बँकिंग ध्यान से

ह्या उपक्रमातून सावध रहा आणि बँकेचे सुरक्षित व्यवहार करा

AXIS BANK

ॲक्सिस बँकेचा ग्राहक सेवा उपक्रम

परिचय

ही पुस्तिका तयार करताना आरबीआय ओंबडसमनच्या (मुंबई– II), महाराष्ट्र, गोवा कार्यालयाने प्रकाशित केलेल्या 'ए बुकलेट ऑन मोडस ऑपरेंडी ऑफ फायनान्शिअल फ्रॉडस्टर्स' ह्या पुस्तकात दिलेल्या माहितीचा आणि ह्या संदर्भातील आमच्या इन–हाउस संशोधनाचा आधार घेण्यात आला आहे.

प्रस्तावना

बँकिंग यंत्रणांचे डिजिटलायझेशन झाल्यामुळे ग्राहकांना आपल्या आर्थिक आवश्यकता सहजपणे आणि जलदपणे पूर्ण करण्यासाठी नवीन माध्यमं तयार झाली आहेत. सध्याच्या परिस्थितीनेही शारीरिक आणि सामाजिक संपर्क कमी करण्यासाठी आम्हाला डिजिटल व्हायला प्रोत्साहन दिलं आहे.

डिजिटल बँकिंगची सुविधा पुरवताना आम्हाला आनंद होत आहे, पण त्यासोबत सायबर गुन्हे आणि बँकिंग फ्रॉड्सलाही तोंड द्यावं लागत आहे. अनेकवेळा ग्राहक न कळत ह्या गुन्ह्यांचे बळी ठरतात आणि सावध न राहिल्यामुळे त्यांना आर्थिक नुकसान सोसावं लागतं.

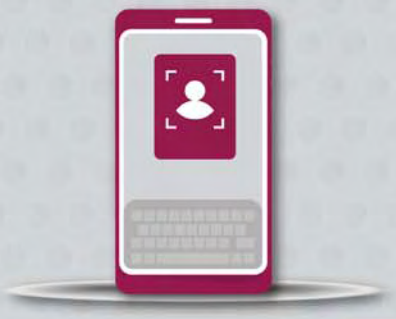
ॲक्सिस बँकेमध्ये आम्ही तुमची पूर्ण काळजी घेतो. वेळोवेळी उपयोगी माहिती देऊन तुमचं हित जपण्यासाठी मदत करतो.

ह्या पुस्तिकेतून आम्ही जागरुकता निर्माण करत आहोत. सध्या चालू असलेल्या संशयास्पद आणि भ्रष्ट कृतींचा तुम्हाला परिचय करून देत आहोत. त्यासाठी आम्ही काही भ्रष्ट कृतींचे उदाहरण दिले आहे आणि त्या कशा ओळखायच्या ते सांगितले आहे. अशा कृती रोखण्यासाठी कोणती काळजी घ्यावी, त्यांची सूचना कशी द्यावी हेसुध्दा सूचवले आहे. तुम्ही सावध राहिलात तर तुम्ही बळी पडण्याची शक्यता कमी होईल आणि तुमचं आर्थिक नुकसान होणार नाही.

आम्हाला विश्वास आहे की ही माहिती तुम्हाला खूप उपयोगी पडेल. जेव्हा तुम्ही सावधपणे बँकिंग कराल तेव्हा सुरक्षिततेचा आनंद घ्याल आणि तुम्हाला अडचण येत नसल्याचा चांगला अनुभवही मिळेल.

सुरक्षित रहा!

आम्ही इथे काही सामान्य सावधगिरीच्या सूचना आणि चांगल्या कार्यपध्दतींची माहिती देत आहोत:



हे टाळा

- असुरक्षित वेबसाइट्सवर भेट देऊ नका किंवा अनोळखी ब्राउजर्स वापरू नका
- सार्वजनिक डिवाइसेसवर पासवर्ड सेव करू नका
- सार्वजनिक किंवा मोफत नेटवर्क्सवर आर्थिक/गोपनीय ई-मेल्सचा वापर करू नका
- संशयास्पद वाटणाऱ्या पॉप अप्स, लिंक्स आणि अनोळखी स्रोतांकडून आलेल्या ई-मेल्सवर क्लिक करू नका
- ई-मेल्स किंवा अनोळखी वेबसाइट्सवर सुरक्षित माहिती किंवा पासवर्ड्स स्टोअर करू नका
- समाज माध्यमावरील अनोळखी व्यक्तींकडे खासगी माहिती देऊ नका
- बँकिंग आणि इतर व्यवहारांसाठी समान पासवर्ड वापरू नका
- अनोळखी ॲप्लिकेशन्स किंवा सॉफ्टवेअर इंस्टॉल करू नका
- तुमचा मोबाइल किंवा इतर इलेक्ट्रॉनिक डिवाइसेस अथवा ॲप्स अनलॉक अवस्थेत ठेवू नका

हे कधीही करू नका

- आपला पिन (वैयक्तिक ओळख क्रमांक), पासवर्ड, क्रेडिट किंवा डेबिट कार्डाचे नंबर्स, सीव्हीव्ही, चेक बुकची प्रत, केव्हायसीचा तपशील कोणालाही देऊ नका
- अनोळखी डिवाइसेसवर संवेदनशील किंवा गोपनीय माहिती साठवू नका

हे नेहमी करा

- सशक्त स्क्रीन पासवर्ड वापरून तुमचा फोन सुरक्षित करा
- जिथे शक्य असेल/उपलब्ध असेल तिथे टू-फॅक्टर ऑथेंटिकेशन करा
- वापर केल्यानंतर तात्काळ इंटरनेट बँकिंग सेशनमधून लॉग आउट करा
- एनॅबल किंवा डिसॅबल फिचर वापरा आणि तुमच्या वापरानुसार तुमच्या कार्डावर किंवा खात्यावर व्यवहाराची मर्यादा सेट करा
- पॅडलॉक्स किंवा https अशी सुरक्षित चिन्ह पाहून वेबसाइटच्या सुरक्षिततेची पडताळणी करा
- ऑनलाइन पेमेंट्स करताना सुरक्षित पेमेंट गेटवेजचा वापर करा
- आकडे-शब्द आणि स्पेशल कॅरेक्टर्सच्या मिश्रणातून तयार झालेला सशक्त पासवर्ड वापरा आणि तो नियमित बदला
- सार्वजनिक डिवाइसेसवर वर्चुअल कीबोर्ड वापरा. कारण डिवाइसेस, कीबोर्ड इत्यादीमध्ये छेडछाड करून कीस्ट्रोक्स मिळवले जाण्याची शक्यता असते
- तुमच्या डिवासेसवर अँटीवायरस आणि अँटी स्पायवेअर इंस्टॉल करा, ते अद्ययावत ठेवा आणि उपलब्ध असतील तेव्हा अपडेट्स इंस्टॉल करा
- वापर करण्याआधी कोणतही यूएसबी डिवाइस/स्टोअरेज डिवाइस स्कॅन करा
- तुमचे मोबाइल ॲप्स पासवर्डने सुरक्षित करा किंवा मोबाइल फोनमधील हिडन स्पेसेसचा वापर करून त्यांचं सामान्य रूप बंद करा

#BankingDhyaanSe

ऑनलाइन/वेबसाइटवरील भ्रष्टाचाराबाबत (1)

गुन्ह्याची पध्दत

तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

ऑनलाइन लूट करण्याच्या पध्दती

कसं लुटतात

- भ्रष्ट व्यक्ती एक वेबसाइट तयार करते, जी बँकेच्या खऱ्या वेबसाइटसारखी दिसते
- ह्या वेबसाइट्सच्या लिंक्स एसएमएस, समाज माध्यमे, ई-मेल इत्यादीद्वारे पसरवल्या जातात
- ह्या वेबसाइट अधिकृत वेबसाइट असल्याचे दाखवले जाते आणि अशी युक्ती केली जाते की लिंक पाहाताच तुम्ही तपशीलवार यूआरएल न तपासता तुमचा तपशील किवा संवेदनशील आणि गोपनीय माहिती देता.
- तुम्ही ह्या वेबसाइट्सवर तपशील एंटर केल्यानंतर, भ्रष्ट व्यक्ती तो कॅप्चर करून त्याचा गैरवापर करतात

सुरक्षिततेच्या सूचना

- अनोळखी लिंक्स अधिकृत वाटत असल्या तरी त्या टाळा
- आर्थिक तपशील देण्याआधी वेबसाइटची माहिती नीट तपासून घ्या

ऑनलाइन फसवणूक

कशी करतात

- भ्रष्ट व्यक्ती ऑनलाइन, ईकॉमर्स प्लॅटफॉर्म्सवर आपण कायदेशीर खरेदीकर्ता/विक्रीकर्ता असल्याचं ढोंग करतात
- तुमच्या प्रॉडक्टमध्ये रुची दाखवतात किंवा मोठी सूट देऊन किंवा सवलत देऊन तुम्हाला त्यांच्याकडून खरेदी करायला भाग पाडतात
- पेमेंट करण्याऐवजी ते तुम्हाला यूपीआय 'रिक्वेस्ट मनी' पर्यायाचं आमिष दाखवतात आणि तुमच्या बँक खात्यातून पैसे लुबाडतात

सुरक्षिततेच्या सूचना

- ऑनलाइन प्रॉडक्ट्सचा आर्थिक व्यवहार करताना सावध रहा
- पैसे प्राप्त करताना तुम्हाला कधीही पिन किंवा पासवर्ड एंटर करायला सांगितले जात नाही

ऑनलाइन/वेबसाइटवरील भ्रष्टाचाराबाबत (2)

गुन्ह्याची पध्दत

तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

संशयास्पद सर्च इंजिन रिझल्ट्स

कसे केले जाते

- भ्रष्ट व्यक्तींकडून कंपन्यांच्या कस्टमर केअरमध्ये हस्तक्षेप केला जातो आणि समाज माध्यमाच्या प्लॅटफॉर्म्सवर सर्च रिझल्ट्समध्ये ते वरच्या भागात आपला बनावट नंबर टाकतात
- तुमच्या बँकेच्या कस्टमर केअरच्या संपर्काचा तपशील किंवा इतर आर्थिक माहिती/संस्था ऑनलाइन शोधताना तुम्ही दिलेला तपशील खरा आहे असे समजता आणि अनावधानाने सदर बेकायदेशीर/बनावट नंबर्सवर संपर्क करता
- तुम्ही तुमची वैयक्तिक किंवा गोपनीय आणि आर्थिक माहिती देऊन भ्रष्ट व्यक्तींच्या कारस्थानाला बळी पडता

सुरक्षिततेच्या सूचना

- सर्च इंजिनवर कस्टमर केअरच्या संपर्काचा तपशील शोधू नका. कारण भ्रष्ट व्यक्तींनी कारस्थान करण्यासाठी त्यात ढवळाढवळ केलेली असू शकते
- बँका/कंपन्यांच्या संपर्काच्या खऱ्या तपशीलासाठी नेहमी अधिकृत वेबसाइट्स पहा

स्क्रीन शेअरिंग/रिमोट ॲक्सेस

हे कसे केले जाते

- तुम्हाला स्क्रीन शेअरिंग ॲप्स डाउनलोड करायला लावून भ्रष्ट व्यक्ती तुमच्या लॅपटॉप/मोबाइल डिवाइसवरील तुमची वैयक्तिक माहिती आणि आर्थिक तपशील मिळवतात व त्यानंतर तुमचं बँकिंग आणि पेमेंट ॲप वापरून पेमेंट्स करतात

सुरक्षिततेच्या सूचना

- कोणत्याही अनोळखी व्यक्तीने स्क्रीन शेअरिंग ॲप्स डाउनलोड करायला सांगितलं तर तसं करू नका
- बँकिंग किंवा आर्थिक ॲपवर अथवा वेबसाइटवर लॉगिन करण्याआधी तुम्ही सर्व स्क्रीन शेअरिंग ॲप्लिकेशन खंडित केल्याची खात्री करा

#BankingDhyaanSe

कॉल/मोबाइल भ्रष्टाचाराबाबत (1)

गुन्ह्याची पध्दत
तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

माहिती चोरणारे कॉल्स

कसे केले जातात

- भ्रष्ट व्यक्ती ग्राहकाला टेलिफोन कॉल्स/सामाजिक माध्यमातून संपर्क करते आणि आपण बँकेचे अधिकारी इत्यादी असल्याचे सांगते व बँकेचा टोल फ्री किंवा कस्टमर केअर नंबर देते
- कॉल करणारी व्यक्ती ग्राहकावर दबाव आणते आणि गोपनीय तपशील किंवा ओटीपी मागते. त्यासाठी सेवा तात्काळ खंडित होईल, केव्हायसी पूर्तता झाली नाही, खाते/कार्ड इत्यादी बंद होईल अशी आणीबाणीची विविध कारणे सांगते
- ग्राहकाने दिलेल्या तपशीलाचा गैरवापर करून ग्राहकाच्या खात्यात भ्रष्ट व्यवहार केला जातो

सुरक्षिततेच्या सूचना

- बँक/कोणतीही खरी व्यक्ती तुम्हाला कधीही यूझरनेम, पासवर्ड, कार्डाचा तपशील, पिन, सीव्हीव्ही, ओटीपी इत्यादी गोपनीय माहिती कधीही विचारत नाही

मोबाइल ॲपचा भ्रष्टाचार

कसा केला जातो

- तुमच्या मोबाइल, लॅपटॉप किंवा डेस्कटॉपवर खात्री न झालेला ॲप डाउनलोड करण्याचं आमिष दाखवलं जातं
- ह्या ॲप्सच्या लिंक्स दिल्या जातात किंवा एसएमएस, सामाजिक माध्यमे इत्यादीद्वारे पुरवल्या जातात.
- हे भ्रष्ट ॲप्लिकेशन्स असतात, ज्यामुळे भ्रष्ट व्यक्तीला तुमच्या डिवाइसवर संपूर्ण नियंत्रण मिळतं

सुरक्षिततेच्या सूचना

- खात्री न केलेल्या/अनोळखी स्रोतांकडून कधीही ॲप्लिकेशन डाउनलोड करू नका
- डाउनलोड केलेल्या लिंकवर नकळत क्लिक होऊ नये ह्यासाठी अनोळखी स्रोतांकडून आलेले एसएमएस/ई-मेल डिलिट करा

कॉल/मोबाइल भ्रष्टाचाराबाबत (2)

गुन्ह्याची पध्दत
तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

ओटीपी आधारित भ्रष्टाचार

कसा केला जातो

- भ्रष्ट व्यक्ती तुम्हाला एसएमएस पाठवते. ज्यात बँकेकडून कर्ज दिलं जात असल्याचं किंवा क्रेडिट मर्यादा वाढवली जात असल्याचं सांगितलं जातं आणि मेसेजमध्ये दिलेल्या क्रमांकावर तुम्हाला संपर्क करायला सांगितलं जातं
- तुम्ही त्या क्रमांकावर कॉल केल्यावर तुम्हाला काही फॉर्म्स (ऑनलाइनसुध्दा) भरायला सांगितलं जातं. ज्यामुळे तुमचा अर्थिक तपशील ते मिळवू शकतात. त्यासाठी ते ओटीपी किंवा पिनचा तपशील मागतात आणि तुमचं आर्थिक नुकसान होतं

सुरक्षिततेच्या सूचना

- तुमचा ओटीपी, पिन किंवा पासवर्डचा तपशील कोणत्याही स्वरूपात कोणालाही देऊ नका
- तुमचा एसएमएस/ई-मेल्स नियमितपणे तपासून तुमच्या माहितीशिवाय कोणताही ओटीपी तयार झाला नसल्याची खात्री करा

माहिती चोरली जाणे

कशी चोरतात

- माहिती चोरण्यासाठी सायबरचा उपयोग केला जातो. तुमचा मोबाइल कोणत्याही अनोळखी/खात्री न केलेल्या चार्जिंग पोर्ट्सला जोडला जातो, तुमच्या डिवाइसवर विशिष्ट अनोळखी ॲप्स/मालवेअर इंस्टॉल केलेले असतील तर भ्रष्ट व्यक्ती संवेदनशील माहिती, ई-मेल, एसएमएस आणि सेव केलेला पासवर्ड चोरू शकते किंवा त्यावर नियंत्रण मिळवू शकते

सुरक्षिततेच्या सूचना

- सार्वजनिक/अनोळखी चार्जिंग पोर्ट्स/केबल्स वापरू नका

#BankingDhyaanSe

कॉल/मोबाइल भ्रष्टाचाराबाबत (3)

गुन्ह्याची पध्दत
तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

सिम स्वॅप भ्रष्टाचार

कसा केला जातो

- तुमच्या रजिस्टर्ड मोबाइल नंबरवर तुमच्या खात्याचा तपशील आणि अधिकृतता जोडलेली असते. भ्रष्ट व्यक्ती तुमच्या नंबरचं नवीन रिप्लेसमेंट सिम कार्ड मिळवून ओटीपी आणि अॅलर्ट्स मिळवते व आर्थिक व्यवहार करते
- भ्रष्ट व्यक्ती तुमच्या मोबाइल ऑपरेटरच्या रिटेल आउटलेटला भेट देऊन तुम्ही स्वत: असल्याचं भासवते. त्यासाठी खोटा पुरावा देऊन तुमचं ओरिजनल सिम ब्लॉक करते आणि तुमच्या मोबाइल नंबरसह नवीन सिम घेते
- त्यानंतर, ती व्यक्ती तुमच्या ऑपरेटरने दिलेला एसएमएस पाठवून तुमचं सिम कार्ड अपडेट होत असल्याचं सांगते. ज्यामुळे तुमचं सिम डिअॅक्टिवेट होतं आणि तुमच्या मोबाइल नंबरसह सिम कार्डवर ते ताबा मिळवतात

सुरक्षिततेच्या सूचना

- तुमचा गोपनीय आणि वैयक्तिक तपशील चोरू पाहाणाऱ्या सोशल इंजिनिअरिंग स्कॅम्सपासून सावध रहा
- जर तुमच्या मोबाइल नंबरवर अचानक नेटवर्क कनेक्टिविटी दिसत नसेल तर तुमच्या मोबाइल सर्व्हिस प्रोवायडरकडे तात्काळ चौकशी करून तुमच्या सेवेचं स्टेटस जाणून घ्या. तुमच्या सिमसाठी दुसरं ड्युप्लिकेट सिम जारी झालं नसल्याची खात्री करा

इतर प्रकारच्या भ्रष्टाचाराबाबत (1)

गुन्ह्याची पध्दत
तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता ?

समाज माध्यमांद्वारे भ्रष्टाचार

कसा केला जातो

- भ्रष्ट व्यक्ती तुम्ही स्वत: असल्याचं भासवून प्रसिध्द समाज माध्यमावर नकली खातं तयार करते
- तुम्ही तुमचा अनलॉक्ड फोन दिल्यावर (इमर्जन्सी कॉल करण्यासाठी किंवा दुरुस्तीसाठी) किंवा तो बेवारस अवस्थेत ठेवल्यावर तुमच्या मोबाइलवर आलेला ओटीपी भ्रष्ट व्यक्तीला मिळतो. त्यामुळे ती तुमचा प्रोफाइल ॲक्सेस करते आणि काही ॲप्लिकेशन्सचं डेस्कटॉप वर्जन तयार करते व तुमचे संपर्क क्रमांक, ऑनलाइन प्रोफाइल व चॅट मेसेज मिळवते.
- तुमच्या मित्राला विनंती करून तात्काळ वैद्यकीय मदतीसाठी किंवा इतर कारणांसाठी पैशांची मागणी करते

सुरक्षिततेच्या सूचना

- पैसे देण्याआधी तुमच्या संपर्कातील व्यक्तींपर्यंत पोहोचून किंवा त्याला संपर्क करून विनंतीची अधिकृतता तपासा
- तुमचा फोन लॉक्ड केल्याशिवाय बेवारस अवस्थेत सोडू नका

क्यूआर स्कॅन–आधारित भ्रष्टाचार

कसा केला जातो

- भ्रष्ट व्यक्ती विविध स्वरूपात तुम्हाला संपर्क करते आणि तुम्हाला क्यूआर कोड स्कॅन करायला भाग पाडते. पेमेंट ॲप्स वापरून पेमेंटची प्रक्रिया पूर्ण करते
- ह्या क्यूआर कोड्समध्ये प्रीडिफाइंड खात्याचा तपशील असतो. भ्रष्ट व्यक्ती तुम्हाला तुमच्या खात्यातून कोणत्याही खात्यात पैसे हस्तांतरित करायला भाग पाडते

सुरक्षिततेच्या सूचना

- पेमेंट ॲप्स वापरून कोणताही क्यूआर कोड स्कॅन करताना सावध रहा

इतर प्रकारच्या भ्रष्टाचाराबाबत (2)

गुन्ह्याची पध्दत
तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

लॉटरी किंवा नोकरीसंबंधी भ्रष्ट घोटाळे

कसे केले जातात

- तुम्ही खूप मोठी लॉटरी/बक्षीस जिंकल्याचे किंवा प्रसिध्द कंपनीचे पद तुम्हाला दिले जात असल्याचे भासवून भ्रष्ट व्यक्ती तुम्हाला ई-मेल पाठवते किंवा फोन कॉल करते
- पैसे/बक्षीस प्राप्त करण्यासाठी किंवा निवडीची प्रक्रिया पूर्ण करण्यासाठी तुम्हाला काही पैसे भरायला सांगते
- लॉटरी/बक्षीसाच्या किंमतीच्या तुलनेत किंवा सुरक्षित नोकरी मिळण्याच्या तुलनेत मागीतलेली रक्कम कमी असल्यामुळे तुम्ही ते पैसे भरता

सुरक्षिततेच्या सूचना

- पैसे देऊ नका किंवा लॉटरी कॉल्स/ई-मेल्ससाठी तुमची गोपनीय माहिती देऊ नका
- अविश्वसनीय लॉटरी किंवा ऑफर्सच्या अधिकृततेची नेहमी चौकशी करा
- लक्षात ठेवा, कोणतीही खरी कंपनी नोकरी देताना पैशांची मागणी करत नाही

एटीएम कार्ड स्किम करणे

कसे केले जाते

- भ्रष्ट व्यक्ती एटीएम मशिन्सवर स्किमिंग डिवाइस लावते आणि माहिती चोरते, ड्युप्लिकेट कार्ड तयार करते आणि तुमच्या खात्यातून पैसे काढून घेते
- तुम्ही एंटर केलेली माहिती चोरण्यासाठी डमी कीपॅड्स लावले जातात किंवा छोट्या कॅमेरातून माहिती मिळवली जाते
- तुम्ही एटीएममध्ये प्रवेश केल्यावर भ्रष्ट व्यक्ती तुमचा पिन पाहण्यासाठी ग्राहक असल्याचा बनाव रचते किंवा तुम्ही रोख पैसे काढू शकला नाहीत तर तुमचा व्यवहार पूर्ण करून देण्यासाठी मदत देते

सुरक्षिततेच्या सूचना

- सतर्क रहा आणि कार्ड इंसर्शन स्लॉट किंवा एटीएम मशिनच्या कीपॅडजवळ कोणतही अतिरिक्त डिवाइस जोडलं नसल्याची खात्री करा
- तुमच्या जवळ कोणी उभं असेल तर त्याच्या उपस्थितीत कार्डाचा तपशील एंटर करू नका
- पिन एंटर करताना कीपॅड झाकून घ्या आणि तुमचं कार्ड किंवा पिन कोणालाही देऊ नका
- तुम्हाला काहीही संशयास्पद वाटलं तर एटीएममधून लगेच बाहेर पडा

#BankingDhyaanSe

कोणताही संशयास्पद किंवा भ्रष्ट व्यवहार दिसून आला तर ॲक्सिस बँकेला कळवा

जर तुम्हाला संशयास्पद किंवा भ्रष्ट व्यवहार दिसून आला तर खाली दिलेल्या चॅनल्सवर तुम्ही संपर्क करू शकता:

- आमच्या फोन बँकिंग नंबर्सवर कॉल करा: 1860 419 5555/1860 500 5555
- आम्हाला इथे लिहा: https://www.axisbank.com/support/
- ॲक्सिस बँकेच्या कोणत्याही शाखेत भेट द्या

तुम्ही वेळ आणि लक्ष दिल्याबद्दल धन्यवाद.

#BankingDhyaanSe