इकडेही घोटाळेबाज,

तिकडेही घोटाळेबाज,

कुठेही फसवणूक होऊ देऊ नका!

#BankingDhyaanSe 2.0

AXIS BANK

पैसे कमावण्यासाठी तुम्ही खूप मेहनत करता, तर मग तुमची कमाई सुरक्षित का नाही ठेवायची?

ॲक्सिस बँक फ्रॉड अवेअरनेस बुकलेट #BankingDhyaanSe 2.0 मध्ये आपले स्वागत आहे**,** जे तुमची आर्थिक घोटाळे समजून घेण्याची आणि ते टाळण्याची किल्ली आहेत. या अत्यंत वेगाने विकसित होणाऱ्या डिजिटल युगामध्ये, ज्ञान हेच तुमचे घोटाळेबाजांपासून संरक्षण करण्यासाठीची ढाल आहे. हे मार्गदर्शक तुम्हाला आत लपलेली माहिती, वास्तविक जीवनातील उदाहरणे आणि तुमच्या कष्टाने कमावलेल्या पैशाचे संरक्षण करण्यासाठी व्यावहारिक सूचना प्रदान करते.

बँकिंगमधील तुमचा विश्वासू भागीदार या नात्याने ॲक्सिस बँक तुम्हाला डिजिटल विश्वामध्ये आत्मविश्वासाने वावरण्यास मदत करण्यासाठी समर्पित आहे. चला अशा फसवणुकीपासून बचाव करूया आणि एकत्रितपणे उज्ज्वल आर्थिक भविष्याची निश्चिती करूया.

OTP घोटाळे

वन-टाईम पासवर्ड ही तुमच्या अभेद्य डिजिटल साम्राज्यात प्रवेश करण्यासाठी एक सोन्याची किल्ली आहे.

आपली मौल्यवान किल्ली धूर्त फसवणूक करणाऱ्यांपासून दूर ठेवण्यासाठी, आपल्यालाच आपल्या किल्ल्याचे रक्षक व्हावे लागेल!

OTP गोपनीय ठेवा: कधीही OTP कोणाशीही फोन कॉल्स, ई-मेल्स, टेक्स्ट मॅसेज किंवा सोशल मेडियाच्या माध्यमातून शेअर करू नका आणि सावध रक्षकासारखे जागृत रहा.

विनंत्या सत्यापित करा: विश्वास ठेवा परंतु पडताळणी करा. अचानक अपेक्षित नसताना OTP विनंती पॉप अप झाल्यास किंवा काही शंका वाटल्यास घाई करू नका. काही प्रतिक्रिया देण्यापूर्वी दोनदा तपासणी करा.

अधिकृत वेबसाइट किंवा ॲप्सचा वापर करा: OTP शेअर करताना सुरक्षेची काळजी घ्या. नेहमी थेट अधिकृत साईट किंवा ॲपला भेट द्या - काही शॉर्टकट घेऊ नका. लिंकवर क्लिक करण्यापेक्षा टाईप करणे कधीही उत्तमच असते.

तातडीच्या विनंत्यांबाबत सावध रहा: घोटाळेबाज अनेकदा तुमचा OTP शेअर करण्यासाठी तुमच्यावर दबाव आणण्यासाठी निकड असल्याची भावना निर्माण करतात. एक पाऊल मागे घ्या, गंभीरपणे विचार करा आणि काहीही कृती करण्यापूर्वी विनंतीची स्वतंत्रपणे पडताळणी करा.

टू-फॅक्टर ऑथेंटिकेशन सक्षम करा: 2FA (टू-फॅक्टर ऑथेंटिकेशन) सह सुरक्षितता दुप्पट करा. ॲप-आधारित किंवा हार्डवेअर टोकन सारखे भर भक्कम पर्याय निवडा. ते कधीही SMS OTPच्या वरचढ असतात.

कृपया लक्षात ठेवा, बँक तुमचा CVV, OTP, PIN, कार्ड क्रमांक, पासवर्ड इ. विचारणार नाही. हे तपशील कोणाशीही शेअर करू नका.

क्रेडिट कार्ड घोटाळे

क्रेडीट कार्ड घोटाळा म्हणजे लपाछपीचा खेळ आहे अशी कल्पना करूया. घोटाळेबाज त्यांचा खरा हेतू लपविण्याचा जसा प्रयत्न करतात, तसेच ते तुमची क्रेडिट कार्ड संबंधी माहिती उघड करण्यासाठी तुमची फसवणूक देखील करू शकतात.

त्यांच्या सापळ्यात सापडू नये म्हणून पुढील सूचना लक्षात ठेवा:

फिशर्सकडे लक्ष द्या: घोटाळेबाज तुमच्या बँकेकडून किंवा एखाद्या परिचित कंपनीकडून असल्याचे भासवू शकतात. त्यांच्या काव्याला बळी पडू नका; त्यांची ओळख पडताळून पहा.

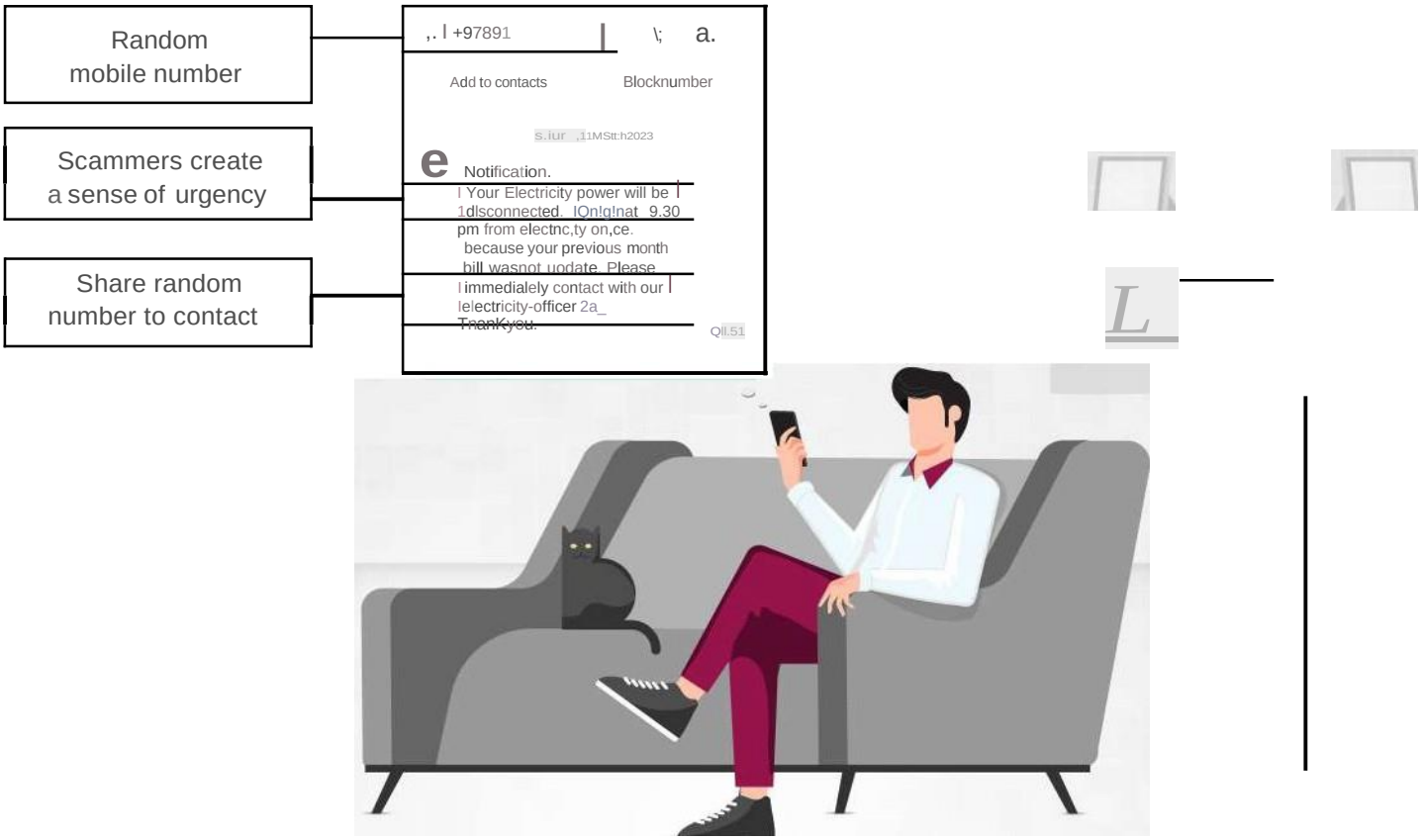
तुमची स्टेटमेंट्स तपासा: तुमच्या क्रेडिट कार्ड स्टेटमेंटचे नियमितपणे पुनरावलोकन करा. तुम्हाला अपरिचित खर्च किंवा शुल्क आढळल्यास, हे खेळामधील लपलेले खेळाडू शोधण्यासारखे आहे-त्यांचा तत्काळ पत्ता लावा.

व्यवहार मर्यादा सेट करा: तुमच्या सर्व पेमेंट चॅनेलवर व्यवहारांची मर्यादा सेट करा आणि तुमच्या गरजेनुसार 'मॅनेज युसेज' विभाग कस्टमाईज करा.

फक्त सुरक्षित साइट्स: ऑनलाइन खरेदी करताना, वेबसाइट सुरक्षित असल्याची खात्री करा (URL मध्ये "https" असल्याचे पहा). हे खेळासाठी सुरक्षित खेळाचे मैदान निवडण्यासारखे आहे.

अपडेटेड रहा: जसे तुम्ही खेळ खेळत असताना नवनवीन रणनीती शिकता त्याप्रमाणे नवीन घोटाळ्याच्या युक्त्यांवर लक्ष ठेवा. अशा प्रकारे, तुम्ही घोटाळेबाजांच्या वरचढ असाल.

इलेक्ट्रिसिटी बिल घोटाळे



बनावट SMS कसा ओळखावा?

कल्पना करा: तुम्ही घरी आरामात संध्याकाळचा आनंद लुटत आहात, तुमचा आवडता कार्यक्रम पाहत आहात आणि मॅसेज आल्यामुळे तुमचा फोन वाजतो. तो तुमच्या वीज पुरवठादाराकडून आहे आणि ते असा दावा करत आहेत की तुमच्या सर्वात अलीकडच्या बिलासाठी तुम्ही अतिरिक्त रक्कम भरणे आवश्यक आहे.

तुम्ही घाबरून जाण्यापूर्वी, पुढील विचार करा: वीज बिल फसवणूक, अगदी एखाद्या अदृश्य भुताप्रमाणे, काही न कळवता तुमच्या आयुष्यात येऊ शकते.

तुमचे गोपनीय तपशील कधीही कोणाशीही शेअर करू नका किंवा अनाहूत लिंकवर क्लिक करू नका.

बिल पेमेंट करण्यासाठी फक्त अधिकृत आणि सुरक्षित वेबसाइटचा वापर करा.

लक्षात ठेवा, विद्युत विभाग कधीही कोणत्याही/अनोंदणीकृत क्रमांकांद्वारे वैयक्तिक तपशील किंवा देयके याबाबत विचारणा करीत नाही.

नोकरी घोटाळे

अशी कल्पना करा की तुम्ही जॉब लिस्ट स्क्रोल करत आहात आणि अचानक तुम्हाला एखादी नोकरीची ऑफर दिसते जी प्रत्यक्षात दिसायला खूप चांगली वाटते. अमर्यादित सुट्टीचे दिवस, तुमच्या सोयीने काम आणि डेटा एंट्री करण्यासाठी सहा आकडी पगार? आम्हाला साइन अप करा!

ते "अप्लाय नाऊ" हीट करण्याआधी, थांबा!

कंपनीविषयी संशोधन करा: कंपनीची ऑनलाइन माहिती पहा आणि ती कंपनी प्रतिष्ठित असल्याची खात्री करा. घोटाळेबाज अनेकदा खात्री पटेल अशा वेबसाइट आणि बनावट कंपन्या तयार करतात.

आगाऊ पैसे देऊ नका: अस्सल नियोक्ते तुम्ही काम सुरू करण्यापूर्वी तुम्हाला प्रशिक्षण, साहित्य किंवा पार्श्वभूमी तपासणीसाठी पैसे देण्यास सांगणार नाहीत.

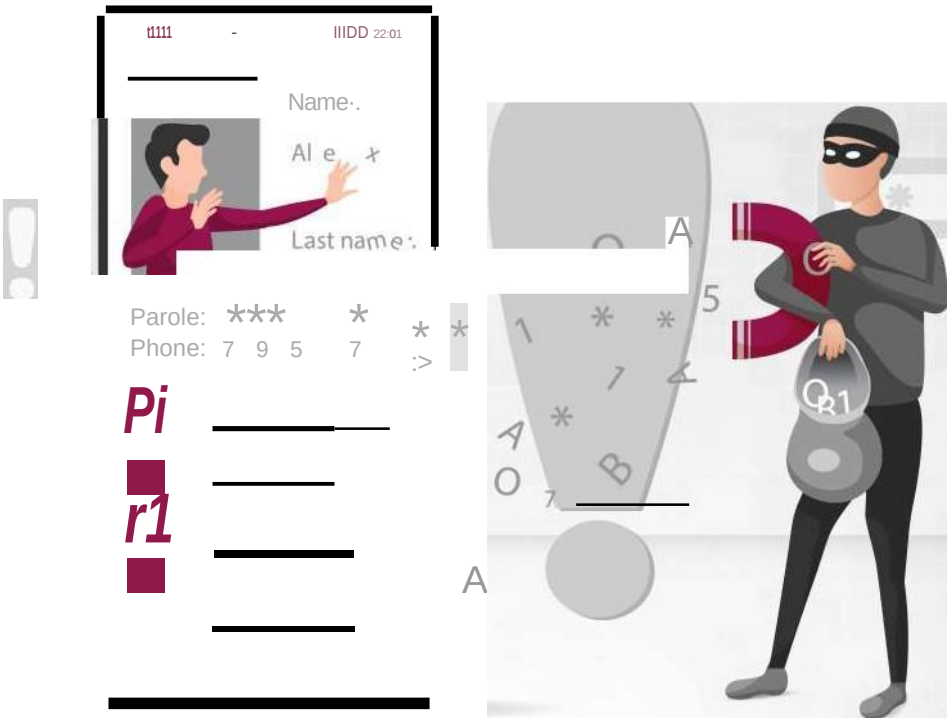
धोक्याच्या खुणांकडे लक्ष द्या: नोकरीसाठी तुम्हाला तुमचा सोशल सिक्युरिटी क्रमांक किंवा आर्थिक तपशील यासारखी संवेदनशील माहिती त्वरित प्रदान करण्याची आवश्यकता असल्यास सावध रहा.

खूप घाईने नियुक्ती: तुम्हाला नोकरीची ऑफर मुलाखतीशिवाय किंवा जास्त माहितीची देवाणघेवाण न करता तत्काळ दिली असल्यास, तो घोटाळा असू शकतो.

आपल्या अंतःप्रेरणे विश्वास ठेवा: काहीतरी गडबड वाटत असल्यास, आपल्या अंतःप्रेरणे वर विश्वास ठेवा आणि सावधगिरीने पुढे जा किंवा बाहेर पडा.

लक्षात ठेवा, नोकरी शोधताना तुमची वैयक्तिक आणि आर्थिक माहिती सुरक्षित ठेवणे हे तुमचे पहिले प्राधान्य असले पाहिजे.

कॉल फसवणूक घोटाळे



जादूगार कसे गोष्टी प्रत्यक्षात आहेत त्यापेक्षा वेगळ्या दाखवू शकतात, त्याचप्रमाणे घोटाळेबाज तुमच्या कॉलर आयडीमध्ये फेरफार करून असे भासवू शकतात की ते तुमच्या ओळखीचे किंवा विश्वासातील व्यक्ती आहेत - या प्रकरणात, तुमची बँक. हे त्यांच्या खऱ्या ओळखीसाठी डिजिटल वेषांतर करण्यासारखे आहे.

या चोरट्या युक्तीपासून स्वतःचे संरक्षण करण्यासाठी, पुढील सूचना लक्षात ठेवा:

सावधगिरी बाळगून पडताळणी करा: जरी कॉलर आयडी ओळखीचा वाटत असला तरीही, संशयी रहा. जर कोणी संवेदनशील माहिती विचारली, तर त्यांची ओळख इतर माध्यमातून पुन्हा तपासा.

वैयक्तिक माहिती शेअर करू नका: फोनवर कधीही वैयक्तिक किंवा आर्थिक माहिती देऊ नका, जरी कॉलर कायदेशीर वाटत असेल तरीही. हँग अप करा आणि विश्वसनीय नंबर वापरून परत कॉल करा.

खाजगी रहा: तुम्ही कोणते वैयक्तिक तपशील ऑनलाइन किंवा सोशल मीडियावर शेअर करता याविषयी सावधगिरी बाळगा. घोटाळेबाज अनेकदा त्यांचे फसवणूक करण्यासाठी केलेले कॉल अधिक खात्रीशीर बनवण्यासाठी या स्त्रोतांकडून माहिती गोळा करतात.

कॉल ब्लॉकिंग चा वापर करा: तुमच्या फोन कॅरीअरने प्रदान केलेली कॉल-ब्लॉकिंग ॲप्स किंवा वैशिष्ट्ये एक्सप्लोर करा. ती संभाव्य स्कॅम कॉल फिल्टर करण्यात मदत करू शकतात.

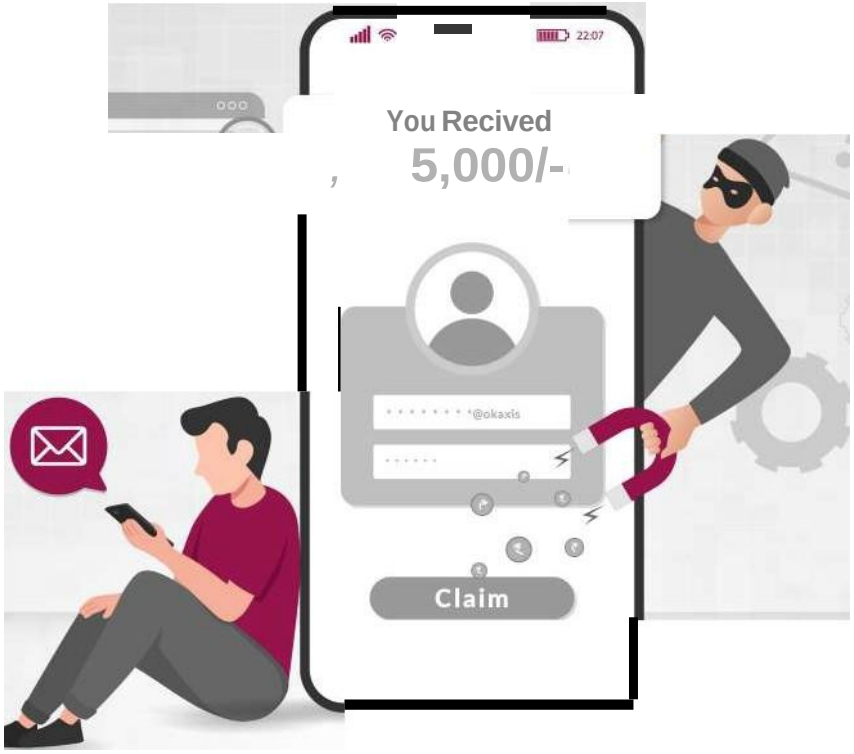
गुगल किंवा कोणत्याही सर्च इंजिनवर फोन नंबर शोधू नका. तुम्ही असे केल्यास, तुम्हाला संस्थेने किंवा मार्चंटने पाठवलेल्या कोणत्याही लिंकवर क्लिक करू नका.

याव्यतिरिक्त, कृपया याची खात्री करा की तुमच्याकडे बँकिंग ॲप्लिकेशन्सच्या नवीनतम आवृत्त्या तुमच्या डिव्हाइसवर फक्त अधिकृत ॲप्लिकेशन स्टोअरवरून डाउनलोड केल्या गेल्या आहेत.

कृपया हे वेळोवेळी तपासा.

लक्षात ठेवा, ज्याप्रमाणे तुम्ही वास्तविक जीवनात मुखवटा घातलेल्या अनोळखी व्यक्तीवर विश्वास ठेवणार नाही, त्याचप्रमाणे फोनवर मुखवटा घातलेल्या कॉलरवर देखील विश्वास ठेवू नका. सतर्क राहा!

UPI परतावा घोटाळे



कल्पना करा की तुम्ही तुमच्या फोनवर स्क्रोल करत आहात आणि तुम्हाला UPI रिफंड नोटिफिकेशन दिसले आणि अचानक तुम्हाला खूपच आनंद होतो! पण थांबा. हा UPI परतावा घोटाळा असू शकतो!

UPI किंवा युनिफाइड पेमेंट्स इंटरफेस हे आपल्या दैनंदिन जीवनाचा एक भाग बनले आहे. तुमच्या स्थानिक किराणा दुकानामध्ये पैसे देण्यापासून ते फोन रिचार्ज करणे ते फ्लाइट तिकीट बुक करण्यापर्यंत, आपण विविध गोष्टींसाठी UPI पेमेंटचा वापर करतो. त्यामुळे घोटाळेबाजांनी UPI ॲप्स वापरून लोकांना फसवण्यासाठी नवीन पद्धती अवलंबण्यास सुरुवात केली आहे.

त्यांच्या अधिकृत शब्दप्रयोगाला आणि व्यावसायिक भाषेला कधीही बळी पडू नका. खालील सूचना लक्षात ठेवा:

लिंक्सबाबतीत सावध रहा: घोटाळेबाज तुम्हाला लिंक पाठवू शकतात आणि तुम्हाला परतावा मागण्यासाठी नोंदणी करण्यास उद्युक्त करू शकतात.

उच्च-दबाव तत्रे: ते तुमच्यावर झटपट पैशासाठी बँक तपशील किंवा UPI पिन भरण्यासाठी दबाव टाकतील.

पात्रता पडताळून पहा: तुम्ही परताव्यासाठी पात्र आहात याची खात्री करा आणि असाल तर स्त्रोत विश्वसनीय आहे का ते तपासा.

लक्षात ठेवा, बँक किंवा इतर अधिकारी तुम्हाला असे संवेदनशील तपशील कधीच विचारणार नाहीत.

फिशिंग घोटाळे

कल्पना करा की तुम्ही स्वच्छ तलावात शांतपणे पोहत असलेला मासा आहात आणि स्वतःच्या जगात व्यस्त आहात. अचानक, एक चमकदार, मोहक आमिष तुमच्यासमोर लटकते. तुम्हाला खूप उत्सुकता आहे पण थांबा - काहीतरी गडबड आहे!

डिजिटल क्षेत्रामध्ये फिशिंग स्कॅमच्या बाबतीमध्ये अगदी हेच घडते.

सायबर गुन्हेगार एखाद्या माशाला जसे आमिष दाखविले जाते त्याप्रमाणे तुम्हाला संवेदनशील माहिती उघड करण्याकरिता फसवण्यासाठी विश्वासार्ह व्यक्ती म्हणून बनाव करतात. ते बनावट ईमेल, मॅसेज किंवा कायदेशीर वाटणाऱ्या वेबसाइट पाठवतात, अनेकदा बँका, सोशल मीडिया किंवा तुमच्या बॉसचे देखील अनुकरण करतात.

या डिजिटल हुकपासून बचाव करण्यासाठी, या सूचना लक्षात ठेवा:

URLs दोनदा तपासा: लिंक्स कुठे नेत आहेत हे पाहण्यासाठी त्यांच्यावर हॉवर करा.

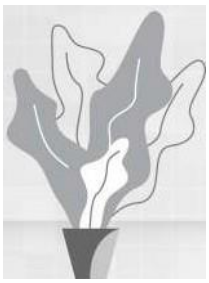
वैयक्तिक माहिती शेअर करू नका: कायदेशीर संस्था ईमेलद्वारे संवेदनशील सामग्रीची मागणी करत नाहीत.

संशयी रहा: अनपेक्षित विनंत्या? कृती करण्यापूर्वी इतर माध्यमांद्वारे पडताळणी करा.

सुरक्षा सॉफ्टवेअर अपडेट करा: तुमचे डिजिटल जग नवीनतम संरक्षणासह संरक्षित ठेवा.

एखाद्या सावध माशाप्रमाणे, सावध रहा आणि इंटरनेटच्या विशाल समुद्रात हुशारीने पोहा!

विशींग घोटाळे



a

तुमचा फोन वाजतो, आणि तुमच्या खात्याशी तडजोड झाल्याचा दावा करणारा 'अर्जंट' कॉल असलेली तुमची तथाकथित बँक आहे, किंवा कदाचित हा तुमचा भाग्यशाली दिवस असल्याचा दावा करणारा 'विजेता' कॉल आहे आणि तुम्ही एक सरप्राईज जिंकला आहात!

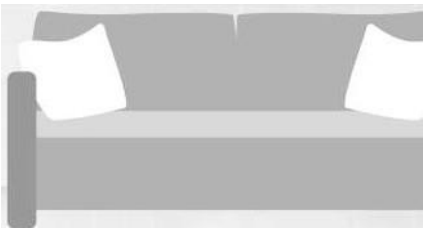
फोन होल्ड करा (अक्षरशः)!

अशा घोटाळ्यांपासून सुरक्षित राहण्यासाठी खालील सूचना लक्षात ठेवा:

- तुमचे वैयक्तिक तपशील कधीही फोनवर प्रसारित करू नका.
- शेरलॉक होम्स व्हा आणि त्या कॉलरची ओळख पडताळून पहा.
- नाटकाला बळी पडू नका! जेव्हा ते गरम होतात तेव्हा तुम्ही थंड रहा.

अनोळखी व्यक्तींसोबत ऑनलाइन माहिती शेअर करताना सावधगिरी बाळगण्याचे लक्षात ठेवा - तुमच्या गोष्टी सुरक्षित ठेवण्यासाठी हुषारीने रहा!

UPI घोटाळे – पैशांची विनंती करणारा पर्याय



स्नेहाने ऑनलाइन खरेदी आणि विक्री ॲपवर तिच्या फर्निचरची जाहिरात केली. निमलष्करी दलाचे कर्मचारी असल्याचा दावा करणाऱ्या एका खरेदीदाराने व्हॉट्सॲपवर पेमेंटसाठी QR कोड पाठवला. स्नेहाने तो स्कॅन केला आणि 75,000 गमावले.
हे ओळखीचे वाटते का? तुम्ही UPI पेमेंट प्लॅटफॉर्मचा वारंवार वापर केल्यामुळे तुम्हाला UPI फसवणुकीला बळी पडण्याची भीती वाटते आहे का?
नेहमी लक्षात ठेवा:

UPI PIN केवळ पैसे देण्यासाठी आवश्यक असतो, पैसे प्राप्त करण्यासाठी नाही.

ज्या क्षणी पैसे प्राप्त करण्यासाठी तुमचा UPI PIN देण्यास सांगितले जाईल, थांबा! प्रत्यक्षात ही पैसे देण्यासाठीची विनंती असू शकते, पैसे प्राप्त करण्याची नाही.

तुमचा OTP, UPI PIN किंवा कोणतेही गोपनीय तपशील कोणाही सोबत शेअर करू नका.

कोणतेही पेमेंट सुरू करण्यापूर्वी नेहमी UPI ॲप्लिकेशनमधील मोबाइल क्रमांक आणि नाव यांची पडताळणी करा.

QR कोड स्कॅन घोटाळा

पेमेंट ॲप वरील QR कोड सावधगिरीने स्कॅन करा; त्यात पैसे ट्रान्सफर करण्यासाठीचे खात्याचे तपशील असतात.

QR कोड पैसे प्राप्त करण्यासाठी स्कॅन करू नका; बारकोड/ QR कोड स्कॅन करणे किंवा मोबाईल बँकिंग PIN (m-PIN), पासवर्ड इ. प्रविष्ट करणे पैसे प्राप्त करण्यासाठीच्या व्यवहारांमध्ये अनावश्यक आहे.

अवास्तव घाई किंवा तत्परता दाखवणारा खरेदीदार/विक्रेता बहुधा फसवणूक करणारा असतो. संयम ठेवा, नेहमी स्पष्टीकरण शोधा आणि आवश्यक चौकशी करा.

असत्यापित मोबाइल ॲप फसवणूक

तुम्हाला बऱ्याच कालावधीसाठी संपर्कात नसलेल्या एका चुलत भावा किंवा बहिणी तर्फे SMS, ईमेल किंवा मॅसेज प्राप्त होतो आणि हे सर्व तुमच्या आवडत्या अधिकृत संस्थेच्या कायदेशीर ॲपसारख्या दिसणाऱ्या लिंकसह केलेले असते.

एक मिनिट थांबा! हे चांगले डाउनलोड नाहीत; ती एका डिजिटल पार्टीसाठी आमंत्रणे आहेत ज्यात तुम्ही नक्कीच उपस्थित राहू इच्छित नाही!

घोटाळेबाज SMS, ईमेल किंवा सोशल मीडियाद्वारे बनावट ॲप लिंक पाठवतात जी अस्सल असल्या सारखीच दिसते. ते वापरकर्त्यांना त्यावर क्लिक करण्यास प्रवृत्त करतात, ज्यामुळे अज्ञात ॲप्स डाउनलोड होतात. एकदा इन्स्टॉल केल्यानंतर, स्कॅमर गोपनीय माहिती आणि OTP सह डिव्हाइसचा ॲक्सेस मिळवतात.

अज्ञात स्त्रोतांकडून किंवा अनोळखी व्यक्तींच्या विनंतीवरून ॲप्स डाउनलोड करणे टाळा.

डाउनलोड करण्यापूर्वी ॲप प्रकाशक आणि वापरकर्ता रेटिंग यांची पडताळणी करा.

परवानग्या आणि ॲप विनंत्यांचे पुनरावलोकन करा (उदा. संपर्क, फोटो) आणि केवळ आवश्यक असेल ते मंजूर करा.

लक्षात ठेवा, बँक किंवा इतर अधिकारी तुम्हाला असे संवेदनशील तपशील कधीच विचारणार नाहीत.

ATM कार्ड स्किमिंग घोटाळा

ATM स्किमिंग म्हणजे डिजिटल पाकीटमारी असते असे समजा. तुम्ही पैसे काढण्यासाठी किंवा तुमची शिल्लक तपासण्यासाठी ATM वापरत असताना, फसवणूक करणारे तुमची कार्ड माहिती रेकॉर्ड करण्यासाठी मशीनवर छुपी उपकरणे सेट करतात. ही उपकरणे बनावट कार्ड स्लॉट किंवा लहान कॅमेऱ्यासारखी शंका येणार नाही अशी असू शकतात.

ATM ची तपासणी करा: ATM वापरण्यापूर्वी नेहमी कार्ड स्लॉट आणि कीपॅड काही असामान्य जोडणी, सुटे भाग किंवा छुपे कॅमेरे यासाठी तपासा.

तुमचा **PIN** झाका: तुमची PIN एंट्री तुमच्या हाताच्या किंवा शरीराच्या सहाय्याने संरक्षित करा, ज्यामुळे कॅमेरा किंवा कोणी पाहत असल्यास ते पाहणे कठीण होईल.

स्टेटमेंट नियमितपणे तपासा: तुमची बँक स्टेटमेंट्स आणि व्यवहारांवर लक्ष ठेवा. तुमच्या बँकेला कोणत्याही अपरिचित गोष्टीची त्वरित तक्रार करा.

कॉल्सपासून सावध रहा: तुमच्या बँकेतील असल्याचा दावा करणारी कोणी व्यक्ति कॉल करून संवेदनशील माहिती विचारत असल्यास, सावध रहा. बँका PIN किंवा पूर्ण कार्ड क्रमांक फोनवर क्वचितच मागतात.

सुरक्षित ATMs चा वापर करा: उत्तम प्रकाश असलेल्या किंवा बँक शाखांशी संलग्न असलेल्या ATMची निवड करा, कारण त्यांच्याशी छेडछाड होण्याची शक्यता कमी असते.

अपडेट रहा: स्वतःचे अधिक चांगले संरक्षण करण्यासाठी नवीनतम घोटाळे आणि फसवणूकीच्या युक्त्यांबद्दल माहिती मिळवा.

लक्षात ठेवा, सतर्क राहणे आणि या सुचनांचे पालन केल्याने तुम्हाला ATM कार्ड स्किमिंग फसवणुकीला बळी पडणे टाळता येईल आणि तुमची आर्थिक स्थिती सुरक्षित ठेवता येईल.

रिमोट ॲक्सेस फसवणूक

स्कॅमर ग्राहकांना स्क्रीन शेअरिंग ॲप डाउनलोड करण्याचे आमिष दाखवतात. त्यासह, ते तुमच्या डिव्हाइसमध्ये डोकावतात, तुमची हेरगिरी करतात आणि तुमची आर्थिक माहिती स्वाइप करतात. मग, ते तुमच्या पैशाने खरेदी करतात!

अशा घोटाळ्यांपासून दूर राहण्यासाठी, या सूचना लक्षात ठेवा:

कॉलर्सची पडताळणी करा: नेहमी कॉलर्स ज्या संस्थेचे प्रतिनिधित्व करत असल्याचा दावा करतात त्या संस्थेची अधिकृत संपर्क माहिती स्वतंत्रपणे शोधून कॉलरची ओळख दोनदा तपासा.

घाईगर्दीत निर्णय नाही: दबावाखाली आवेगपूर्ण निर्णय घेऊ नका. ॲक्सेस मंजूर करण्यापूर्वी किंवा संवेदनशील माहिती शेअर करण्यापूर्वी विचार करण्यासाठी आणि पडताळून पाहण्यासाठी आपला वेळ घ्या.

तुमची डिव्हाईस सुरक्षित करा: नवीनतम सुरक्षा पॅचसह तुमचे डिव्हाइस अपडेटेड ठेवा आणि प्रत्येक खात्यासाठी मजबूत, अद्वितीय पासवर्ड वापरा.

स्वतःला शिक्षित करा: सामान्य घोटाळे आणि डावपेचांबद्दल जाणून घ्या जेणेकरुन ते घडल्यावर तुम्ही त्यांना ओळखू शकता.

वैयक्तिक माहितीचे रक्षण करा: तुम्हाला वैयक्तिक किंवा आर्थिक तपशील शेअर करण्याबाबत विनंतीच्या वैधतेबद्दल खात्री असल्याशिवाय फोन, ईमेल किंवा ऑनलाइन सावधानता बाळगा.

तुमच्या डिजिटल जीवनात डोकावून पाहणाऱ्या रिमोट ऍक्सेस फसवणूक करणाऱ्यांविरुद्ध व्हर्च्युअल दरवाजा बंद ठेवण्यासाठी सतर्क रहा.

कृपया नोंद घ्या - जर तुम्हाला काळी / रिकामी स्क्रीन दिसली तर, कृपया तुमच्या सिस्टमवर कारवाई करण्यायोग्य कोणतीही प्रक्रिया करू नका. हे तुमची स्क्रीन इतरांना दिसत असल्याचे लक्षण असू शकते.

SIM स्वॅप फसवणूक

कल्पना करा की स्कॅमर फोनवरुन चोरी करत आहेत! ते तुम्ही असल्याचे भासवतात आणि त्यांचे सिमकार्ड हरवले आहे असे संगतात, आणि झाले त्यांना तुमचा क्रमांक मिळतो. त्याचा वापर करून ते तुमच्या बँक किंवा ईमेल सारख्या तुमच्या ऑनलाइन खात्यांमध्ये धडक देतात आणि अराजक माजवतात!
स्वॅप स्कॅम थांबवा! खालील सूचना लक्षात ठेवा.

सिम कार्ड ओळख तपशील शेअर करू नका.

तुमच्या फोनच्या नेटवर्क ऍक्सेसचे निरीक्षण करा.

काही काळ नेटवर्क नसल्यास, डुप्लिकेट SIM विषयीची तपासणी करण्यासाठी तुमच्या ऑपरेटरशी संपर्क साधा.

तुमच्या डिजिटल जीवनात डोकावून पाहणाऱ्या रिमोट ऍक्सेस फसवणूक करणाऱ्यांविरुद्ध व्हर्च्युअल दरवाजा बंद ठेवण्यासाठी सतर्क रहा.

फसवणुकीच्या व्यवहाराची तक्रार कशी करावी?

भेट द्या **www.axisbank.com** > सपोर्ट > 'रिच अस हिअर' विभागापर्यंत स्क्रोल करा > टॉक टू अस > निवडा 'रिपोर्ट अ फ्रॉड ऑर डिस्प्यूट' > रिपोर्ट अ फ्रॉड > ड्रॉप-डाउन सूचीमधून तुमच्या शंकेशी संबंधित पर्यायाची निवड करा > कॉल वर क्लिक करा

RBI कडे तक्रार करण्यासाठी, भेट द्या https://cms.rbi.org.in

टोल-फ्री क्रमांक 14448 वर संपर्क करा (सोमवार ते शुक्रवार, सकाळी 9:30 ते संध्याकाळी 5:15, राष्ट्रीय सुट्ट्या वगळून).

भौतिक तक्रार पाठवा: पत्र पाठवा 'केंद्रीकृत प्राप्ती आणि प्रक्रिया केंद्र, 4था मजला, भारतीय रिझर्व्ह बँक, सेक्टर -17, सेंट्रल व्हिस्टा, चंदीगड - 160 017'. आवश्यक स्वरूपाच्या अधिक तपशीलासाठी **कृपया भेट द्या** https://cms.rbi.org.in.

सायबर गुन्ह्याची तक्रार करण्यासाठी, मदत क्रमांक **155260** किंवा **1930 डायल करा किंवा** घटना नॅशनल सायबर क्राईम रिपोर्टिंग पोर्टल **(www.cybercrime.gov.in)** वर रिपोर्ट करा.
