
बनावट गुंतवणूक / ट्रेडिंग ॲप स्कॅम	16
बनावट नोकरी ऑफर स्कॅम	18
बनावट लिंक / QR कोड स्कॅम	21
बनावट कर्ज ॲप स्कॅम	23
बनावट मोबाइल रिचार्ज स्कॅम	25
पार्सल डिलिव्हरी स्कॅम	26
भेसळयुक्त मालवेअर स्कॅम	28
टेकनिकल सपोर्ट स्कॅम	29
OTP स्कॅम	31
रिवॉर्ड स्कॅम	33
SIM स्वॅपिंग / SIM क्लोनिंग स्कॅम	34
बनावट ओळख स्कॅम	35
स्किमिंग मशीन फ्रॉड	36
बनावट कल्याणकारी योजना स्कॅम	37
काय करावे काय करू नये	38
प्रो टिप्स	39
इंडस्ट्रीतील सर्वोत्तम पद्धती वापरकर्त्यांच्या सुरक्षिततेसाठी	41

SAFER INTERNET INDIA

प्रिय वाचक

सेफर इंटरनेट इंडिया (SII) ही भारतात वेगाने वाढणाऱ्या डिजिटल अर्थव्यवस्थेच्या विविध विभागांमध्ये पसरलेल्या क्षेत्रांतील समान विचारधारेच्या कंपन्यांची एक संघटना आहे.

ऑनलाइन स्कॅम्स, सायबर धोके आणि डेटा चोरीच्या वाढत्या घटनांचा सामना करण्यासाठी SII तातडीच्या सामाजिक गरजेला प्रतिसाद देते. आम्ही विविध क्षेत्रातील तज्ञांना एकत्र आणतो एकत्रित येऊन वापरकर्त्याचा विश्वास आणि सुरक्षितता मजबूत करण्यासाठी प्रयत्न करतो.

तुमच्यासारख्या इंटरनेट युजर्सना ऑनलाइन फ्रॉड आणि स्कॅमपासून स्वत:चे रक्षण करता यावे यासाठी आम्ही ही मार्गदर्शिका लिहिली आहे.

या मार्गदर्शिकेत सामान्य फ्रॉड आणि स्कॅमची रचना सविस्तर दिली आहे, तसेच
इंटरनेट वापरकर्त्यांना इंटरनेट सर्फिंग करण्यासाठी आणि सुरक्षित आणि सुरक्षित मार्गाने डिजिटल व्यवसायांशी संलग्न होण्यासाठी काय करावे आणि काय करू नये याची शिफारस करते. ऑनलाइन जागा सुरक्षित करण्यासाठी व्यवसाय आणि धोरणकर्त्यांनी उचललेल्या पावलांनाही मान्यता देण्यात आली आहे.

सेफर इंटरनेट इंडिया वाचल्याबद्दल धन्यवाद

परिचय

डिजिटल स्पेस आपल्या आयुष्याच्या प्रत्येक पैलूला स्पर्श करते. भारतातील 90 कोटीपेक्षा जास्त इंटरनेट वापरकर्ते नियमितपणे घरगुती जीवनावश्यक वस्तूंपासून ते लक्झरी वस्तू, करमणूक सब्सक्रिप्शन आणि अगदी वित्तीय सेवांपर्यंत सर्व काही काम, शिकण्यासाठी आणि खरेदी करण्यासाठी ऑनलाइन जातात.

तथापि, वापरकर्त्यांनी ते ऑनलाइन कोणाशी संवाद साधतात आणि ते ऑनलाइन काय खरेदी करतात याबद्दल सावधगिरी बाळगणे आवश्यक आहे. ऑनलाईन जगात अनेक ऑफर्स आणि डील्स असतात ज्या खूप आकर्षक वाटतात, पण बहुतांश वेळा त्या खऱ्या नसतात. 2024 च्या पहिल्या नऊ महिन्यांत ऑनलाइन स्कॅम्समुळे भारतीयांचे सुमारे 11,333 कोटी रुपयांचे नुकसान झाले आहे!

फ्रॉडस्टर आणि स्कॅमर अत्यंत चलाख, संधीसाधू आणि परिस्थितीनुसार बदलणारे असतात. दुर्दैवाने, हे लोक अधिकाधिक चतुर होत चालले आहेत, तर अनेक नागरिकांकडे मूलभूत डिजिटल कौशल्यांचा अभाव आहे. भारत सरकारच्या (GoI) 2022-23 च्या सर्वेक्षणानुसार भारतातील जवळपास निम्म्या इंटरनेट वापरकर्त्यांना ईमेल कसे पाठवायचे हे माहित नव्हते आणि केवळ 38 टक्के लोक ऑनलाइन बँकिंग व्यवहार करू शकले. डिजिटल कौशल्यांच्या बाबतीत ग्रामीण भारताची स्थिती शहरी भारतापेक्षा वाईट आहे आणि वेगवेगळ्या लिंगांमध्ये मोठ्या असमानता आहेत. सारांश असा की, स्कॅम्स हा संपूर्ण समाजासमोरील एक मोठे आव्हान आहे. भारतातील अनेक लोक फसवणुकीच्या धोक्यात आहेत, त्यामुळे त्यांना ऑनलाइन सुरक्षित राहण्यासाठी कौशल्ये आणि जागरूकता मिळणे आवश्यक आहे.

ऑनलाइन स्कॅमपासून भारतीय इंटरनेट वापरकर्त्यांचे संरक्षण करण्याची गरज भारत सरकारने ओळखली आहे. गृह मंत्रालय (MHA) आणि इलेक्ट्रॉनिक्स व माहिती तंत्रज्ञान मंत्रालय, तसेच इंडियन सायबर क्राईम कोऑर्डिनेशन सेंटर (I4C) आणि इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-in) यांसारख्या विशेष संस्थांसोबत मिळून, फ्रॉड आणि स्कॅमची चौकशी करून ती थांबवण्यासाठी आणि ऑनलाइन सुरक्षिततेशी संबंधित समस्या सोडवण्यासाठी सतत कार्यरत आहेत. रिझर्व्ह बँक ऑफ इंडिया (आरबीआय) आणि टेलिकॉम रेग्युलेटरी अथॉरिटी ऑफ इंडिया (TRAI) सारखे नियामक देखील भारतीयांच्या संरक्षणासाठी तंत्रज्ञानाचा वापर करत आहेत, मग ते मनी लॉन्ड्रिंगमध्ये वापरल्या जाणार्या खच्चर खात्यांचा शोध घेण्यासाठी AI (Artificial Intelligence) प्रणाली असो किंवा फसवणूक / पेस्की कॉलमर्यादित करण्यासाठी टेलिमार्केटर्सची वितरित लेजर टेक्नॉलॉजी (DLT) आधारित नोंदणी असो, तसेच त्यांच्या डोमेनमध्ये नवीन नियम लागू केले जातील.

परंतु ऑनलाइन सुरक्षिततेच्या समस्येचा व्यापक प्रमाणावर विचार करता, आपल्याला सर्वांचा सहभाग आवश्यक आहे - वापरकर्त्यांना ऑनलाइन सुरक्षित ठेवण्यासाठी सर्वांनी एकत्र काम केले पाहिजे.

मूलभूत गोष्टी

ऑनलाइन सुरक्षित राहणे पूर्वीपेक्षा जास्त महत्वाचे आहे. या विभागात आम्ही आपल्याला काही मूलभूत अटी आणि संकल्पनांशी परिचित करतो, जेणेकरून आपण डिजिटल स्पेसनेव्हिगेट करू शकता चांगले.

वैयक्तिक माहिती

वैयक्तिक माहिती म्हणजे तुमच्याबद्दलची कोणतीही माहिती जी तुमची ओळख पटवू शकते. यामध्ये तुमचे नाव, पत्ता, फोन नंबर, ईमेल, जन्मतारीख किंवा बँक तपशील यांसारखी माहिती समाविष्ट आहे. स्कॅमर अनेकदा ही माहिती चोरून तुमच्या नावाने बनावट ओळख तयार करण्याचा किंवा तुमच्या खात्यांमध्ये प्रवेश मिळवण्याचा प्रयत्न करतात.

संवेदनशील वैयक्तिक माहिती

संवेदनशील वैयक्तिक माहिती ही आपल्याबद्दलची खाजगी माहिती आहे ज्यास अतिरिक्त संरक्षणाची आवश्यकता आहे कारण जर ती चुकीच्या हातात पडली तर त्यांचा गैरवापर केला जाऊ शकतो. यामध्ये तुमचे पासवर्ड, बँक खाते क्रमांक, क्रेडिट कार्ड अशा गोष्टींचा समावेश आहे तपशील, वैद्यकीय नोंदी किंवा सरकारी आयडी क्रमांक (जसे की आधार किंवा PAN). आपली ओळख टिकवून ठेवण्यासाठी या माहितीचे संरक्षण करणे खूप महत्वाचे आहे आणि आर्थिक स्थिती सुरक्षित आहे. अशी माहिती कोणासोबत शेअर करत आहात याबाबत खूप काळजी घ्या.

फ्रॉड

ऑनलाइन फ्रॉड म्हणजे कोणी तरी खोटे बोलून किंवा फसवणूक करून बेकायदेशीररित्या पैसा घेणे. किंवा इंटरनेटच्या माध्यमातून संवेदनशील माहिती. यामध्ये अकाऊंट हॅक करणे, पेमेंटडिटेल्स चोरणे किंवा लोकांना फसवण्यासाठी बनावट वेबसाइट तयार करणे यासारख्या गोष्टींचा समावेश आहे.

स्कॅम

ऑनलाइन स्कॅम म्हणजे जेव्हा कोणी इंटरनेटवर पैसे, वैयक्तिक माहिती किंवा संवेदनशील डेटा चोरी करण्यासाठी आपल्याला फसवते. स्कॅमर अनेकदा विश्वासार्ह असल्याचे भासवतात, बनावट सौदे देतात, अधिकारी असल्याचे भासवतात किंवा संदेश पाठवतात की खरे वाटतील अशा पद्धतीने तयार केलेले असतात.

ऑनलाइन स्कॅम हा ऑनलाइन फ्रॉडचा एक प्रकार आहे, परंतु सर्व फ्रॉड हे स्कॅम नसतात. स्कॅममध्ये अनेकदा लोकांना पैसे किंवा माहिती स्वेच्छेने देण्यासाठी फसवण्याचा प्रयत्न केला जातो (उदा. बनावट बक्षिसे किंवा नोकरीच्या ऑफर). दुसरीकडे, ऑनलाइन फ्रॉडमध्ये याचा समावेश होऊ शकतो ओळख चोरी किंवा हॅकिंगसारख्या कृती, जिथे पीडितव्यक्तीला लगेच लक्ष्य केले गेले आहे याची जाणीवदेखील नसते.

थोडक्यात, स्कॅम लोकांना फसवण्यावर अवलंबून असतात, तर फ्रॉडमध्ये माहिती चोरणे किंवा गैरवापर करणे यासारख्या व्यापक पद्धतींचा समावेश असतो. म्हणूनच वापरकर्त्यांनी केवळ ऑनलाइन लोकांशी संवाद साधतानाच नव्हे तर वेबसाइटवर जाताना किंवा ॲप्स डाउनलोड करण्याचा प्रयत्न करताना देखील सतर्क राहणे आवश्यक आहे.

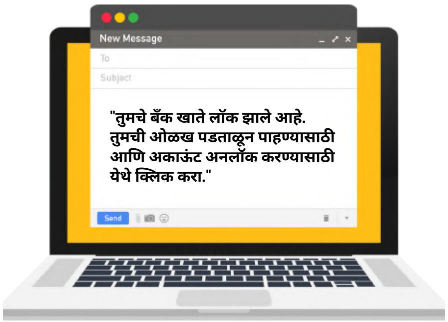
हॅक

हॅक म्हणजे जेव्हा एखादी व्यक्ती माहिती चोरण्याची, नुकसान करण्याची किंवा नियंत्रण घेण्याची परवानगी न घेता संगणक, खाते किंवा नेटवर्कमध्ये प्रवेश करते. हॅकर्स अनेकदा कमतरता शोधण्यासाठी आणि अनधिकृत प्रवेश मिळवण्यासाठी विशेष साधने किंवा युक्त्या वापरतात.

फिशिंग

फिशिंग ही एक युक्ती आहे जी स्कॅमर्सद्वारे पासवर्ड, बँक तपशील किंवा क्रेडिट कार्ड नंबर सारख्या आपली वैयक्तिक माहिती चोरण्यासाठी वापरली जाते. ते सहसा आपली बँक, कंपनी किंवा सरकारी एजन्सी सारख्या आपल्या विश्वासाची व्यक्ती असल्याचे भासवतात जेणेकरून आपल्याकडून बनावट लिंकवर क्लिक केले जाईल किंवा संवेदनशील माहिती शेअर केली जाईल.

फिशिंग अटॅक अनेक माध्यमातून होऊ शकतात. SMS/मेसेजिंग ॲप्सच्या माध्यमातून होणाऱ्या हल्ल्यांना स्मिशिंग अटॅक म्हणतात, तर फोन कॉलद्वारे होणाऱ्या हल्ल्यांना व्हिशिंग (व्हॉईस-फिशिंग) अटॅक म्हणतात.



उदाहरण:

आपल्याला एक ईमेल येतो जो म्हणतो:

"तुमचे बँक खाते लॉक झाले आहे. तुमची ओळख पडताळून पाहण्यासाठी आणि अकाऊंट अनलॉक करण्यासाठी येथे क्लिक करा."

ही लिंक तुम्हाला बनावट वेबसाइटवर घेऊन जाते, जी तुमच्या बँकेच्या साइटसारखी दिसते, पण तुम्ही टाकलेली कोणतीही माहिती थेट स्कॅमरकडे जाते.

फिशिंग ईमेलचे आणखी एक उदाहरण म्हणजे जेव्हा स्कॅमर एखाद्या व्यक्तीच्या संस्थेत सहकारी असल्याचे भासवतो आणि त्यांना ईमेल पाठवून पैसे विचारतो. अशा वेळी कृपया कोणतेही पैसे ट्रान्सफर करू नका आणि आपल्या सहकाऱ्याला (जरी तो तुमचा बॉस असला तरी) फोन करून त्यांची ओळख पटवून द्या. आणखी एक टीप म्हणजे ईमेलची पडताळणी करा. थोडक्यात, ईमेल आपल्या संस्थेच्या नावाशी किंवा आपल्या सहकाऱ्याच्या प्रत्यक्ष कामाच्या ईमेलशी जुळत नसेल.

मालवेअर

मालवेअर हे हानिकारक सॉफ्टवेअर आहे, जे आपल्या परवानगीशिवाय आपला संगणक, फोन किंवा इतर उपकरणेला नुकसान करण्यासाठी, माहिती चोरण्यासाठी किंवा नियंत्रण मिळवण्यासाठी तयार केले जाते. हे बनावट ॲप्स, ईमेल अटॅचमेंट (ईमेलसह असलेल्या फाइल्स) किंवा वेबसाइट्समध्ये लपवू शकते आणि आपली माहिती चोरणे किंवा आपली गती कमी करणे यासारख्या समस्या उद्भवू शकते.

आर्टिफिशियल इंटेलिजन्स

AI हे तंत्रज्ञान आहे जे डेटाचे विश्लेषण करू शकते, मानवी वर्तनाची नक्कल करू शकते आणि तयार करू शकते खऱ्यासारखा कंटेंट, जसं मेसेजेस किंवा आवाज. स्कॅमर्स AIचा वापर त्यांच्या युक्त्या अधिक खात्रीशीर बनविण्यासाठी करू शकतात, जसे की वास्तविक वाटणारे बनावट संदेश तयार करणे, एखाद्याच्या आवाजाची नक्कल करणे किंवा पैसे किंवा वैयक्तिक माहिती शेअर करण्यासाठी लोकांना फसवण्यासाठी वैयक्तिकृत ईमेल पाठविणे. AI स्कॅमर्सला पीडितांना अधिक प्रभावीपणे लक्ष्य करण्यात मदत करते आणि त्यांचे स्कॅम्स शोधणे कठीण करते.

स्पॅम

स्पॅम म्हणजे नको असलेला किंवा निरुपयोगी संवाद, जो सहसा फोन कॉल, ईमेल, मेसेज किंवा सोशल मीडियाद्वारे केला जातो. हे बर्याचदा गोष्टींची जाहिरात करण्यासाठी वापरले जाते, परंतु कधीकधी आपली माहिती किंवा पैसे चोरण्याच्या प्रयत्नाचा हा एक भाग आहे.

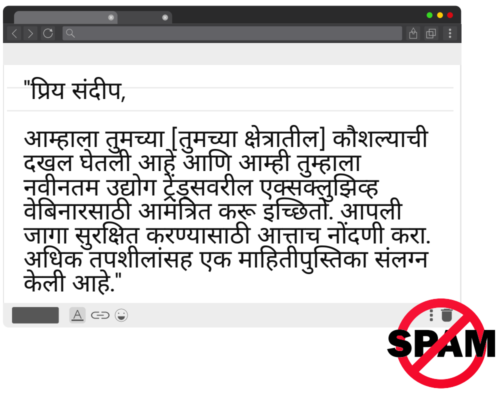
उदाहरण:

"अभिनंदन! आपण $1,000 गिफ्ट कार्ड जिंकले आहे! आत्ताच बक्षीस मिळवण्यासाठी येथे क्लिक करा."

हा ईमेल सहसा बनावट असतो आणि दुव्यावर क्लिक केल्याने स्कॅम होऊ शकते किंवा हानिकारक सॉफ्टवेअरसह आपल्या डिव्हाइसला संक्रमित केले जाऊ शकते.

स्पॅम आता अधिक स्मार्ट होत आहे आणि तो तुमच्या व्यवसाय, प्रोफेशन किंवा कामाशी संबंधित असलेल्या संवादासारखा दिसेल अशा प्रकारे तयार केला जाऊ शकतो.

तुमच्या प्रोफेशनसाठी खास तयार केलेल्या स्मार्ट स्पॅमचे एक उदाहरण असे असू शकते:



ईमेल प्रोफेशनल आणि तुमच्या कामाशी संबंधित वाटतो, पण त्या लिंकवर क्लिक केल्यास ती फिशिंग साइट असू शकते, आणि संलग्न फाइलमध्ये मालवेअर असण्याची शक्यता असते. या प्रकारचा स्पॅम फसवण्यासाठी तयार केला जातो प्रोफेशनल्सना फसवण्यासाठी तो वैध आणि वैयक्तिक वाटेल अशा पद्धतीने तयार केला जातो.

सामान्य फ्रॉड आणि स्कॅम्स

स्कॅम # 1 AI आवाज स्कॅम

ते काय आहे?

AI व्हॉइस स्कॅम म्हणजे जेव्हा स्कॅमर्स आपल्याला फसवण्यासाठी कुटुंबातील सदस्य किंवा बॉस सारख्या एखाद्याच्या आवाजाची कॉपी करण्यासाठी AI चा वापर करतात. आणीबाणी असल्याचे भासवून ते तुम्हाला फोन करून पैशांची मागणी करू शकतात किंवा माहिती चोरण्याच्या खोट्या सूचना देऊ शकतात. कारण आवाज खऱ्यासारखा वाटतो, तो खूप विश्वासार्ह वाटू शकतो आणि ओळखणे अवघड होऊ शकते.

हे कसे कार्य करते

स्कॅमर्स सोशल मीडिया, व्हिडिओ किंवा व्हॉईसमेलवरून एखाद्याच्या आवाजाचे रेकॉर्डिंग शोधतात. AI साधनांचा वापर करून, ते त्या व्यक्तीचा आवाज वास्तविक आणि नैसर्गिक वाटण्यासाठी कॉपी करतात.

स्कॅमर बनावट आवाजाचा वापर करून आपल्याला कॉल करतो आणि मित्र, कुटुंबातील सदस्य किंवा बॉस सारख्या आपल्या ओळखीची व्यक्ती असल्याचे भासवतो. आणीबाणी असल्याचा दावा करणे आणि पैसे, गिफ्ट कार्ड किंवा संवेदनशील माहिती मागणे यासारखे तातडीचे वातावरण ते निर्माण करतात.

जर आपण त्यात अडकलात तर ते आपले पैसे किंवा वैयक्तिक माहिती चोरण्यासाठी आपण त्यांना जे देता त्याचा वापर करतात.

- तातडीच्या मागण्यांपासून सावध राहा: स्कॅमर्स बऱ्याचदा आपल्यावर त्वरीत कारवाई करण्यासाठी दबाव आणतात. काहीही करण्यापूर्वी विचार करा आणि योग्य ती पडताळणी करा.
- फोन करणाऱ्याची पडताळणी करा: जर कोणी पैसे किंवा संवेदनशील वैयक्तिक माहिती मागितली तर त्याची पुष्टी करण्यासाठी त्यांना त्यांच्या नेहमीच्या क्रमांकावर कॉल करा खरोखर तेच आहेत की नाही.
- वैयक्तिक प्रश्न विचारा: स्कॅमर्सला पकडण्यासाठी खऱ्या व्यक्तीलाच माहित असेल असे काही तरी विचारा.
- सुरक्षित शब्द वापरा: "द्रविडीवाल" किंवा "रवाडोसा" सारख्या केवळ विश्वासू लोकांना माहित असलेला कौटुंबिक किंवा कामाच्या ठिकाणी "सुरक्षित शब्द" सेट करा. नातेवाईक किंवा बॉस असल्याचा दावा करून कोणी पैशांची मागणी करत असेल तर पुढे जाण्यापूर्वी सुरक्षित शब्द विचारा. एखाद्या स्कॅमरला हे माहित नसते, ज्यामुळे आपल्याला त्यांची ओळख पडताळण्यास मदत होते.

स्कॅम # 2 डेटिंग ॲप स्कॅम

ते काय आहे

जेव्हा कोणी डेटिंग ॲपवर एखाद्या व्यक्तीशी जुळते आणि स्कॅमचा भाग असलेल्या रेस्टॉरंट किंवा कॅफेमध्ये त्यांना भेटण्यासाठी आमंत्रित करते तेव्हा हा स्कॅम होतो. स्कॅमर महागडे पदार्थ मागवतो, कधी कधी मेन्यूवरही नसलेल्या गोष्टी मागवतो, मग निघून जाण्याचे निमित्त बनवतो. पीडितव्यक्तीकडे मोठे बिल शिल्लक राहते आणि कर्मचारी किंवा बाऊन्सर्सकडून पैसे भरण्यास भाग पाडले जाते.

हे कसे कार्य करते

नियोजन दिनांक: स्कॅमर तारखेची योजना आखतो आणि पीडितेला एका विशिष्ट कॅफेमध्ये भेटण्यास सांगतो. कधीकधी स्कॅमर एखाद्या परिसराचा प्रस्ताव देऊ शकतो आणि पीडितेला मेट्रो स्टेशनवर भेटण्यास सांगू शकतो, कारण ते जवळच कॅफे निवडतील.

कॅफे मध्ये: आत गेल्यावर स्कॅमर खाण्यापिण्याची ऑर्डर देतो, कधीकधी मेन्यूवर नसलेल्या गोष्टीही मागवतो. ते खोटी आपत्कालीन परिस्थिती निर्माण करून पटकन निघून जाऊ शकतात.

सरप्राईज बिल: जेव्हा बिल येते, तेव्हा ते अपेक्षेपेक्षा जास्त खूप जास्त असते - बहुतेकदा नेहमीच्या किमतीपेक्षा कित्येक पट जास्त. पीडितेने विरोध केल्यास कॅफेचे कर्मचारी किंवा बाऊन्सर त्यांना धमकावतात, पैसे देण्यास भाग पाडतात.

स्कॅमचा डाव: हा स्कॅम कॅफे मालक, व्यवस्थापक किंवा बाऊन्सर्ससह कर्मचारी आणि डेटिंग ॲपवर पीडितेशी जुळणारी व्यक्ती यांचा समावेश असलेल्या गटाद्वारे चालविला जातो. फसवणुकीने वाढवलेल्या बिलांतून गोळा झालेल्या पैशातून प्रत्येकाला त्याचा हिस्सा मिळतो.

बहुतेक बळी ही स्कॅम पोलिसांना सांगत नाहीत, कारण त्यांना लाज वाटते किंवा आपल्या कुटुंबाला आपण डेटिंग ॲप वापरत होतो, हे कळण्याची भीती वाटते.

जर तुमच्यासोबत असे झाले तर कृपया स्थानिक पोलिस ठाण्यात किंवा ऑनलाईन फसवणूक तक्रार पोर्टलवर तक्रार करा. **www.cybercrime.gov.in.**

- भेटीच्या ठिकाणाबाबत सावध रहा: आपण त्या क्षेत्राशी परिचित असल्याशिवाय समोरच्या व्यक्तीने निवडलेल्या ठिकाणी भेटणे टाळा.

- समोरच्या व्यक्तीने सुचवलेल्या कॅफेचा आधी शोध घ्या: कॅफे ऑनलाईन शोधा आणि त्याच्या रिव्ह्यूज तपासा, जेणेकरून ते विश्वासार्ह आहे की नाही याची खात्री होईल. नक्की खात्री करण्यासाठी वेगवेगळ्या स्रोतांवरील रिव्ह्यूज तपासा.

- कधी कधी स्कॅमर्स बनावट रिव्ह्यू टाकून त्या ठिकाणाला विश्वासार्ह असल्यासारखं दाखवतात तुमच्या अंत:प्रेरणांवर विश्वास ठेवा: जर काहीतरी विचित्र वाटत असेल—जसं की समोरची व्यक्ती ठिकाणाबाबत खूप आग्रह धरत असेल किंवा रेस्टॉरंटमध्ये बसल्यानंतर अचानक कुल आणि दूर जाण्यासारखं वागत असेल—तर सावध रहा.

- संशयास्पद वर्तनाची तक्रार करा: तुम्हाला फसवणुकीचा संशय आल्यास, त्वरित पोलिसांना आणि डेटिंग ॲपला कळवा, जेणेकरून इतर लोक या स्कॅमचा बळी ठरणार नाहीत.

स्कॅम # 3 डिजिटल अरेस्ट स्कॅम

ते काय आहे

डिजिटल अरेस्ट स्कॅम म्हणजे जेव्हा स्कॅमर्स ऑनलाइन किंवा फोनवर कस्टम अधिकाऱ्यांसारखे पोलिस किंवा सरकारी अधिकारी असल्याचे भासवतात. ते असा दावा करतात की आपण कायदेशीर अडचणीत आहात आणि "अटक टाळण्यासाठी" त्वरित पैसे देण्याची मागणी करतात. पीडितांवर त्वरीत पैसे भरण्यासाठी दबाव आणण्यासाठी ते बऱ्याचदा भीती आणि तातडीचा वापर करतात.

हे कसे कार्य करते

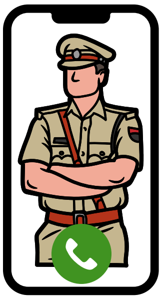
बनावट कॉल किंवा मेसेज: आपण कायदा मोडला आहे असा दावा करणारा कॉल, ईमेल किंवा मजकूर आपल्याला प्राप्त होतो आणि दंड भरावा लागतो किंवा अटकेला सामोरे जावे लागते. उदाहरणार्थ, एका पीडितेला एका आंतरराष्ट्रीय क्रमांकावरून फोन आला की पार्सलची नियोजित डिलिव्हरी रद्द करण्यात आली आहे.

धमक्या आणि दबाव: जर आपण त्वरित पैसे दिले नाहीत तर आपल्याला तुरुंगवासासारख्या गंभीर परिणामांना सामोरे जावे लागेल, असे स्कॅमर म्हणतो. वर नमूद केलेल्या उदाहरणात, फोन करणाऱ्याने पीडितेला समर्थनासाठी "0" दाबण्यास प्रवृत्त केले. हे करताच कस्टमर सपोर्ट रिप्रेझेंटेटिव्ह असल्याचे भासवून कोणीतरी कॉलवर आले आणि आपल्या नावाशी जोडलेल्या पॅकेजमध्ये बेकायदा पदार्थ असून ते चीनला पाठवण्यात आल्याचा दावा केला. त्याच्याविरोधात अटक वॉरंट जारी करण्यात आल्याचा दावाही या प्रतिनिधीने केला आहे. त्यानंतर बनावट पोलिस अधिकारी आणि तपासकर्ते व्हिडिओ कॉलमध्ये सामील झाले.

स्कॅमर्स आपल्याला हे पटवून देण्यासाठी खूप प्रयत्न करतील की ते खरे पोलिस आहेत. ते तुम्हाला बनावट लेटरहेड आणि ओळखपत्र दाखवतील. ते बनावट पोलिस स्टेशने तयार करतात आणि व्हिडिओ कॉलिंग करताना पोलिसांसारखे कपडे घालतात.

एकटेपणा आणि तातडीचा दबाव: स्कॅमर करणारा तुम्हाला इतरांपासून दूर ठेवण्याचा प्रयत्न करेल. ते तुम्हाला एखाद्या दूरच्या ठिकाणी जाण्यास सांगतील किंवा खोलीत एकटे राहून पडदे लावायला सांगतील. ते तुम्हाला इतर कोणाचेही कॉल न घेण्यास सांगतील.

पुन्हा पुन्हा पैशाची मागणी: ते वारंवार पैशांची मागणी करतात आणि सहसा वेगवेगळ्या खात्यांवर पैसे पाठवायला सांगतात, जेणेकरून ते ट्रॅक करता येऊ नयेत.



उदाहरण:

तुम्हाला फोन येतो की: "मी सायबर क्राईम युनिटमधून ऑफिसर X बोलतो. आम्हाला आपल्या खात्याशी संबंधित बेकायदेशीर क्रियाकलाप आढळले आहेत. तुम्हाला पैसे द्यावे लागतील अटक टाळण्यासाठी आत्ताच ₹10,000 त्याचे पालन न केल्यास अटक केली जाईल."

- शांत रहा: भारतात फोन कॉल किंवा व्हिडिओ कॉलद्वारे पोलीस अटक करू शकत नाहीत आणि करणारही नाहीत. स्कॅमरने तुमचा पत्ता, नाव इत्यादी तुमच्याबद्दल वैयक्तिक माहिती जाणून घेण्याचा दावा केला तरी घाबरू नका. ताबडतोब कॉल डिस्कनेक्ट करा आणि गुंतणे थांबवा.

- दाव्याची पडताळणी करा: कॉल ठेवा आणि संबंधित अधिकृत संस्थेशी थेट संपर्क करा, त्यांचा अधिकृत फोन नंबर किंवा वेबसाइट वापरून. ते पोलिस असो, इतर सरकारी अधिकारी असो किंवा त्या संस्थेचे ग्राहक सेवा प्रतिनिधी असो, ज्यांनी तुम्हाला कॉल केला.

- एकटे राहण्यास नकार द्या: कधीही कोणालाही तुम्हाला एकटे राहण्यास किंवा मित्रांशी किंवा कुटुंबियांशी कॉल न घेण्यास पटवू देऊ नका. ताबडतोब कॉल ठेवा आणि कोणावर विश्वास ठेवता त्या व्यक्तीशी ताबडतोड बोला.

- पेमेंट करू नका: खऱ्या कायद्याची अंमलबजावणी करणारे कधीही फोनवर पैसे मागणार नाहीत. अशा सर्व मागण्या फेटाळून लावा.

- लाल झेंड्यांवर लक्ष ठेवा: तुम्ही ओळखत नसलेल्या आंतरराष्ट्रीय किंवा देशांतर्गत नंबरवरून आलेले कॉल. आपले नाव, बँक खाते किंवा ID सारख्या वैयक्तिक तपशीलांची "पडताळणी" करण्याची विनंती.

- काळजी घ्या: परदेशातून आलेल्या कॉलसारख्या अनोळखी किंवा संशयास्पद नंबरवरून फोन कॉलला उत्तर देताना सावध गिरी बाळगा.

स्कॅम # 4 बनावट गुंतवणूक/ ट्रेडिंग ॲप स्कॅम

ते काय आहे

फेक ट्रेडिंग अॅप स्कॅममध्ये गुंतवणूकदारांची फसवणूक करण्यासाठी डिझाइन केलेल्या फसव्या ट्रेडिंग अनुप्रयोगांची निर्मिती आणि प्रचार समाविष्ट आहे. हे ॲप्स अनेकदा उच्च परतावा आणि कमी जोखीम यांचे आश्वासन देतात, ज्यामुळे तुम्हाला तुमचे पैसे गुंतवण्यासाठी आकर्षित केले जाते. तथापि, एकदा आपण या बनावट ॲप्समध्ये पैसे जमा केले की, आपल्याला अनेक फसवणुकीच्या पद्धतींचा सामना करावा लागू शकतो.

हे कसे कार्य करते

बनावट गुंतवणूक ॲप्ससाठी जाहिराती आणि प्रचार: सकॅमर्स भ्रामक जाहिरातींचा वापर करून पीडितांना असामान्य पणे उच्च आर्थिक परताव्याचे आमिष दाखवतात. बऱ्याचदा, स्कॅमर्सद्वारे पीडितांना WhatsApp ग्रुपमध्ये जोडले जाते, ज्यात "ICICI IR टीम" सारखी वैध नावे असतात ज्यामुळे पीडितांना वाटते की ते परवानाधारक वित्तीय संस्थांशी संबंधित आहेत. स्कॅमर्स सामान्यत: पीडितेचा विश्वास संपादन करण्यासाठी खोट्या यशोगाथा शेअर करण्यासाठी या गटांचा वापर करतात.

फेक अॅप्स डाउनलोड करा आणि गुंतवणूक करा: गुंतवणुकीच्या खऱ्या संधी देणारी फसवी अॅप्स डाऊनलोड करण्याची सूचना पीडितांना देण्यात आली आहे. 'आयसी ऑर्गन मॅक्स' आणि 'Techstars.shop' सारख्या या अॅप्समध्ये प्रसिद्ध शेअर्स आणि फायनान्शिअल इन्स्ट्रुमेंट्सची नावे दाखवली जातात, जेणेकरून युजर्सला ते वैध असल्याचे भासवता येईल.

बनावट चार्ट, खाते शिल्लक आणि नफ्याच्या स्टेटमेंटसह हे अॅप वास्तविक दिसण्यासाठी डिझाइन केले ले आहे ज्यामुळे आपली गुंतवणूक वाढत असल्याचे दिसते.

उच्च परताव्याचे बनावट प्रदर्शन: एकदा पीडितांनी बनावट ॲप इन्स्टॉल केले आणि त्यांचे पैसे गुंतवले, तेव्हा त्यांना सुरुवातीला डॅशबोर्डवर चांगला परतावा दिसतो, ज्यामुळे त्यांना अधिक गुंतवणूक करण्यास प्रोत्साहित केले जाते. मात्र, हा परतावा केवळ बनावट आकडे असतात. जेव्हा बळी पडलेले लोक त्यांचे पैसे काढण्याचा प्रयत्न करतात, तेव्हा त्यांना अतिरिक्त शुल्क जसे की कायदेशीर कर किंवा ब्रोकरेज फी भरण्यास सांगितले जाते, जेणेकरून स्कॅमर्स त्यांच्याकडून अधिक पैसे उकळू शकतील.

फसवे व्यवहार

अडकलेली रक्कम: तुम्हाला असे आढळून येईल की तुम्ही तुमचे पैसे काढू शकत नाही.

शुल्कांची मागणी: ॲप तुम्हाला तुमची रक्कम मिळण्यापूर्वी अतिरिक्त "शुल्क" किंवा "कर" भरण्यास सांगू शकते.

गायब होण्याचा प्रकार: स्कॅमर्स आपले पैसे सोबत घेऊन ॲप पूर्णपणे बंद करू शकतात.

बनावट सपोर्ट: जर तुम्ही मदतीसाठी संपर्क केला, तर तुम्हाला बनावट ग्राहक सेवा मिळू शकते, जी वेळकाढूपणा करेल किंवा अधिक पैसे जमा करण्यासाठी दबाव टाकेल.

गायब होणारे स्कॅमर्स: एकदा स्कॅम उघडकीस आल्यानंतर, ॲप काढून टाकले जाते आणि स्कॅमर्स गायब होतात, ज्यामुळे बळी पडलेल्यांना त्यांचे पैसे परत मिळवण्याचा कोणताही मार्ग राहत नाही.

- अनपेक्षित किंवा न मागता आलेल्या मेसेजपासून सावध राहा, जे ऑनलाइन गुंतवणुकीद्वारे जलद पैसे कमवण्याचे आश्वासन देतात.
- अवास्तव परताव्याचे आश्वासन देणाऱ्या गुंतवणुकीच्या संधींपासून दूर राहा.
- अधिकृत वेबसाइट्स किंवा अ◌ॅप्सद्वारे गुंतवणूक प्लॅटफॉर्मची वैधता पडताळून पहा. उदाहरणार्थ, जर त्यांनी ICICI सारख्या विशिष्ट बँकेशी संलग्न असल्याचे सूचित केले तर ICICI च्या ग्राहक सहाय्यावर कॉल करा किंवा हे सत्य आहे की नाही हे पाहण्यासाठी त्याची अधिकृत वेबसाइट तपासा.
- लॉगिन क्रेडेंशियल्स, वैयक्तिक किंवा आर्थिक माहिती अनोळखी व्यक्तींशी, विशेषत: मेसेजिंग ॲपवर शेअर करू नका.
- अनोळखी संपर्कांच्या विनंतीवरून अज्ञात ॲप किंवा फाइल्स डाउनलोड करणे टाळा.

स्कॅम # 5 बनावट नोकरीचे ऑफर स्कॅम

ते काय आहे

बनावट जॉब ऑफर स्कॅम म्हणजे जेव्हा स्कॅमर्स आपल्याला पैसे किंवा वैयक्तिक माहिती देण्यासाठी फसवण्यासाठी नोकरी देण्याचे नाटक करतात. हे स्कॅम्स बऱ्याचदा नोकरीच्या शोधात असलेल्या लोकांना लक्ष्य करतात, त्यांना आकर्षित करण्यासाठी उच्च वेतन, सोपे काम किंवा फायदे देण्याचे आश्वासन देतात.

हे कसे कार्य करते

आकर्षक नोकरीची जाहिरात: स्कॅमर्स वेबसाइट्स, सोशल मीडियावर नोकरीच्या बनावट जाहिराती तयार करतात किंवा ईमेल किंवा संदेशांद्वारे पाठवतात. कधीकधी, स्कॅमर्स सल्लागार असल्याचे नाटक देखील करू शकतात जे आपल्याला प्रतिष्ठित कंपनीत प्लेसमेंटची हमी देतात.

जलद निवड प्रक्रिया: ते आपल्याला सांगतात की आपण नोकरीसाठी "निवडलेले" आहात, बऱ्याचदा मुलाखत किंवा योग्य स्क्रीनिंगशिवाय.

पेमेंट किंवा वैयक्तिक माहितीसाठी मागणी करतात : तुमच्याकडून प्रशिक्षण, नोंदणी, कामाच्या साहित्य किंवा व्हिसा प्रोसेसिंगसाठी (जर ती आंतरराष्ट्रीय नोकरी असेल तर) शुल्क भरण्याची मागणी केली जाते.

बनावट कागदपत्रे किंवा लिंक्स: ते बनावट ऑफर लेटर, कॉन्ट्रॅक्ट पाठवू शकतात किंवा आपल्याला वैध दिसण्यासाठी फसव्या वेबसाइटवर निर्देशित करू शकतात.

गायब होण्याचा प्रकार: एकदा पैसे किंवा आपली वैयक्तिक माहिती गोळा केली की स्कॅमर्स गायब होतात आणि नोकरी अस्तित्वात नसते.

बनावट रोजगार स्कॅमची उदाहरणे

बनावट जॉब स्कॅम्सचे अनेक प्रकार आहेत

- **वर्क फ्रॉम होम जॉब स्कॅम**
- **जॉब प्लेसमेंट सर्व्हिस स्कॅम**
- **नॅनी, केअरगिव्हर आणि व्हर्च्युअल पर्सनल असिस्टंट नोकरीतील स्कॅम**

वर्क फ्रॉम होम जॉब स्कॅम

स्कॅमर्स असा दावा करतात की जिथे तुम्ही कमी वेळ आणि मेहनतीने घरून काम करून महिन्याला लाखो रुपये कमवू शकता.

वर्क फ्रॉम होम जॉब स्कॅम्समध्ये रिशिपिंग स्कॅम्स आणि माल पुनर्विक्री स्कॅम्स यांचा समावेश आहे.
री-शिपिंग स्कॅम्स: स्कॅमर्स क्वालिटी कंट्रोल मॅनेजर किंवा व्हर्च्युअल असिस्टंट सारख्या बनावट नोकऱ्यांची जाहिरात करतात. एकदा "भाड्याने" घेतल्यानंतर, आपले कार्य महागड्या वस्तू प्राप्त करणे, रिपॅकेज करणे आणि पुन्हा पाठविणे आहे, बर्याचदा चोरीच्या क्रेडिट कार्डद्वारे खरेदी केले जाते. पेचेक कधीच येत नाही आणि कंपनी गायब होते, ज्यामुळे आपण एखाद्या गुन्ह्यात सामील होऊ शकता. जर आपण "पेरोल" साठी वैयक्तिक तपशील प्रदान केला असेल तर आपल्याला ओळख चोरीस देखील सामोरे जावे लागू शकते.

माल पुनर्विक्री स्कॅम्स: स्कॅमर्स नफ्यात लक्झरी उत्पादनांची पुनर्विक्री करण्याची नोकरी देण्याचे आश्वासन देतात. फसवणूक करणारे महागड्या उत्पादनांची पुनर्विक्री करून नफा कमावण्याची नोकरीचे आश्वासन देतात.

नॅनी, केअरगिव्हर आणि व्हर्च्युअल पर्सनल असिस्टंट नोकरीतील स्कॅम

स्कॅमर्स जॉब साइट्सवर नॅनी, केअरगिव्हर्स आणि व्हर्च्युअल असिस्टंटसाठी बनावट नोकरीच्या जाहिराती पोस्ट करतात. किंवा ते अशा ईमेल पाठवू शकतात ज्या तुमच्या समुदायातील कोणीतरी पाठवल्यासारख्या दिसतात. हा संदेश आपल्या कॉलेज किंवा विद्यापीठासारख्या आपल्या ओळखीच्या संस्थेचा भाग असलेल्या एखाद्या व्यक्तीकडून देखील येऊ शकतो.

जर तुम्ही अर्ज केला, तर तुम्हाला नियुक्त करणारी व्यक्ती तुम्हाला चेक पाठवू शकते. ते आपल्याला चेक जमा करण्यास सांगतील, पैशांचा काही भाग आपल्या सेवेसाठी ठेवतील आणि उर्वरित दुसऱ्या कोणाला तरी पाठवतील.

हि स्कॅम आहे. एक विश्वासार्ह नियोक्ता कधीही तुमच्याकडून असे करण्याची अपेक्षा करणार नाही. तो चेक बनावट असतो आणि बाउन्स होतो, आणि बँक तुमच्याकडून त्या बनावट चेकची पूर्ण रक्कम परत मागेल, तर स्कॅमर तुमच्या कडून पाठवलेले खरे पैसे ठेवून गायब होईल.

जॉब प्लेसमेंट सर्व्हिस स्कॅम

स्कॅमर स्वतःला कन्सल्टन्सी म्हणून सादर करेल आणि तुम्हाला टॉप कंपनीमध्ये नोकरी मिळवून देण्याचे आश्वासन देईल. ते तुम्हाला मुलाखतीसाठी बोलवतील. जेव्हा तुम्ही पोहोचता, तेव्हा प्रवेशद्वाराजवळ मोठ्या व्यक्ती उभ्या असू शकतात. स्कॅमर स्वतःला कन्सल्टंट म्हणून सादर करेल आणि तुमच्या पात्रतेबाबत काही साधारण प्रश्न विचारेल. ते तुम्हाला अशा लोकांचे बनावट फोटोही दाखवू शकतात, ज्यांना त्यांनी आधी मोठ्या बहुराष्ट्रीय कंपन्यांमध्ये नोकरी लावल्याचा दावा करतात. यानंतर ते तुमच्याकडे पैसे मागतील आणि मोठी माणसे तुम्हाला पैसे देण्यास भाग पाडू शकतात.

- कोणतीही संस्था/कंपनी त्यांच्यासाठी काम करण्यासाठी कधीही पैसे मागत नाही.
- फसवणूक / जंक ईमेल किंवा संदेशांमधून पाठविलेल्या नोकरीच्या ऑफरकडे दुर्लक्ष करा. जर तुम्हाला असा जॉब ऑफर मिळाला की ज्यामध्ये चेक जमा करून त्यातील काही रक्कम वापरण्यास सांगितले जात असेल, तर ती स्कॅम आहे. त्यापासून निघून जा.
- प्लेसमेंट कंपन्या उमेदवारांकडून फी मागत नाहीत. नोकरीसाठी उमेदवार शोधण्यासाठी कंपन्या त्यांना फी देतात. जर एखादी प्लेसमेंट फर्म तुमच्याकडून शुल्क मागत असेल—विशेषतः आगाऊ पैसे भरायला सांगत असेल—तर लगेच निघून जा. कदाचित तुम्ही स्कॅमच्या जाळ्यात अडकत आहात.
- जर कोणी तुम्हाला नोकरी देऊ करत असेल आणि तुम्ही कमी कामात कमी वेळात भरपूर पैसे कमवू शकता असा दावा करत असेल तर ती नक्कीच स्कॅम आहे.
- कंपनीची अधिकृत वेबसाइट, रिव्यू आणि संपर्क तपशील तपासा.
- ऑनलाइन उपस्थिती नसलेल्या किंवा स्केच तपशील नसलेल्या कंपन्यांकडून ऑफर टाळा.
- कंपनीची पडताळणी केल्याशिवाय तुमचे बँक खाते, आधार किंवा पॅन सारखे संवेदनशील तपशील शेअर करू नका.

स्कॅम # 6 बनावट लिंक / QR कोड स्कॅम

ते काय आहे

बनावट लिंक/QR कोड स्कॅम तुम्हाला धोकादायक लिंक क्लिक करण्यास किंवा फसवे QR कोड स्कॅन करण्यास भाग पाडते. ही स्कॅम्स तुमची वैयक्तिक माहिती, पेमेंट डिटेल्स चोरण्यासाठी किंवा तुमच्या डिव्हाइसमध्ये हानिकारक सॉफ्टवेअर इन्स्टॉल करण्यासाठी तयार केली जाते.

हे कसे कार्य करते

बनावट लिंक्स: सकॅमर्स ईमेल, मेसेज किंवा सोशल मीडियाद्वारे लिंक्स पाठवतात आणि मोठ्या (उदा. सवलती, बक्षिसे किंवा तातडीचे अपडेट्स) देण्याचे आश्वासन देतात. लिंक क्लिक करताच तुम्हाला एका बनावट वेबसाइटवर नेले जाते, जी खरी वाटते पण तुमची वैयक्तिक माहिती चोरण्यासाठी तयार केलेली असते.

बनावट QR कोड: सकॅमर्स असे QR कोड तयार करतात जे तुम्हाला फिशिंग वेबसाइटवर नेतात किंवा हानिकारक क्रिया ट्रिगर करतात (उदा. मालवेअर इन्स्टॉल करणे). हे कोड डिजिटलपद्धतीने पाठवले जाऊ शकतात किंवा फिजिकल पोस्टर्स किंवा जाहिरातींवर ठेवले जाऊ शकतात.

कधी कधी सकॅमर्स खरी जाहिरात घेऊन त्यातील QR कोड बनावट कोडने बदलतात, जेणेकरून लोकांना तो खरा असल्याचा भास होईल.

बनावट लिंक / QR कोड स्कॅमची उदाहरणे

- एक संदेश येतो की तुमच्या पार्सलचे वितरण उशीर झाला आहे; दिलेली लिंक पेमेंटच्या तपशीलांची मागणी करते.
- सकॅमर्स बनावट पेमेंट लिंक किंवा QR कोड शेअर करून तुम्हाला क्रेडिट कार्डची माहिती किंवा UPI PIN टाकायला भाग पाडू शकतात.
- सकॅमर्स बनावट वेबसाइटच्या लिंक पाठवतात, ज्या बँकांसारख्या विश्वासार्ह संस्थांच्या वेबसाइटसारख्या दिसतात आणि तुम्हाला KYC माहिती अपडेट करण्यास सांगतात.
- पोस्टरवरील QR कोड सवलत देतो परंतु फिशिंग साइटकडे जातो.

- जर आपल्याला अनपेक्षित ठिकाणी QR कोड दिसला तर तो उघडण्यापूर्वी URLची तपासणी करा. जर ते आपण ओळखत असलेल्या URLसारखे दिसत असेल तर ते बनावट नाही याची खात्री करा - चुकीचे स्पेलिंग किंवा बदललेले अक्षर शोधा.
- तुम्ही अपेक्षा न केलेल्या ईमेल किंवा मजकूर संदेशातील QR कोड स्कॅन करू नका – विशेषतः जर तो त्वरित कृती करण्यास सांगत असेल. तुम्हाला संदेश खरा वाटत असेल, तर कंपनीशी संपर्क साधण्यासाठी तुम्हाला माहीत असलेला अधिकृत फोन नंबर किंवा वेबसाइट वापरा.
- अनोळखी स्त्रोतांकडून पेमेंट लिंकवर क्लिक करू नका.
- QR कोड पेमेंट करताना नेहमी इच्छित प्राप्तकर्त्याच्या नावाची पडताळणी करा.
- जेव्हा आपल्या KYC साठी विचारले जाते तेव्हा KYC चा हेतू आणि अशी माहिती मागणाऱ्या व्यक्तीची ओळख पडताळून पहा.

स्कॅम # 7 बनावट कर्ज ॲप स्कॅम

ते काय आहे

बनावट कर्ज ॲप स्कॅमत सकॅमर्स असे बनावट ॲप तयार करतात जे कमी कागदपत्रांवर जलद आणि सोपे कर्ज देण्याचे आश्वासन देतात. ही ॲप्स सहसा तातडीने पैशांची गरज असलेल्या लोकांना लक्ष्य करताना दिसतात आणि त्यांना शुल्क भरायला किंवा वैयक्तिक माहिती शेअर करायला भाग पाडतात. त्यांच्याकडे अनेकदा छुपे शुल्क आणि खूप जास्त व्याजदर असतात.

हे कसे कार्य करते

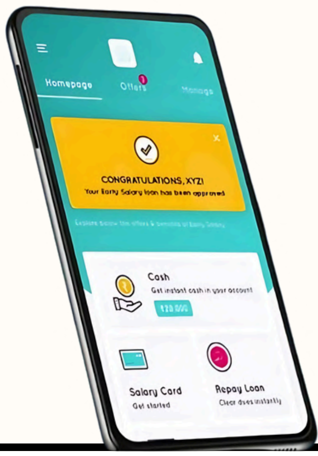
आकर्षक ऑफर: हे ॲप कोणतेही क्रेडिट तपासणी नाही, त्वरित मंजुरी किंवा अत्यंत कमी व्याजदरासह कर्ज देण्याचे जाहिरात करून तुम्हाला त्यांच्या सेवांचा वापर करण्यास प्रवृत्त करतात. सकॅमर्स बऱ्याचदा बँकांसारख्या नामांकित वित्तीय संस्थांसारखीच नावे निवडतात जेणेकरून आपल्याला ते वैध समजतील.

पूर्वनिर्धारित शुल्क: तुम्ही अर्ज केल्यानंतर, हे ॲप कर्ज वितरीत करण्यापूर्वी प्रोसेसिंग फी, सेवा शुल्क किंवा इतर देयके मागतात.

डेटा चोरी आणि मालवेअर हल्ले: हे ॲप तुमचा बँक खाते क्रमांक, ओळखपत्र आणि फोन संपर्कांसारखी संवेदनशील वैयक्तिक माहिती गोळा करते. कधी कधी या ॲप्समध्ये मालवेअर असते, जे तुम्ही ॲप डाउनलोड केल्यानंतर तुमच्या फोनवर इन्स्टॉल होते.

छळ: तुम्ही पैसे भरले नाहीत तर सकॅमर्स चोरलेल्या माहितीकडून तुम्हाला, तुमच्या कुटुंबाला किंवा संपर्कातील लोकांना धमक्या देतात किंवा सार्वजनिक अपमान करण्याचा प्रयत्न करतात. उदाहरणार्थ, व्हिडिओ-KYC करण्याच्या बहाण्याने ते आपल्या फोटोंमध्ये प्रवेश करू शकतात आणि त्यांना जे सापडते त्याआधारे आपल्याला ब्लॅकमेल करू शकतात.

कर्ज वितरित होत नाही: अनेकदा फी भरल्यानंतरही कर्ज दिले जात नाही आणि ॲप गायब होते किंवा प्रतिसाद देणे बंद होते.



- स्रोताची सत्यता तपासा: कर्ज ॲप्स स्वतः कधीही कर्ज देत नाहीत; त्याऐवजी ते RBI नियमन असलेल्या बँका किंवा बिगर-बँक वित्तीय संस्थां (NBFCs) सोबत भागीदारी करतात.

  बँका आणि NBFC च्या अधिकृत वेबसाइटवर जाऊन तपासा की संबंधित कर्ज ॲपने ज्या भागीदारीचा दावा केला आहे, ती प्रत्यक्षात अस्तित्वात आहे का. जर तुम्हाला वेबसाईटवर काही सापडत नसेल तर बँकेच्या/NBFC च्या कस्टमर सर्व्हिस नंबरवर फोन करून अधिक पडताळणी करा.

- परवानग्यांबाबत सावध राहा: जे ॲप्स संपर्क, फोटो किंवा संदेशांसाठी अनावश्यक परवानगी मागतात, त्यांचा वापर टाळा.

- विश्वसनीय स्रोतांचा वापर करा: ॲप वापरण्यापूर्वी त्याची विश्वासार्हता आणि रिव्यू तपासा. आपण एकाधिक स्त्रोतांकडून रिव्यू तपासत असल्याचे सुनिश्चित करा. आधी सांगितल्याप्रमाणे, सकॅमर्स बऱ्याचदा खरे वाटण्यासाठी बनावट रिव्यू देतात.

- पूर्वनिर्धारित शुल्क: विश्वसनीय कर्जदाता सामान्यतः कधीही आगाऊ शुल्क मागत नाहीत. कर्ज देण्यापूर्वी पैसे देण्याची मागणी करणाऱ्या सावकारांना टाळा.

- सावधानता संकेत: त्वरित कर्जाच्या ऑफरपासून सावध राहा, विशेषतः जर त्या कोणतीही क्रेडिट तपासणी न करता हमीशीर मंजुरी देण्याचे आश्वासन देत असतील.

- व्याजदर: व्याजदर आणि अटी काळजीपूर्वक तपासा. जर ते खरे वाटत असतील तर कदाचित ते आहेत.

- संपर्क माहिती: कर्जदाराचा संपर्क तपशील आणि प्रत्यक्ष पत्त्याची पुष्टी करा. सकॅमर्स अनेकदा खोटी माहिती वापरतात.

- संशयास्पद फ्रॉडची तक्रार करा: जर आपल्याला संभाव्य सायबर लोन शार्कचा सामना करावा लागला किंवा आपला स्कॅम झाला आहे असे वाटत असेल तर ताबडतोब योग्य अधिकाऱ्यांना कळवा.

स्कॅम # 8 बनावट मोबाइल रिचार्ज स्कॅम

ते काय आहे

बनावट मोबाइल रिचार्ज स्कॅम आपल्याला फोन रिचार्ज किंवा बनावट ऑफर्ससाठी पैसे देण्यास प्रवृत्त करतो. स्कॅमर्स बनावट वेबसाइट्स, ॲप किंवा मेसेजचा वापर करून डिस्काउंट, कॅशबॅक किंवा फ्री रिचार्ज देण्याचा दावा करतात.

हे कसे कार्य करते

बनावट ऑफर: स्कॅमर्स मोठ्या सवलती किंवा "मोफत रिचार्ज" सारख्या अवास्तव ऑफर संदेश, सोशल मीडिया किंवा बनावट ॲप्सद्वारे जाहिरात करतात. कधी कधी स्कॅमर्स TRAI चे अधिकारी असल्याचे भासवतात, जेणेकरून तुमचा त्यांच्यावर विश्वास बसेल.

रिचार्जसाठी पेमेंट: पीडित व्यक्ती बनावट प्लॅटफॉर्मद्वारे रिचार्जसाठी पैसे देते, परंतु प्रत्यक्षात कोणतेही रिचार्ज केले जात नाही.

माहितीची चोरी: बनावट रिचार्ज प्लॅटफॉर्म प्रक्रियेदरम्यान बर्याचदा वैयक्तिक तपशील, देयक माहिती किंवा बँक तपशील / क्रेडिट कार्डची माहिती गोळा करतात.

फिशिंग लिंक: स्कॅमर्स SMS किंवा ईमेलद्वारे लिंक पाठवतात, जी तुम्हाला बनावट वेबसाइटवर पुनर्निर्देशित करतात, ज्या वास्तविक टेलिकॉम रिचार्ज सेवा सारख्या दिसतात.

- विश्वसनीय प्लॅटफॉर्म्सचा वापर करा: फक्त तुमच्या मोबाइल प्रदात्याच्या ॲपद्वारे किंवा तुमच्या UPI शी संबंधित ॲपद्वारे रिचार्ज करा.
- अवास्तविक ऑफर्सपासून सावध रहा: मोठ्या प्रमाणात सूट किंवा विनामूल्य रिचार्ज सारख्या खऱ्या वाटणाऱ्या व्यवहारांकडे दुर्लक्ष करा.
- वेबसाइट्स आणि ॲपची सत्यता तपासा: बनावट किंवा चुकीचे स्पेलिंग असलेल्या नावांसाठी URL तपासा आणि फक्त अधिकृत ॲप स्टोअरमधून ॲप डाउनलोड करा.
- सत्यापित न केलेल्या लिंकवर क्लिक करू नका: अज्ञात स्रोतांद्वारे SMS, WhatsApp, किंवा ईमेलद्वारे पाठवलेल्या रिचार्ज लिंकवर क्लिक करण्यापासून टाळा.
- सुरक्षित पेमेंट तपशील: कधीही तुमची पेमेंट माहिती अविश्वसनीय तिसऱ्या पक्षांच्या प्लॅटफॉर्मवर शेअर करू नका.
- संशयास्पद क्रियाकलापांची माहिती द्या: आपल्याला स्कॅम झाल्यास आपल्या दूरसंचार प्रदात्यास किंवा स्थानिक सायबर क्राईम हेल्पलाइनला कळवा.

स्कॅम # 9 पार्सल वितरण स्कॅम

ते काय आहे

पार्सल डिलिव्हरी स्कॅम आपल्याला असा विचार करण्यास प्रवृत्त करतो की आपल्याकडे डिलिव्हरी ची वाट पाहत असलेले पॅकेज आहे. सकॅमर्स लोक पॅकेज सोडवण्यासाठी पेमेंट किंवा वैयक्तिक माहिती मागणारी खोटी संदेशे किंवा ईमेल्स पाठवतात.

हे कसे कार्य करते

खोटी नोटिफिकेशन्स: तुम्हाला एक टेक्स्ट, ईमेल, किंवा कॉल प्राप्त होतो ज्यात सांगितले जाते की तुमचे पॅकेज आले आहे, परंतु अपूर्ण पत्त्याच्या माहिती किंवा देयक न भरल्यामुळे ते वितरित केले जाऊ शकत नाही. हे FedEx, DHL किंवा India Post सारख्या विश्वासार्ह कुरिअर कंपनीचे असू शकते.

फिशिंग लिंक: या मेसेजमध्ये तुमचा पत्ता अपडेट करण्यासाठी एक लिंक असते, साधारणत: 12 तासांच्या आत. संदेशात "डिलिव्हरीची पुष्टी करण्यासाठी" किंवा शुल्क भरण्याची लिंक देखील समाविष्ट असू शकते. लिंकवर क्लिक केल्याने आपण एका बनावट वेबसाइटवर जातो जिथे स्कॅमर्स आपले पेमेंट किंवा वैयक्तिक तपशील चोरतात.

फॉलो-अप कॉल: थोडक्यात, SMS किंवा ईमेलसह कुरिअर कंपनीचा प्रतिनिधी असल्याचे भासवून एखाद्याचा फोन कॉल असतो. ते असे पुन्हा सांगतील की तुमचे पार्सल वितरित केले जाऊ शकत नाही कारण तुमचा पत्ता अपूर्ण आहे किंवा काही देयक बाकी आहे, आणि तुम्हाला दिलेल्या लिंकवर फॉर्मलिटी पूर्ण करण्यास सांगतील.

तत्कालता आणि दबाव: फोन करणारा पीडितेवर दबाव टाकतो, पत्ता अपडेट न केल्यास किंवा पैसे न दिल्यास ऑर्डर रद्द केली जाईल किंवा पार्सल नष्ट केली जाईल, अशी धमकी देते.

पेमेंट ट्रॅप: तुम्हाला पुन्हा वितरित करण्यासाठी एक छोटा शुल्क भरण्याचा सांगितला जातो. हे पेज केवळ डेबिट किंवा क्रेडिट कार्ड पेमेंट स्वीकारते, UPI किंवा कॅश ऑन डिलिव्हरीसाठी कोणताही पर्याय नाही.

कोणतीही डिलिव्हरी नाही: एकदा तुम्ही पेमेंट केले किंवा माहिती दिली, की स्कॅमर्स गायब होतात, आणि तुम्हाला पॅकेज मिळत नाही आणि तुमची माहिती चोरीला जाते.

- तुम्ही ऑर्डर दिली आहे का याची आठवण करा: तुम्ही खरोखरच पॅकेज पाठवले आहे का, किंवा तुम्ही ऑर्डर दिली आहे जी अजून वितरित व्हायची आहे का ते आठवण करा.
- मेसेज पडताळून पहा: डिलिव्हरीची पुष्टी करण्यासाठी कुरिअर कंपनीशी त्यांच्या अधिकृत वेबसाइट किंवा फोन नंबरद्वारे थेट संपर्क साधा.
- अज्ञात लिंकवर क्लिक करणे टाळा: पार्सलबद्दल असल्याचा दावा करणाऱ्या मेसेजमधील लिंकवर क्लिक करू नका, विशेषत: अनोळखीकडून.
- सावधानता संकेत शोधा: खराब व्याकरण, सामान्य ग्रीटिंग्स किंवा संशयास्पद ईमेल पत्त्यांपासून सावध रहा.
- तुमची माहिती सुरक्षित करा: स्रोत वैध असल्याची खात्री असल्याशिवाय कधीही वैयक्तिक किंवा पेमेंट माहिती शेअर करू नका.

स्कॅम # 10 लपलेला मालवेअर स्कॅम

ते काय आहे?

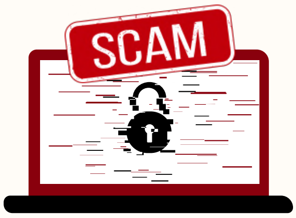
एक लपलेला मालवेअर स्कॅम आपल्याला मालवेअर पसरविण्यासाठी किंवा वैयक्तिक माहिती चोरण्यासाठी डिझाइन केलेल्या हानिकारक लिंकवर क्लिक करण्यास प्रवृत्त करतो. हे लिंक बऱ्याचदा वैध दिसतात, परंतु त्यावर क्लिक केल्याने आपले डिव्हाइस संक्रमित होऊ शकते किंवा आपल्याला हानिकारक साइटवर निर्देशित केले जाऊ शकते.

हे कसे कार्य करते

वेबसाइटवर स्थानिकरण: सकॅमर्स हे लिंक वेगवेगळ्या मार्गांनी जसे की वेबसाइटवरील जाहिरातींद्वारे ठेवतात.स्कॅमर्स वेबसाइटवरील जाहिरातींसारख्या विविध माध्यमातून या लिंक टाकतात.

क्लिक आणि संक्रमित: जेव्हा आपण लिंकवर क्लिक करता तेव्हा हे होऊ शकते:

- तुमच्या डिव्हाइसवर मालवेअर इन्स्टॉल करणे,
- तुम्हाला फिशिंग वेबसाइट्सकडे रीडायरेक्ट करणे,
- किंवा बनावट सॉफ्टवेअर किंवा अद्यतने डाउनलोड करण्यासाठी आपल्याला फसवा.



कोणतीही संवादाची आवश्यकता नाही: काही हानिकारक लिंकना क्लिकची देखील आवश्यकता नसते-ते केवळ विशिष्ट वेबसाइटवर प्रदर्शित करून (कोडद्वारे) आपल्या डिव्हाइसला संक्रमित करू शकतात.

संशयास्पद लिंक टाळा: अविश्वसनीय सौदे, विनामूल्य सॉफ्टवेअर किंवा तातडीचे इशारे देणाऱ्या लिंकवर क्लिक करू नका.

सॉफ्टवेअर अपडेटेड ठेवा: तुमचा ब्राउझर आणि सुरक्षा सॉफ्टवेअर अपडेटेड ठेवा, जेणेकरून हानिकारक जाहिराती ब्लॉक होऊ शकतील.

सुरक्षा फीचर्स ऑन करा: धोके शोधण्यासाठी आणि ब्लॉक करण्यासाठी अँटीव्हायरस सॉफ्टवेअर आणि ब्राउझर सुरक्षा सेटिंग्ज वापरा. काही अँटीव्हायरस सॉफ्टवेअर मालवेअर संरक्षणासह येतात जे आपण नकळत एखाद्या चुकीच्या वेबसाइटवर गेल्यास धोके सांगतात. अशा वैशिष्ट्यांसह आपल्याला अँटीव्हायरस सॉफ्टवेअर मिळेल याची खात्री करा. तसेच, आपल्या ब्राउझरवरील जोखीम देखरेख सेटिंग्ज चालू आहेत याची खात्री करा.

विश्वसनीय वेबसाइट्सचा वापर करा: संशयास्पद किंवा अप्रमाणित वेबसाइटला भेट देणे किंवा त्यांच्याशी संवाद साधणे टाळा. विश्वसनीय आणि प्रसिद्ध वेब ब्राउझर्सचा वापर करा, जे तुम्हाला हानिकारक सामग्री, मालवेअर किंवा सुरक्षा प्रमाणपत्रांचा अभाव असलेल्या वेबसाइट्स उघडण्यापूर्वी इशारा देतात.

स्कॅम # 11 टेक सपोर्ट स्कॅम

ते काय आहे

टेक सपोर्ट स्कॅम आपल्याला आपल्या संगणक किंवा डिव्हाइसमध्ये समस्या आहे यावर विश्वास ठेवण्यास प्रवृत्त करते. सर्कमर्स Microsoft किंवा Apple सारख्या वास्तविक कंपन्यांपासून असल्याचं भासवून, अस्तित्वात नसलेल्या समस्यांना सोडवण्यासाठी खोटी "सपोर्ट" ऑफर करतात, आणि अनेक वेळा पैसे किंवा वैयक्तिक माहिती चोरतात.

हे कसे कार्य करते

खोटे चेतावणी संदेश: तुम्हाला तुमच्या संगणकावर किंवा फोनवर एक पॉप-अप दिसतो ज्यात सांगितले जाते की ते व्हायरसने संक्रमित आहे किंवा त्यात गंभीर त्रुटी आहे. यात अनेकदा बनावट कस्टमर सपोर्ट नंबर चा समावेश असतो.

स्पॅम कॉल्स: सर्कमर्स टेक सपोर्ट म्हणून कॉल करून सांगतात की त्यांनी तुमच्या डिव्हाइससह काही समस्या शोधली आहे.

स्क्रीन मिररिंग सॉफ्टवेअर: सर्कमर्स आपल्या संगणकावरील त्रुटी दुरुस्त करण्याच्या बहाण्याने आपल्याला रिमोट डेस्कटॉप सॉफ्टवेअर किंवा स्क्रीन-शेअरिंग ॲप डाउनलोड करण्यास सांगतात. ते आपल्याला एक पिन शेअर करण्यास सांगतील, जे त्यांना कोणत्याही ठिकाणाहून आपल्या डिव्हाइसवर प्रवेश करण्यास सक्षम करेल. सर्कमर्स नंतर तुमची फाइल्स पाहू शकतात, त्यात बदल करू शकतात, डेटा ट्रान्सफर करू शकतात, व्हायरस इन्स्टॉल करू शकतात आणि तुमच्या डिव्हाइसवर नियंत्रण घेऊ शकतात.

पैशाची मागणी: ते समस्या सोडविण्याचा दावा करतात आणि बऱ्याचदा क्रेडीट कार्ड किंवा गिफ्ट कार्डद्वारे बनावट सेवांसाठी पैसे देण्याची मागणी करतात.

डेटा चोरी: आपल्या डिव्हाइसमध्ये प्रवेश करताना, ते पासवर्ड किंवा बँकिंग तपशीलसारखी संवेदनशील माहिती चोरू शकतात.

- अनोळखी कॉल्सवर विश्वास ठेवू नका: वैध कंपन्या आपल्याला आपण अहवाल न दिलेल्या समस्यांबद्दल कॉल करत नाहीत.
- पॉप-अप्सकडे दुर्लक्ष करा: कोणतेही संशयास्पद पॉप-अप बंद करा आणि दिसणाऱ्या नंबरवर कॉल करू नका. त्याऐवजी आपले डिव्हाइस स्कॅन करण्यासाठी अँटीव्हायरस सॉफ्टवेअर वापरा.
- कधीही रिमोट प्रवेश देऊ नका तुम्ही विश्वसनीय आणि प्रमाणित सपोर्ट सर्व्हिसला संपर्क केले नाहीत तोपर्यंत कोणालाही तुमच्या डिव्हाइसवर रिमोट कंट्रोल देऊ नका.
- सपोर्टच्या दाव्यांची तपासणी करा: सकॅमरने दिलेल्या संपर्काच्या तपशिलांऐवजी, कंपनीला त्यांच्या अधिकृत वेबसाइटवरील संपर्क तपशिलांद्वारे थेट संपर्क करा.
- अँटीव्हायरस सॉफ्टवेअर वापरा: विश्वासार्ह अँटीव्हायरस सॉफ्टवेअरसह आपली उपकरणे अपडेटेड आणि संरक्षित ठेवा.
- स्कॅम रिपोर्ट करा: जर आपल्याला टेक सपोर्ट स्कॅम आढळली तर स्थानिक अधिकाऱ्यांना कंपनीची फसवणूक केल्याची तक्रार करा.

स्कॅम # 12 OTP स्कॅम

ते काय आहे

वन टाइम पासवर्ड (OTP) स्कॅममुळे तुमचा OTP फ्रॉडस्टर्सना उघड होतो. OTP चा वापर सामान्यत: आपली ओळख किंवा ऑनलाइन व्यवहार किंवा वेबसाइटमध्ये लॉग इन करण्यासाठी अधिकृतता पडताळण्यासाठी केला जातो. हे कोड सहसा SMS किंवा ईमेलद्वारे पाठवले जातात, जे केवळ एकदाच वापरण्याचा हेतू आहे.

हे कसे कार्य करते

प्रतिरूप: स्कॅमर्स कॉल किंवा ईमेलद्वारे बँका, ई-कॉमर्स वेबसाइट्स, पार्सल डिलिव्हरी सेवा किंवा इतर सेवा प्रदात्यांसारख्या वैध सेवांची नक्कल करतात.

खोटी तात्काळता: स्कॅमर्स खोटी तात्काळता निर्माण करतात, ज्यामुळे तुम्ही निर्णय घेण्यात गडबड कराल आणि तुम्हाला OTP शेअर करण्यास दबाव आणतात, जोपर्यंत तुम्ही पाठवणाऱ्याची सत्यता तपासत नाही.

पैशाची चोरी किंवा वैयक्तिक माहिती: स्कॅमर्स संवेदनशील माहिती मिळवण्यासाठी OTP चा वापर करतात जसे की बँकिंग तपशील किंवा ओळख चोरीसाठी वैयक्तिक माहिती.

- शांत राहा: निर्माण झालेल्या तातडीच्या भावनेत अडकू नका, शांत रहा आणि आपल्या व्यवहाराचा इतिहास शोधा, प्रेषकाची ओळख पडताळून पहा आणि योग्य काळजी घ्या.
- अज्ञात कॉल आणि ईमेलपासून सावध रहा: अनपेक्षितपणे आपल्याशी संपर्क साधणाऱ्या व्यक्तीशी वैयक्तिक माहिती किंवा OTP कधीही शेअर करू नका. सामान्यत:, फक्त जेव्हा तुम्ही बँका किंवा इतर सेवा संपर्क करता ज्यांना संवेदनशील माहितीची आवश्यकता असू शकते, तेव्हा ते CVV आणि इतर संवेदनशील वैयक्तिक किंवा वित्तीय माहिती विचारतात.
- पाठवणाऱ्याची ओळख पडताळून पाहा: ईमेल किंवा लिंकवर क्लिक करण्यापूर्वी, पाठवणाऱ्याचीओळख पडताळून पहा.
- सावधगिरी बाळगा: कॉल करणाऱ्याकडून OTP साठी अचूक कारण विचारून तुमच्या वैयक्तिक रेकॉर्डसह क्रॉस-चेक करा की तुम्ही अशा कोणत्याही ट्रांजेक्शन केल्या आहेत का आणि त्या ट्रांजेक्शनसाठी OTP फोनवर किंवा लिंकवर शेअर करणे आवश्यक आहे का.

स्कॅम # 13 रिवॉर्ड स्कॅम

ते काय आहे

रिवॉर्ड स्कॅम आपल्याला रिवॉर्डच्या नावाखाली संवेदनशील माहिती शेअर करण्यास फसवतात.

हे कसे कार्य करते

रिवॉर्डसंबंधी संदेश शेअर करणे: सकॅमर्स मोठ्या प्रमाणात रोख रक्कम किंवा क्रेडिट कार्ड पॉईंट्स जिंकल्याबद्दल आपले अभिनंदन करणारे ईमेल किंवा SMS पाठवतील. हे तुम्हाला वेबसाइट किंवा फसव्या ॲपसाठी लिंकवर क्लिक करण्यास सांगेल.

हे असे दिसू शकते: "प्रिय मूल्यवान ग्राहकांनो, आपले SBI नेटबँकिंग रिवॉर्ड पॉईंट्स (9980 रुपये) आज संपत आहेत! आता SBI रिवॉर्ड ॲप इन्स्टॉलद्वारे रिडीम करा आणि आपल्या खात्यात रोख रक्कम जमा करून आपल्या बक्षिसाचा दावा करा".

खोटी वेबसाइट: वेबसाइट खरी वाटू शकते आणि आपल्याला आपली वैयक्तिक किंवा बँकिंग माहिती शेअर करण्यास सांगू शकते. तथापि, डेटा सकॅमर्सकडून पाहीला जातो.

खोटे ॲप: सकॅमर्स तुम्हाला 'SBI रिवॉर्ड्स' सारखी दिसणारी खोटी ॲप्स डाउनलोड करण्यास सांगू शकतात, ज्यामुळे तुम्ही रिवार्ड प्राप्त करू शकता. तथापि, हे एक हानिकारक ॲप आहे आणि ते संवेदनशील ॲप जसे की कॅमेरा, मायक्रोफोन, संपर्क सूची, फोटोज, संदेश आणि इतर गोष्टींमध्ये प्रवेश करू शकते.

हानिकारक रिवॉर्ड्स: वैकल्पिकरित्या, सकॅमर्स हे देखील सांगू शकतात की आपण नवीन फोन, टॅब्लेट किंवा लॅपटॉप जिंकला आहे. तथापि, या डिव्हाइसेसवर हानिकारक ॲप किंवा व्हायरस आधीच इन्स्टॉल केलेले असतात, जे तुमची संवेदनशील वैयक्तिक माहिती, समावेश बँकिंग डेटा, चोरी करू शकतात.

- सावध राहा: कोणत्याही रिवार्ड आणि बक्षिसांचा दावा करण्यासाठी लिंकवर क्लिक करण्यापूर्वी संदेशाचा मजकूर काळजीपूर्वक वाचा.
- पडताळा: असा रिवॉर्ड कार्यक्रम लाइव्ह असल्यास बँका किंवा इतर सेवांशी संपर्क साधा. उदाहरणार्थ, रिवॉर्ड कार्यक्रम चालविणार् या मोठ्या कंपन्या त्यांच्या अधिकृत वेबसाइटवर त्याचा प्रचार करतील.
- फॅक्टरी रिसेट: तुम्हाला भेट किंवा रिवॉर्ड म्हणून मिळालेल्या कोणत्याही डिव्हाइसेसला वैयक्तिक माहिती टाकण्यापूर्वी फॅक्टरी रिसेट करा. हे तुम्ही खरेदी केलेल्या कोणत्याही पुनर्विक्री डिव्हाइसेससाठी देखील एक चांगली सवय आहे.

स्कॅम # 14 SIM स्वॅपिंग / SIM क्लोनिंग फसवणू स्कॅम

ते काय आहे

SIM स्वॅपिंग, ज्याला SIM क्लोनिंग देखील म्हणतात, जेव्हा स्कॅमर्स आपल्या फोन नंबरवर नियंत्रण ठेवण्यासाठी आपल्या SIM कार्डची नक्कल करतात. एकदा त्यांना प्रवेश मिळाल्यावर, ते OTP-आधारित सुरक्षा तपासणी टाळून तुमच्या बँक खात्यातील पैसे चोरू शकतात.

हे कसे कार्य करते

टेलिकॉम प्रोव्हायडरला पोर्ट नंबरवर पटवून देणे: स्कॅमर्स फिशिंग ईमेल, मालवेअर हल्ले किंवा डेटा लीक वापरून वैयक्तिक तपशील गोळा करतात. त्यानंतर ते आपल्या मोबाइल नेटवर्क प्रदात्याशी संपर्क साधतात, आपण असल्याचे भासवतात, बनावट ID प्रूफ प्रदान करतात आणि जुने SIM कार्ड हरवले किंवा खराब झाल्याचा दावा करून नवीन सिमकार्डची विनंती करतात.

तुम्हाला SIM स्वॅपसाठी पटवणे: कधीकधी स्कॅमर्स आपल्याला सिम स्वॅप अॅक्टिव्हेट करण्याचा प्रयत्न करतात. या पध्दतीत स्कॅमर आपल्या टेलिकॉम प्रोव्हायडरचा एक्झिक्युटिव्ह असल्याचे भासवून तुम्हाला फेक कॉल करतो. स्कॅमर एक चांगले मोबाइल सब्सक्रिप्शन पॅकेज ऑफर करतो आणि आपल्याला आपला 20 अंकी SIM नंबर सामायिक करण्यास आणि ऑफर सक्रिय करण्यासाठी "1" दाबण्यास राजी करतो. तथापि, जेव्हा आपण "1" दाबता तेव्हा आपण आपल्या नंबरवरील SIM स्वॅप प्रमाणित करता आणि स्कॅमरला नियंत्रण देता.

नियंत्रण मिळवणे: एकदा SIM कंपनीने नवीन SIM जारी करताच किंवा SIM स्वॅप पूर्ण होताच, तुमची मूळ SIM निष्क्रिय होते. स्कॅमरला तुमचे कॉल, मेसेज आणि OTP अॅक्सेस मिळतो.

आर्थिक फ्रॉड आणि ओळख चोरी: स्कॅमर्स निधी हस्तांतरित करण्यासाठी, पासवर्ड रीसेट करण्यासाठी आणि आपली आर्थिक आणि सोशल मीडिया खाती ताब्यात घेण्यासाठी OTP चा वापर करतात.

- SIM लॉक सक्रिय करा: आपल्या डिव्हाइसवरील सेटिंग्जमध्ये आपले SIM लॉक करण्यासाठी SIM पिन सेट करा. स्कॅमर्स सिम पिनशिवाय तुमचे SIM स्वॅप किंवा डिॲक्टिव्हेट करू शकणार नाहीत.
- नेटवर्क समस्यांकडे सतर्क रहा: जर आपला फोन अचानक नेटवर्क गमावत असेल तर इतरांकडे सिग्नल असल्यास, ताबडतोब आपल्या प्रदात्याशी संपर्क साधा.
- आपल्या डिजिटल फूटप्रिंटबद्दल सावध गिरी बाळगा: Google, Meta सारख्या लोकप्रिय सेवांवर आपल्या गोपनीयता सेटिंग्जचे पुनरावलोकन करण्यात वेळ घालवा. आपला वैयक्तिक डेटा तृतीय-पक्षांशी किती शेअर केला जातो हे आपल्याला कळेल.

स्कॅम # 15 भेसळ स्कॅम

ते काय आहे

सकॅमर्स हॅकिंग, चोरलेले पासवर्ड आणि फिशिंग तंत्रांचा वापर करून तुमच्या मित्र, नातेवाईक किंवा सहकाऱ्याच्या नावाने प्रतिरूपण करतात आणि मग तुम्हाला पैसे पाठवण्यासाठी फसवतात. हे मेसेज ओळखीच्या व्यक्तीकडून येत असल्याने अनेकदा पीडित या स्कॅमला बळी पडतात.

हे कसे कार्य करते

सकॅमर्स एखाद्याच्या सोशल मीडिया अकाउंटला हॅक करून त्यांच्या संपर्कांना आपत्कालीन परिस्थिती असल्याचे सांगून मेसेज पाठवतात.

संदेश असे दिसू शकतात: "हाय, मी दिल्लीत अडकलो आहे. सुट्टीसाठी आलो होतो, पण माझी चोरी झाली. मला तातडीने ₹5000 लागतील, पण तू मदत म्हणून कितीही पाठवले तरी खूप उपकार होतील. मी परत गेल्यावर लगेच परत करीन. कृपया मदत कर".
कधी कधी सकॅमर्स तुमच्या सहकर्मी किंवा बॉसच्या ईमेल आयडीसारखीच दिसणारी ईमेल तयार करतात. ते तुम्हाला अधिकृत स्वरात पत्र लिहितात, एखादे महत्त्वाचे काम पूर्ण करण्यासाठी तातडीने पैसे पाठवण्यास सांगतात.

एकदा तुम्ही हॅक केलेल्या अकाउंटवर किंवा बनावट ईमेलवर स्कॅमरला प्रत्युत्तर दिल्यावर, ते तुम्हाला ठराविक खात्यात किंवा UPI हँडलवर पैसे ट्रान्सफर करण्यास सांगतात. सकॅमर्स पैसे मिळाल्यानंतर गायब होतात आणि पीडिताला ब्लॉक करतात.

- तातडीच्या संदेशांपासून सावध रहा: सकॅमर्स घाईगडबडीची परिस्थिती निर्माण करून तुम्हाला लवकर निर्णय घेण्यास भाग पाडतात. मेसेजिंग ॲप, सोशल मीडिया किंवा ईमेलवर अचानक आलेल्या पैशांची तातडीची विनंती असलेल्या संदेशांपासून सावध गिरी बाळगा.
- विनंत्या पडताळून पहा: पैशांच्या तातडीच्या विनंतीवर कार्यवाही करण्यापूर्वी आपण त्या व्यक्तीला थेट कॉल करा किंवा एखाद्या सामान्य मित्राशी / नातेवाईकाशी बोला याची खात्री करा.
- सावधानता संकेत तपासा: संदेश पाठवणारा सहसा ज्या प्रकारे संवाद साधतो त्याप्रमाणे नेहमी बोलतो का? नवीन/अज्ञात बँक खात्यांमध्ये पैसे हस्तांतरित करण्यासाठी असामान्य विनंत्या, विचित्र व्याकरण आणि फॉरमॅटिंग आणि विनंत्या शोधा.

स्कॅम # 16 स्किमिंग मशीन फ्रॉड

ते काय आहे

स्किमिंग म्हणजे स्कॅमर्स ATM किंवा हँडहेल्ड कार्ड पेमेंट मशीनमध्ये लपवलेले उपकरण बसवतात, ज्याद्वारे ते तुमच्या कार्ड नंबर, एक्सपायरी डेट आणि मागील बाजूवरील तीन अंकी (CVV) यांसारखी महत्त्वाची माहिती चोरी करतात.

ही उपकरणे अनेकदा मशीनच्या सामान्य भागासारखी दिसण्यासाठी लपवलेली असतात. एकदा कार्डची माहिती मिळाल्यावर, स्कॅमर्स डुप्लिकेट कार्ड तयार करून तुमच्या खात्यातून व्यवहार करतात.

हे कसे कार्य करते

स्किमर बसवणे: फ्रॉडस्टर्स ATM किंवा स्वाइप मशीनच्या कार्ड रीडरवर डिव्हाइस जोडतात.

कार्ड डेटा मिळवणे: जेव्हा आपण आपले कार्ड घालता तेव्हा स्किमर आपल्या कार्डचे तपशील वाचतो.

PIN रेकॉर्ड करणे: एक छोटा कॅमेरा किंवा बनावट कीपॅड ATM मध्ये आपला पिन रेकॉर्ड करतो.

क्लोनिंग आणि फसवणुकीचे व्यवहार: स्कॅमर्स चोरलेल्या तपशीलांचा वापर डुप्लिकेट कार्ड तयार करण्यासाठी आणि पैसे काढण्यासाठी करतात.

- ATM तपासा: ATM मध्ये लूज कार्ड स्लॉट, डगमगणारे कीपॅड किंवा अतिरिक्त कॅमेरे तपासा.
- सावध राहा: कार्ड स्वाइप मशिन नेहमी समोर वापरण्यास सांगा आणि संशयास्पद ठिकाणी किंवा मशीनवर आपले कार्ड स्वाइप करताना सावध गिरी बाळगा.
- बँक स्टेटमेंट्स नियमितपणे तपासा: अनधिकृत डेबिट व्यवहारांसाठी आपले बँक स्टेटमेंट आणि SMS नियमितपणे तपासा.
- अनधिकृत व्यवहार त्वरित बँकेत रिपोर्ट करा. आपण शक्य तितक्या लवकर आपल्या बँकेला कळवल्यास आपण तोटा मर्यादित करू शकाल.

स्कॅम # 17 बनावट कल्याण योजना स्कॅम

ते काय आहे

सर्कमर्स बनावट पोर्टल तयार करतात, जे PM किसान योजना, PM आवास योजना यांसारख्या सामान्य योजनांच्या अधिकृत वेबसाइटसारखेच दिसतात. पीडितांना आपले बँक खाते, मोबाइल क्रमांक आणि आधार तपशील फसवणूकदारांना उघड करण्याचे आमिष दाखवले जाते.

हे कसे कार्य करते

आपण समाजकल्याण योजनेअंतर्गत निधी मिळविण्यास पात्र आहात, असे सांगून स्कॅमर्स आपल्याला फोन करतात, परंतु आपल्याला रक्कम पाठविण्यापूर्वी आपल्याला प्रथम आपल्या बँक तपशीलांची 'पडताळणी' किंवा 'अपडेट' करणे आवश्यक आहे.

त्यानंतर स्कॅमर्स तुम्हाला 'व्हेरिफिकेशन' प्रक्रिया पूर्ण करण्यासाठी तुमचे बँक खाते आणि डेबिट कार्डतपशील शेअर करण्यास सांगतात. शेवटी पडताळणी पूर्ण करण्यासाठी ते आपल्याला OTP मागतात.

पण सर्कमर्स तुमच्या बँक आणि डेबिट कार्डच्या तपशीलांचा वापर तुमच्या खात्यावर पेमेंट सेटअप करण्यासाठी करतात, आणि OTP चा वापर डेबिट व्यवहार अधिकृत करण्यासाठी केला जातो. पीडितांनी OTP शेअर केल्यावर त्यांच्या लक्षात येते की सर्कमर्सनी त्यांच्या खात्यातून पैसे काढले आहेत.

- मोफत वस्तूंबद्दल सावध गिरी बाळगा: सर्कमर्स अनेकदा मोफत वस्तू, कर सवलती किंवा इतर प्रोत्साहने देण्याचे आश्वासन देऊन तुम्हाला तुमची वैयक्तिक आणि आर्थिक माहिती शेअर करण्यास प्रवृत्त करतात.
- सरकारी वेबसाइट्सची सत्यता तपासा: कल्याणकारी योजनांसाठी अधिकृत पोर्टलचा वापर करा. सरकारी वेबसाइट्सच्या शेवटी सहसा ".gov.in" किंवा ".nic.in" असे एक्स्टेंशन असते.
- योजनेचे तपशील तपासा: आपल्या जिल्ह्यातील ग्रामपंचायत किंवा तहसीलदार कार्यालयातून कोणत्याही शासकीय योजनांचा तपशील पडताळून पहा.
- योग्य ती काळजी घ्या: OTP असलेला मेसेज वाचा. ते वैध दिसते की नाही किंवा ते दुसऱ्या कशासाठी आहे हे तपासा. पृष्ठ 38 वरील आमच्या प्रो-टिप्स पहा.

काय करावे काय टाळावे

सुरक्षित सर्फिंग टिप्स

- नियमितपणे गोपनीयता धोरणाची समीक्षा करा आपण ऑनलाइन आपल्याबद्दल शेअर केलेली माहिती मर्यादित करण्यासाठी आपल्या ब्राउझर आणि मेसेजिंग, सोशल मीडिया आणि नकाशांसाठी ॲपवरील सेटिंग्ज.
- तृतीय-पक्ष आणि सोशल मीडिया ॲपना तुमच्या डिव्हाइसवरील फोटो, फायली आणि कोअलिशनसारख्या डेटाचा मर्यादित प्रवेश आहे याची खात्री करा.
- पासवर्ड लक्षात ठेवा किंवा त्यांची भौतिक नोंद ठेवा सुरक्षित आणि विश्वासार्ह ठिकाणी. तुमचा पासवर्ड नियमितपणे बदलण्याची खात्री करा.
- आणि वेगवेगळ्या वेबसाइट्स आणि अ ॅप्सवर तोच पासवर्ड वापरणे टाळा.
- जर तुम्ही फिशिंग स्कॅमच्या जाळ्यात अडकला असाल आणि तुमचे बँक किंवा कार्ड तपशील धोक्यात आले असतील, तर तुमच्या बँकेशी संपर्क साधा आणि रिपोर्ट करा ताबोडतोब.
- आवश्यक नसल्यास आपल्या डिव्हाइसवर कोअलिशन सेवा बंद ठेवा.
- गुंतवणूक योजना/नोकरी असल्यास ऑफर खूपच आकर्षक वाटत असेल, तर ती बहुधा बनावट असण्याची शक्यता आहे.

अगदी टाळा अशा गोष्टी

- SMS, ईमेल किंवा मेसेजिंग ॲपवरील अनोळखी स्रोतांमधील लिंक्स सावधपणे न वाचता क्लिक करू नका.
- OTP, ATM किंवा UPI पिन आणि पासवर्ड कॉल, SMS वर शेअर करू नका,ऑनलाइन फॉर्म आणि ईमेल.
- मेसेजिंग ॲपवर अनोळखी नंबरवरून फाईल्स (जसे की लग्नाचे निमंत्रण) डाऊनलोड करू नका.
- सोशल मीडियावर अनोळखी व्यक्तींकडून फ्रेंड रिक्वेस्ट आणि मेसेज रिक्वेस्ट स्वीकारू नका.
- सॉफ्टवेअरच्या पायरेटेड प्रती डाउनलोड आणि स्थापित करू नका आणि मीडिया; त्यामध्ये मालवेअर असू शकतात.
- असुरक्षित वेबसाइट्सवर व्यवहार करताना सावध राहा (वेब पत्त्याची सुरुवात “https://” ने होतेय का आणि “http://” नाही, याची पुष्टी करा).
- ऑनलाइन व्यवहारांसाठी CVV मध्ये प्रवेश करताना सावध गिरी बाळगा.

प्रो टिप्स

1 पासवर्ड स्वच्छता

- कमीत कमी 16 वापरा अपरकेस, लोअरकेस, संख्या आणि चिन्हांचे मिश्रण असलेली वर्णे.
- अनुमानित नमुने, वैयक्तिक माहिती टाळा किंवा सलग येणारे अक्षर किंवा संख्या.
- शक्य असल्यास पासकीज सक्रिय करा.
- पासकीज वापरा पारंपारिक ऐवजी बोटांचे ठसे, फेस ID किंवा व्हॉईस रिकग्निशन सारखे बायोमेट्रिक्स पासवर्ड.
- जेव्हा जेव्हा अतिरिक्त साठी उपलब्ध असेल तेव्हा मल्टी फॅक्टर ऑथेंटिकेशन सेट करा सुरक्षा

कमकुवत पासवर्ड

साधे: आदिती1995 (नाव + जन्म वर्ष)
क्रमिक: abcdxyz123
सहज अंदाज लावता येण्याजोगा: SalmanBhaiFan

मजबूत पासवर्ड

वैयक्तिक: Maachbhaat&Dal92

अविशिष्ट शब्द आणि अनेक अक्षरे: C@rr0tcake&MnMs!

2 SMS कोड समजून घेणे

फसवे SMS संदेश खरे असल्यासारखे भासवण्यासाठी तयार केले जातात आणि सहसा त्वरित कृती करण्यासाठी घाई निर्माण करतात. अशा घोटाळ्यांपासून स्वतःला कसे ओळखावे आणि स्वतःचे संरक्षण कसे करावे ते येथे आहे:

अनेकदा वैयक्तिक मोबाइल नंबर किंवा 567678 किंवा 909090 सारख्या जेनेरिक न्यूमेरिकल ID वरून बनावट मेसेज पाठवले जातात.
अस्सल SMSचे स्वरूप [XY-ABCDEF] आहे
X हे प्रेषकाच्या दूरसंचार सेवा प्रदात्याचे नाव आहे (उदा. जिओसाठी J, एअरटेलसाठी A आणि व्होडाफोनसाठी V).
Y हे सेवा क्षेत्राचे नाव आहे (उदा. दिल्लीसाठी D, मुंबईसाठी M आणि कर्नाटकसाठी X).

- ABCDEF प्रेषकास दिलेल्या कोडचा संदर्भ देते (उदा. SPICEJ म्हणजे स्पाइस जेट).

.. पुढे चालू

उदाहरणे:

- SMS कोड 'AD-SHPRKT' म्हणजे प्रेषक शिप रॉकेट आहे, प्रेषकाचा वाहक एअरटेल आहे आणि संदेश पाठविला जातो.

दिल्ली.

- SMS कोड 'VM-SBIUPI' म्हणजे पाठवणारा स्टेट बँक ऑफ इंडिया, पाठवणारा वाहक व्होडाफोन आणि मुंबईहून मेसेज पाठवला जातो.

- TRAI सेवा प्रदात्यांच्या, सेवा क्षेत्र कोड आणि व्यवसायांना वाटप केलेली हेडर्सची
- सविस्तर यादीचे व्यवस्थापन करते. खात्री करा SMS ची सत्यता पडताळण्यासाठी, विशेषत: कोणत्याही पेमेंट लिंकवर क्लिक करण्यापूर्वी.

#3 सर्कमर्स आणि फ्रॉडस्टर्सला प्रतिसाद देणे

- कॉल कट करा आणि नंबर ब्लॉक करा: अपरिचित कॉल करणाऱ्यांनी वापरलेल्या घाई घालण्याच्या किंवा भीती दाखवण्याच्या युक्त्यांना प्रतिसाद देऊ नका, जरी ते स्वत:ला बँक किंवा सरकारी प्रतिनिधी म्हणून सांगत असले तरी.
- अहवाल: 'संचार साथी' पोर्टलवरील 'चक्षु' ला तक्रार करून सकॅमर्सचा नंबर अक्षम करा (www.sancharsaathi.gov.in).
- जर आपण आधीच पैसे गमावले असतील तर: ताबडतोब आपल्या बँकेला फोन करा आणि व्यवहाराची माहिती द्या. तसेच राष्ट्रीय सायबर क्राईम रिपोर्टिंग पोर्टल (1930 वर डायल करा किंवा भेट द्या आणि घटनेची नोंद करा
- www.cybercrime.gov.in).
- स्पॅम गाळून काढा: 1909 वर डायल करा आणि TRAI च्या निर्देशांनुसार आपल्या दूरसंचार प्रदात्याने दिलेल्या फसवणूक ब्लॉकिंग सुविधेसाठी नोंदणी करा.
- सतत सावधगिरी: नवीनतम अपडेटसाठी सोशल मीडियावर I4C ला फॉलो करा: (@CyberDost ला X (Twitter) वर, CyberDostI4C ला Facebook वर किंवा @cyberdosti4c ला Instagram वर शोधा.
- तुमचा डिजिटल ठसा तपासा: तुमच्या डिजिटल उपस्थितीच्या प्रमाणाबद्दल जागरूक राहा
- ठसा आपण आपला डेटा किती कंपन्यांना दिला याचा आढावा घ्या. गरज पडल्यास त्यांना तुमचा डेटा डिलीट करण्यास सांगा. तसेच, विनामूल्य साधने वापरा
- 'www.haveibeenpwned.com' सारख्या वेबसाइटचा वापर करून तपासा की तुमचा डेटा कोणत्याही डेटा उल्लंघनाचा भाग झाला आहे का.

वापरकर्त्यांच्या सुरक्षिततेसाठी उद्योगातील सर्वोत्तम पद्धती

वापरकर्त्यांची सुरक्षितता सुनिश्चित करणे ही एक सतत चालणारी प्रक्रिया आहे. डिजिटल स्पेस अधिक इमर्सिव्ह होत असताना, व्यवसायांनी वापरकर्त्यांना सूचित करण्यासाठी, सक्षम करण्यासाठी आणि त्यांचे संरक्षण करण्यासाठी त्यांच्या पद्धती विकसित केल्या पाहिजेत.

वापरकर्त्यांच्या सुरक्षिततेसाठी चार मूलभूत तत्त्वे आहेत:

🤖 **वापरकर्त्यांचे संरक्षण आणि सक्षमीकरण करण्यासाठी एआय साधने वापरणे**

🔐 **डिझाइनद्वारे सुरक्षित उत्पादने तयार करणे**

🤝 **वेगवान आणि प्रभावी तक्रार निवारण सुनिश्चित करणे.**

💪 **वेगवान आणि प्रभावी तक्रार निवारण सुनिश्चित करणे.**

🤖 वापरकर्त्यांचे संरक्षण आणि सक्षमीकरण करण्यासाठी AIचा वापर

AI (आर्टिफिशियल इंटेलिजन्स) एक अल्गोरिदम-आधारित निर्णय प्रणाली आहे जी सामान्यत: मानवी बुद्धिमत्तेची आवश्यकता असलेली कार्ये करू शकते. उदाहरणार्थ, नैसर्गिक भाषा प्रक्रिया अल्गोरिदम मजकूर, प्रतिमा आणि व्हिडिओचे विश्लेषण करतात सामग्रीमध्ये फेरफार ओळखण्यासाठी आणि असामान्य क्रियाकलाप किंवा व्यवहार चिन्हांकित करण्यासाठी विश्लेषण केले जाते.

भारतीय अधिकारी काय म्हणतात

- स्पॅम गाळणी: TRAI ने सर्व दूरसंचार सेवा प्रदात्यांना (जसे की Airtel आणि Vodafone) स्पॅम/त्रासदायक कॉल फिल्टर करण्यासाठी AI वापरण्यास सांगितले आहे
- म्युल अकाऊंट देखरेख: रिझर्व्ह बँकेने बँकांना आपल्या उपकंपनी - RBI इनोव्हेशन हब (RBIH) द्वारे तयार केलेल्या AI मॉडेलसह सहकार्य करण्यास सांगितले आहे जे बँका आणि वित्तीय संस्थांना फ्रॉडस्टर्स आणि मनी लॉन्ड्रिंगद्वारे वापरल्या जाणार्या खच्चर खात्यांचा शोध घेण्यास मदत करते.

.. पुढे चालू

आंतरराष्ट्रीय येणारे स्पूफ कॉल प्रतिबंध प्रणाली: DoT ने अशी प्रणाली कार्यान्वित केली आहे जी आंतरराष्ट्रीय स्पॅम कॉल शोधून ब्लॉक करते, जे भारतातून येत असल्यासारखे भासतात. परिणामी, आंतरराष्ट्रीय सर्कमर्स जे कॉलरचे तपशील बदलून भारतीय क्रमांक "(+91 XXXXX XXXXX)" दर्शवतात, त्यांची स्वयंचलितपणे ओळख करून त्यांना ब्लॉक केले जाते.

🤖 AI सोल्यूशन्स कृती करत आहे

AIRTEL

स्पॅम गाळणी

Airtelचे AI संचालित स्पॅम डिटेक्शन टूल स्पॅम कॉल आणि संदेश ओळखण्यासाठी वापराचे पॅटर्न, SMS फ्रिक्वेन्सी, कॉल कालावधी इत्यादी माहितीवर रिअल टाइममध्ये प्रक्रिया करते.

हानीकारक संदेश चिन्हांकित करणे

Airtel चे AI टूल्स विविध घटकांची तपासणी करतात मजकूर संदेशाच्या विविध पैलूंची तपासणी करतात, जसे की शेअर केलेली लिंक ब्लॅकलिस्टेड आहे का नाही, जेणेकरून संदेश संशयास्पद असल्यास त्याची ओळख पटवता येईल.

TRUECALLER

AI असिस्टंट

Truecaller AI असिस्टंट व्हॉईस-टू-टेक्स्ट तंत्रज्ञानाचा वापर करून कॉल स्क्रीन करतो, फोन करणाऱ्याची चौकशी हेतू, स्पॅम कॉल ओळखण्यास आणि कोणत्या कॉलवर कॉल करावे हे ठरविण्यात मदत करणे उत्तर.

शोध संदर्भ

सर्च कॉन्टेक्स्ट रिअल-टाइममध्ये संशयास्पद गतिविधी ओळखतो, जसे की फोन नंबरसाठी वारंवार नाव बदलणे, ज्यामुळे तुम्हाला फसवणूक करणारे कॉलर ओळखणे सोपे होते.

🔐 डिझाइनद्वारे सुरक्षा

'सिक्युरिटी बाय डिझाइन' म्हणजे आपले डिव्हाइस, डेटा आणि नेटवर्क सुरक्षित ठेवण्यासाठी आपल्याला अतिरिक्त पावले उचलावी लागणार नाहीत अशा प्रकारे तंत्रज्ञान उत्पादने तयार करणे पायाभूत सुविधा डिझाइनद्वारे उत्पादने सुरक्षित बनविणे म्हणजे गोपनीयता, अखंडता आणि गेट-गोपासून उपलब्धतेवर लक्ष केंद्रित करणे आवश्यक आहे.

गोपनीयता

संवेदनशील ठेवण्यासाठी एन्क्रिप्शन साधनांचा वापर पासवर्ड सारख्या वैयक्तिक डेटा खाजगी

सत्यनिष्ठा

रोखण्यासाठी तांत्रिक उपाययोजनांचा वापर डेटाच्या उल्लंघनं आणि अनधिकृत प्रवेश

उपलब्धता

डेटा बॅकअप आणि ए ची उपलब्धता सुनिश्चित करणे संपूर्ण हॅकनंतरचा डेटा पुनर्प्राप्ती योजना

गोपनीयता-वृद्धी तंत्रज्ञान (PETs) ही महत्त्वाची सुरक्षा साधने आहेत जी तुमचा डेटा अनधिकृत प्रवेशापासून संरक्षण करतात. एनक्रिप्शन, अनोनीमायझेशन आणि सुरक्षित संगणन यांसारख्या तंत्रज्ञानांचा प्रचलितपणे PETs म्हणून वापर केला जातो.

ही तंत्रे डेटा उपयुक्तता आणि गोपनीयतेची गरज यामध्ये समतोल साधण्यास मदत करतात.

भारतीय अधिकारी काय म्हणतात

- क्लाऊड सेवा: MeitY व्यवसायांना 'पूर्ण डिस्क एनक्रिप्शन' आणि 'फॉरमॅट' यांसारख्या सुरक्षा उपायांची अंमलबजावणी करण्याची शिफारस करते.
- डेटाची रचना (उदा. क्रेडिट कार्ड नंबर) कायम ठेवत माहितीचे संरक्षण करण्यासाठी ‘प्रिझर्विंग एनक्रिप्शन’ लागू करण्याची शिफारस केली जाते.
- आर्थिक सेवा: RBI बँका आणि वित्तीय कंपन्यांना खालील बाबी लागू करण्यास आवश्यक ठरवते:
- मास्क डेटा: माहितीचे संवेदनशील भाग लपवा, जसे की कार्डचे फक्त शेवटचे चार आकडे दाखवणे.
- ऑनलाइन कार्ड पेमेंटसाठी CVV + OTP सारख्या सुरक्षिततेचा अतिरिक्त थर जोडण्यासाठी मल्टी-फॅक्टर ऑथेंटिकेशन वापरा.
- मजबूत एनक्रिप्शन अवलंबा: अशी साधने वापरा ज्यामुळे हॅकर्सना डेटा वाचणे आव्हानात्मक होते.

🔐 डिझाइनद्वारे सुरक्षा उपाय प्रत्यक्ष अंमलात

MICROSOFT

झिरो-ट्रस्ट मॉडेल
Microsoftचे झिरो ट्रस्ट मॉडेल प्रत्येक डेटा प्रवेश विनंतीची सत्यता तपासते, प्रमाणीकरण करते आणि एनक्रिप्ट करते, जरी ती असुरक्षित ओपन नेटवर्कमधून आली असली तरी.

सुरक्षित भविष्य उपक्रम
Microsoft उत्पादनांमधील सुरक्षा संरक्षण डिफॉल्टद्वारे सक्षम आणि लागू केले जाते, कोणत्याही अतिरिक्त प्रयत्नांची आवश्यकता नाही,आणि हे ऐच्छिक नाहीत.

AIRTEL

फेस मॅच
Airtel पेमेंट्स बँक सिक्युरिटी अल्गोरिदमचा वापर करते जे ओळख चोरी किंवा फ्रॉडचा धोका आढळल्यास सेल्फी आधारित चेहरा ओळखण्याची पडताळणी सक्रिय करते.

आंतरराष्ट्रीय नंबर ओळखणे
Airtel एक तांत्रिक उपाय लागू करते जो सर्व कॉल्ससाठी "आंतरराष्ट्रीय कॉल" दाखवतो जे आलेले कॉल्स आंतरराष्ट्रीय असतात.

हे आपल्याला सहजपणे आंतरराष्ट्रीय कॉल ओळखण्यास सक्षम करते आणि अपेक्षित कॉलमध्ये फरक करण्यास मदत करते आणि संभाव्य फ्रॉड किंवा स्पॅम.

META

एंड-टू-एंड एन्क्रिप्शन
WhatsApp हे सुनिश्चित करते की फक्त पाठवणारा आणि प्राप्त करणारा व्यक्तीच संदेश, कॉल्स, फोटो आणि व्हिडिओसाठी प्रवेश करू शकतात.

मर्यादित डेटा संकलन
WhatsApp फक्त आवश्यक डेटा जसे की फोन नंबर संग्रहित करते आणि संएंडदेशांची सामग्री किंवा स्थान डेटा संग्रहित करण्यापासून आपोआप टाळते.

🤝 वापरकर्त्यांसाठी तक्रार निवारण मार्ग

स्पष्ट आणि साधे तक्रार निवारण प्रणाली डिजिटल सेवा वापरणाऱ्या वापरकर्त्यांना त्यांची तक्रार सोडवण्याची सुविधा पुरवतात. जसे की तुम्हाला डिजिटल व्यवसायांसोबत कार्य करत असताना तुम्ही ज्या समस्यांचा सामना करू शकता, त्यासाठी वेळेवर उपाय मिळावा. व्यवसाय आपल्या ई-कॉमर्स खरेदीच्या वितरणास उशीर किंवा तक्रार निवारणाद्वारे कॅब प्रवासासाठी पैसे देण्याच्या समस्या यासारख्या समस्यांचे निराकरण करतात चॅनेल्स.

तक्रार निवारण यंत्रणा

- संचार साथी: दूरसंचार विभाग (DoT) टेलिकॉम फ्रॉडचा सामना करण्यासाठी आपल्याला मदत करण्यासाठी विविध उपक्रम ऑफर करते. संचार साथी उपक्रम आपल्याला अनुमती देतो:
  - चाक्षूवरील संशयित फ्रॉडच्या संप्रेषणाचा अहवाल द्या (भेट www.sancharsaathi.gov.in/sfc/);
  - आपल्या नावाने जारी केलेले सर्व मोबाइल कनेक्शन ओळखा आणि व्यवस्थापित करा; आणि
- हरवलेले/ चोरीला गेलेले मोबाइल हँडसेट ची तक्रार करा जेणेकरून ते ब्लॉक केले जाऊ शकतील, शोधले जाऊ शकतील आणि परत मिळवता येतील.
- आर्थिक क्षेत्राचे देखरेख करणारे संस्था: RBI ची एकात्मिक ओमबुड्समन योजना एक केंद्रीकृत तक्रार निवारण यंत्रणा तयार करते, ज्याद्वारे तुम्ही बँका, पेमेंट सेवा प्रदाते, क्रेडिट ब्युरो आणि इतर वित्तीय संस्थांविरोधात RBI कडे तक्रार करू शकता.
- ग्राहक हेल्पलाइन: ग्राहक सुरक्षा विभाग (DoCA) आपल्याला तक्रारींचे निराकरण करण्यासाठी अनेक चॅनेल प्रदान करतो व्यवसाय आणि सेवा प्रदाते: जसे की व्हॉट्सअ◌ॅप-इंटिग्रेटेड हेल्पलाइन नंबर (8800001915), राष्ट्रीय ग्राहक हेल्पलाइन वेब पोर्टल (www.consumerhelpline.gov.in), आणि UMANG ॲप.
- मध्यमस्थ मार्गदर्शक तत्त्वे: MeitY डिजिटल प्लॅटफॉर्म्ससाठी जसे की सोशल मीडिया आणि गेमिंग कंपन्यांना तक्रार निवारण यंत्रणा स्थापित करण्याची आणि ग्राहकांच्या तक्रारी वेळेवर सोडवण्याची आवश्यकता आहे. जर तुम्ही कंपनीच्या तक्रार निवारण प्रक्रियेतून समाधानी नसलात, तक्रार निवारण प्रक्रियेत, तुम्ही सरकारद्वारे नियुक्त केलेल्या तक्रार अपील समिती (GAC) कडे ई-तक्रार दाखल करू शकता.

🤝 तक्रार निवारण चॅनेल्स क्रियाशीलतेत

VODAFONE IDEA (VI)

विशेष हेल्पलाईन

Vi तुमच्या विविध आवश्यकतांनुसार विशेष हेल्पलाइन्स प्रदान करते, जसे की मोबाईल नंबर पोर्टबिलिटी, डेटा,अॅक्टिव्हेशन वगैरे.

My VI App

MyVi App आपल्याला विविध उत्पादने आणि सुरक्षिततेमध्ये प्रवेश करण्यास अनुमती देते पर्याय. तुम्ही डू नॉट डिस्टर्ब (DND) सुविधा निवडू शकता, टेलिमार्केटर्सविरोधात तक्रार करूशकता आणि सेवा विनंती आणि तक्रारी ग्राहक सेवा कार्यकारींकडे करू शकता.

AIRTEL

Airtel Thanks ॲप

Airtel Thanks ॲप तुम्हाला नको असलेली नंबर मॅनेज/ब्लॉक करण्याची, दुष्ट गतिविधी रिपोर्ट करण्याची आणि मार्केटिंग संदेश टाळण्यासाठी डू नॉट डिस्टर्ब (DND) सेवा निवडण्याची सुविधा देते.

तक्रारींसाठी दोन-स्तरीय अपील प्राधिकरण

जर तुम्ही निराकरणावर समाधानी नसाल, तर तुम्ही एका अपील प्राधिकरणासमोर अपील करू शकता 30 दिवसांच्या आत सेवा क्षेत्र आधारित अपील प्राधिकरणासमोर अपील करू शकता.

💪 इंटरनेट वापरकर्त्यांना सक्षम करण्यासाठी अलर्ट आणि साधने

व्यवसाय त्यांच्या ॲप्स आणि डिजिटल सेवांमध्ये डिझाइन वैशिष्ट्ये समाकलित करतात जी तुम्हाला तुमच्या डेटावर लक्ष ठेवण्यास, गोपनीयता आणि सुरक्षा सेटिंग्ज समायोजित करण्यास आणि सुरक्षित राहण्यास मदत करतात माहिती दिली.

हे आपल्याला आपली माहिती तृतीय पक्षांना कशी सामायिक केली जात आहे हे तपासण्यास आणि नियंत्रित करण्यास मदत करते, कोणती माहिती सामायिक करावी आणि काय खाजगी ठेवावे हे ठरविण्यात आणि एखाद्याने आपल्या खात्यात प्रवेश करण्याचा प्रयत्न केल्यासारखे संशयास्पद क्रियाकलापांबद्दल सूचित केले जाते.

काय म्हणतात भारतीय अधिकारी

- पुनरावृत्ती देयकांसाठी व्यवहार सूचना: RBI बँकांना पुनरावृत्ती देयकांसाठी प्रक्रिया करण्यापूर्वी किमान 24 तास आधी सूचना जारी करण्याचे आदेश देतो, जसे की सदस्यता किंवा प्रणालीबद्ध गुंतवणूक योजना.
- विस्तृत गोपनीयता सूचना: इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालय (MeitY) व्यवसायांना तुमच्याकडून कोणत्या प्रकारचा वैयक्तिक डेटा संकलित केला जातो आणि त्याचे संकलनाचे उद्दीष्ट काय आहे, याबद्दल स्पष्ट आणि विशिष्ट होण्याची आवश्यकता आहे.
- स्पॅम/पेस्की कॉलचा सामना करण्यासाठी TRAI चे नियम: TRAIचे आदेश कंपन्या ज्या बड्या प्रमाणावर ॲप्ससाठी लिंक असलेल्या संदेश पाठवतात आणि वेबसाइट्सनी त्यांच्या सामग्रीची नोंद टेलिकॉम प्रदात्यांसोबत करणे. यामुळे फक्त सत्यापित आणि व्हाइटलिस्टेड लिंक आणि अटॅचमेंट्सच प्रचारात्मक संदेशांमध्ये सार्वजनिकरित्या वितरित केली जातात.
- डार्क पॅटर्न्सपासून संरक्षण: ग्राहक व्यवहार विभाग (DoCA) म्हणतो की, धोखाधडी करणारे डिझाइन पॅटर्न्स जे वापरण्यात येतात, व्यवसायांकडे एक अनुचित व्यापार प्रथा म्हणून पाहिले जाऊ शकते.
  - धोखाधडीच्या डिझाइन्समध्ये त्या ॲप्सचा समावेश होतो ज्यामध्ये गुंतागुंतीची वापरकर्ता इंटरफेस (UI) असते, ज्यामुळे नियमित सब्सक्रिप्शन रद्द करणे कठीण होते व्यवहार, किंवा ॲप्सज्या अतिरिक्त शुल्क आणि लपलेले खर्च चेकआउटच्या अगोदर जोडतात.
  - जर तुम्हाला असे फसवे डिझाइन कृतीत दिसले तर तुम्ही 1915 डायल करून किंवा INGRAM पोर्टलवर जाऊन DoCA कडे तक्रार करू शकता(www.consumerhelpline.gov.in/user/).

💪 इंटरनेट वापरकर्त्यांना कृतीत सक्षम करण्यासाठी साधने

MICROSOFT

कोपायलट कंट्रोल्स
आपण कोपायलटवर प्राधान्य सेट करू शकता, डेटा पाहू, संपादित करू किंवा हटवू शकता आणि संवाद इतिहास व्यवस्थापित करू शकता.

स्काइपवरील गोपनीयता आणि अहवाल
आपण स्काईपवर हानिकारक संदेशांची तक्रार करू शकता,संशयास्पद संदेशांना ब्लॉक करू शकता किंवा तक्रार करू शकता.

META

प्रायव्हसी सेंटर
आपण आपल्या गोपनीयतेचे व्यवस्थापन आणि नियंत्रण करण्यासाठी सेटिंग्ज समायोजित करू शकता. Facebook, Instagram, Messenger आणि इतर Meta उत्पादने.

WhatsApp गोपनीयता नियंत्रण
आपण आपली प्रोफाइल फोटो, शेवटचा पाहिला तपशील आणि इतर गोष्टी कोण पाहू शकतात हे कस्टमाईझ करू शकता
WhatsApp वर चॅट्स देखील लॉक करू शकता.

TRUECALLER

कॉलर ID
Truecaller चा कॉलर ID फक्त नावे दाखवण्यापर्यंत मर्यादित नाही—तो कॉलरचे स्थान, समुदाय रेटिंग्स आणि फ्रॉडचे इशारे देखील प्रदान करतो.
शंका असलेल्या कॉल्सना "स्पॅम" किंवा "फ्रॉडचा इशारा" यासारख्या लेबल्सने चिन्हित केले जाते, ज्यामुळे आपल्याला सूचित निर्णय घेण्यात मदत होते.

व्हेरिफाइड बिझनेस ID
Truecaller बिझनेस कॉलमध्ये छेडछाड-प्रूफ नाव, हिरवा बॅज आणि लोगो जोडतो, ज्यामुळे स्कॅम रोखल्या जातात आणि आपल्याला अस्सल ओळखण्यास मदत होते फ्रॉडस्टर्सचे फोन करणारे.

SAFER INTERNET INDIA

www.saferinternetindia.com ला भेट द्या
secretariat@saferinternetindia.com यावर आम्हाला लिहा

Safer Internet India
@saferinternetindia
SaferInternetIN
@SaferInternetIndia