सतर्क रहिए और सुरक्षित बैंकिंग का पालन कीजिए

बैंकिंग ध्यान से

के साथ

AXIS BANK

ऐक्सिस बैंक द्वारा ग्राहक सेवा उपक्रम

आभार

यह दस्तावेज आरबीआई ऑम्बड्समैन (मुंबई–2) महाराष्ट्र, गोवा के कार्यालय द्वारा जारी एक बुकलेट 'ऑन मोडस ऑपरांडी ऑफ फायनांशियल फ्रॉडस्टर्स' तथा इस विषय पर किए गए हमारे कुछ इन–हाउस रिसर्च के आधार पर निर्मित किया गया है.

प्रस्तावना

बैंकिंग सिस्टम के डिजिटाइजेशन ने ग्राहकों की आर्थिक जरूरतों को आसानी से और तेज रफ्तार के साथ पूरा करने के लिए नए आयामों का निर्माण किया है. वर्तमान स्थिति ने हमें जहां तक संभव हो डिजिटल तरीकों को अपनाने के लिए प्रेरित भी किया है ताकि शारीरिक और सामाजिक संपर्क को न्यूनतम किया जा सके.

हम डिजिटल बैंकिंग की बढ़ी हुई सुविधाओं का आनंद ले रहे हैं तो वहीं हमारे साथ सायबर क्राइम और बैंकिंग संबंधी धोखाधडी होने की संभावनाएँ भी बढ़ गई हैं. अधिकतर, ग्राहक अनजाने में ही शिकार हो जाते हैं और यदि वे सतर्क नहीं रहे तो उन्हें आर्थिक नुकसान भी झेलना पड़ सकता है.

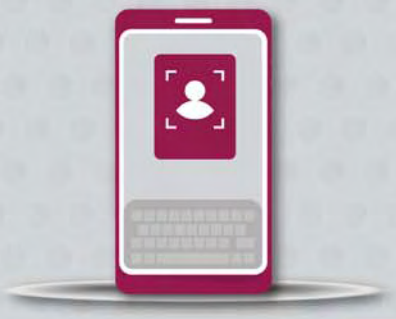
ऐक्सिस बैंक में, हमें आपका ख्याल रहता है और हम लगातार ऐसे उपायों की तलाश में रहते हैं ताकि समय समय पर आपको उपयोगी जानकारी देते हुए हम आपके हितों की रक्षा कर सकें.

यह दस्तावेज जागरूकता फैलाने और आपको आज–कल होने वाली संदिग्ध तथा धोखाधड़ी भरी गतिविधियों से परिचित कराने के लिए हमारी पहल है. हमने कुछ महत्वपूर्ण धोखाधडी के प्रसंगों का संकलन किया है ताकि आपको यह समझने में मदद मिले कि ऐसी गतिविधि को कैसे पहचाना जा सकता है, आपको कौन सी सावधानियाँ बरतनी चाहिए और उनकी रिपोर्ट कैसे करनी चाहिए. सावधान रहने से आप शिकार बनने और आर्थिक हानि झेलने की संभावनाओं को न्यूनतम करने में सक्षम हो सकेंगे.

हमें विश्वास है कि आपको यह जानकारी उपयोगी लगेगी और यह कि जब आप बैंकिंग ध्यान से करेंगे तक आप एक सुरक्षित और निर्दोष बैंकिंग का अनुभव ले सकेंगे.

सुरक्षित रहें!

यहाँ पर कुछ सामान्य सावधानी के उपाय और अच्छी पद्धतियाँ दी गई हैं:



टालें

- अनसिक्योर्ड वेबसाइट्स पर विजिट करना या अनजाने ब्राउजर्स का उपयोग करना
- पब्लिक डिवाइसेस पर पासवर्ड्स को सेव करना
- पब्लिक या फ्री नेटवर्क्स पर फायनांशियल/गोपनीय ई-मेल ऐक्सेस करना
- अनजाने स्रोतों से संदिग्ध लगनेवाले पॉप अप्स, लिंक्स और ई-मेल पर क्लिक करना
- ई-मेल में या अनजानी वेबसाइटों पर सूरक्षित विश्वसनीय जानकारियां या पासवर्ड स्टोर करना
- सोशल मीडिया पर अनजाने व्यक्तियों के साथ निजी जानकारी साझा करना
- बैंकिंग और अन्य ट्रांजैक्शन्स के लिए एक ही पासवर्ड्स का उपयोग करना
- अनजाने एप्लिकेशन्स या सॉफ्टवेयर इंस्टॉल करना
- अपने मोबाइल या अन्य इलेक्ट्रॉनिक डिवाइसेस या ऐप्स को अनलॉक रखना

कभी न करें

- अपना पिन (पर्सनल आयडेंटिफिकेशन नंबर), पासवर्ड, क्रेडिट या डेबिट कार्ड नंबर्स, सीवीवी, चेक बुक की प्रतियाँ, केवाईसी विवरण किसी के भी साथ साझा न करें
- अनजाने डिवाइसेस पर संवेदनशील या गोपनीय जानकारी संग्रहित करना

हमेशा करें

- अपने फोन को सशक्त स्क्रीन पासवर्ड से सुरक्षित रखें
- जहाँ भी लागू/उपलब्ध हो, टू-फैक्टर ऑथेंटिफिकेशन का उपयोग करें
- उपयोग करने के बाद तुरंत इंटरनेट बैंकिंग सेशन से लॉग आउट करें
- अपने उपयोग के आधार पर अपने कार्ड या अकाउंट पर एनेबल या डिसेबल फीचर का उपयोग करें और ट्रांजैक्शन की सीमाएँ सेट करें.
- पैडलॉक या https जैसे सुरक्षित संकेतों को देखकर वेबसाइट की सुरक्षा सत्यापन करें
- ऑनलाइन भुगतानों के लिए सुरक्षित पेमेंट गेटवे का उपयोग करें
- सशक्त पासवर्ड रखें जो खासकर अल्फान्यूमरिक और खास कैरेक्टर्स का मेल हो और उन्हें नियमित रूप से बदलते रहें
- पब्लिक डिवाइसेस पर वर्चुअल कीबोर्ड का उपयोग करें क्योंकि कीस्ट्रोक्स की जानकारी कॉम्प्रोमाइज्ड डिवाइसेस, कीबोर्ड इत्यादि के माध्यम से हासिल की जा सकती है
- अपने डिवाइसेस पर एंटीवायरस और एंटी-स्पायवेयर इंस्टॉल करें, उन्हें अप टू डेट रखें और जब भी उपलब्ध हों अपडेट्स इंस्टॉल करें
- किसी भी यूएसबी ड्राइव/स्टोरेज डिवाइसेस को उपयोग से पहले स्कैन करें
- अपने मोबाइल ऐप्स को पासवर्ड से सुरक्षित करें या मोबाइल फोन्स में निहित हिडेन स्पेस फीचर का उपयोग करके उन्हें नॉर्मल व्यू से छिपा दें

#BankingDhyaanSe

ऑनलाइन/वेबसाइट फ्रॉड्स के बारे में (1)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

ऑनलाइन फिशिंग

ये कैसे किया जाता है

- जालसाज ऐसी वेबसाइट बनाते हैं जो बैंक की जेनुइन वेबसाइट जैसी ही दिखती है
- इन वेबसाइट लिंक्स को एसएमएस, सोशल मीडिया, ई-मेल इत्यादि के माध्यम से फैलाया जाता है
- इन लिंक्स को इस तरह से बनाया जाता है कि वे असली वेबसाइट जैसी दिखती हैं और उन्हें इस तरह से डिजाइन किया जाता है ताकि आप विस्तृत यूआरएल को जाँचे बिना ही अपने क्रेडेंशियल्स या संवेदनशील और गोपनीय जानकारी सिर्फ लिंक को देखते ही एंटर कर दें.
- जब आप इन वेबसाइट्स पर अपने क्रेडेंशियल्स एंटर करते हैं तब वह कैप्चर कर लिया जाता है और जालसाजों द्वारा उनका दुरूपयोग किया जाता है.

सुरक्षा संबंधी सुझाव

- अनजानी लिंक्स यदि असली जैसी लगती हैं तो भी उन्हें टालें
- फायनांशियल क्रेडेंशियल्स एंटर करने से पहले वेबसाइट के विवरणों का सत्यापन करें

ऑनलाइन फ्रॉड्स

इसे कैसे किया जाता है

- जालसाज ऑनलाइन, ईकॉमर्स प्लेटफॉर्म पर असली खरीदार/विक्रेता होने का दिखावा करते हैं
- वे आपके उत्पाद में रुचि प्रदर्शित करते हैं या फिर बडे डिस्काउंट्स या इंसेंटिव्स देते हुए उनसे खरीदने के लिए आपको झांसा देते हैं
- भुगतान करने के बजाय वे आपको यूपीआई 'रिक्वेस्ट मनी' विकल्प को पूरा करने के लिए लालच देते हैं ताकि आपके बैंक खाते से पैसे निकाल सकें

सुरक्षा संबंधी सुझाव

- ऑनलाइन प्रोडक्ट्स के लिए फायनांशियल ट्रांजैक्शन्स करते समय सतर्क रहें
- धन प्राप्त करने के लिए आपसे अपना पिन या पासवर्ड एंटर करने के लिए कभी नहीं कहा जाएगा

ऑनलाइन/वेबसाइट फ्रॉड्स के बारे में (2)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

नकली सर्च इंजिन के परिणाम

ये कैसे किया जाता है

- जालसाज कंपनियों के कस्टमर केयर कोऑर्डिनेट्स को बदलते हैं और सर्च इंजिन ऑप्टिमाइजेशन (एसईओ) का उपयोग करके अपने नकली नंबर को सोशल मीडिया प्लेटफॉर्म्स पर सर्च रिजल्ट्स में सबसे ऊपर ले आते हैं
- अपने बैंक या अन्य फायनांशियल जानकारी/निकायों के कस्टमर केयर संपर्क विवरणों को ऑनलाइन सर्च करते समय आप संयोगवश ऐसे असत्यापित/गलत नंबरों के संपर्क में आ सकते हैं, और उन्हें असली समझ सकते हैं
- आप अपने निजी या गोपनीय और फायनांशियल क्रेडेंशियल्स को साझा कर सकते हैं और आप धोखाधड़ी का शिकार हो सकते हैं

सुरक्षा संबंधी सुझाव

- सर्च इंजिन पर कस्टमर केयर संपर्क विवरणों का सर्च करना टालें क्योंकि शिकारों को ललचाने के लिए जालसाजों द्वारा उसकी आड में छिपकर धोखाधडी की जा सकती है
- हमेशा असली विवरणों के लिए बैंकों/कंपनियों की आधिकारिक वेबसाइट्स देखें

स्क्रीन शेयरिंग/रिमोट ऐक्सेस

ये कैसे किया जाता है

- आपको स्क्रीन शेयरिंग ऐप्स डाउनलोड करने का झांसा देते हुए, जालसाज आपका निजी डाटा और फायनांशियल क्रेडेंशियल्स अपने लैपटॉप/मोबाइल डिवाइसेस पर ऐक्सेस कर लेते हैं और बाद में आपके बैंकिंग और पेमेंट ऐप्स का उपयोग करके भुगतान करते हैं

सुरक्षा संबंधी सुझाव

- किसी भी अपरिचित व्यक्ति की सिफारिश पर स्क्रीन शेयरिंग ऐप्स डाउनलोड नहीं करें
- सुनिश्चित करें कि आप किसी भी बैंकिंग या फायनांशियल ऐप या वेबसाइट में लॉगिंग करने से पहले किसी भी स्क्रीन शेयरिंग ऐप्लिकेशन को डिऐक्टिवेट करें

ऑन कॉल/मोबाइल फ्रॉड्स के बारे में (1)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

जालसाजी भरे कॉल्स

ये कैसे किया जाता है

- जालसाज व्यक्ति टेलीफोन कॉल/सोशल मीडिया जरिए बैंकिंग एक्जिक्यूटिव्स का छद्म नाम लेकर ग्राहकों से संपर्क करता है, कभी कभी आपके बैंक के टोल फ्री या कस्टमर केयर नंबर की नकल करते हैं
- कॉलर ग्राहक पर दबाव डालता है और उसे अपनी गोपनीय जानकारियाँ या तरह तरह के आपात्कालीन कारण बताते हुए ओटीपी साझा करने के लिए ग्राहक को मनाता है जैसे कि सेवाएँ तुरंत खंडित हो जाएंगी, केवाईसी नॉन-कंप्लायंस, खाता/कार्ड बंद होना इत्यादि
- वे आपके खाते में धोखाधडी भरी गतिविधियाँ करने के लिए इन जानकारियों का दुरूपयोग करते हैं

सुरक्षा संबंधी सुझाव

- बैंक/कोई भी प्रामाणिक निकाय कभी भी गोपनीय जानकारी साझा करने के लिए आपसे नहीं कहेगा जैसे कि यूज़रनेम, पासवर्ड, कार्ड के विवरण, पिन, सीवीवी, ओटीपी इत्यादि

मोबाइल ऐप धोखाधड़ी

यह कैसे की जाती है

- आपको अपने मोबाइल, लैपटॉप या डेस्कटॉप पर अप्रमाणित ऐप डाउनलोड करने के लिए ललचाया जाता है
- इन ऐप्स के लिंक्स को एसएमएस, सोशल मीडिया प्लेटफॉर्म्स इत्यादि के जरिए साझा और प्रमोट किया जाता है
- ये दुर्भावनापूर्ण एप्लिकेशन्स होते हैं जिनकी बदौलत जालसाजों को आपके डिवाइस का संपूर्ण ऐक्सेस मिल जाता है

सुरक्षा संबंधी सुझाव

- अप्रमाणित/अज्ञात स्रोतों से एप्लिकेशन कभी डाउनलोड न करें
- अनजाने स्रोतों से प्राप्त एसएमएस/ईमेल को डिलीट कर दें ताकि डाउनलोड लिंक पर अनजाने में क्लिक न हो

ऑन कॉल/मोबाइल फ्रॉड्स के बारे में (2)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

ओटीपी आधारित धोखाधड़ी

ये कैसे की जाती है

- आपको जालसाजों से लोन्स देने या क्रेडिट लिमिट बढ़ाने का प्रस्ताव देने के लिए मानो बैंक की ओर से एसएमएस मिल सकता है और इसमें आपसे मैसेज में वर्णित नंबर पर संपर्क करने के लिए कहा जाता है
- जब आप उस नंबर पर कॉल करते हैं तो आपसे कुछ फॉर्म (ऑनलाइन भी) भरने के लिए कहा जाता है जिसमें आपकी वित्तीय जानकारियाँ मौजूद होती हैं जिससे उनके लिए आपको ओटीपी या पिन के विवरण साझा करने हेतु तैयार करना आसान हो जाता है, जिसके परिणामस्वरूप आर्थिक नुकसान हो सकता है

सुरक्षा संबंधी सुझाव

- किसी के भी साथ अपना ओटीपी, पिन या निजी विवरण कभी साझा न करें
- अपना एसएमएस/ई-मेल नियमित रूप से देखें ताकि सुनिश्चित हो कि आपकी जानकारी के बिना भी ओटीपी निर्मित न हो

जूस जैकिंग

ये कैसे किया जाता है

- जूस जैकिंग एक प्रकार की सायबर चोरी है जहां एक बार आपका मोबाइल किसी अज्ञात/अप्रमाणित चार्जिंग पोर्ट्स से जुडता है तो कुछ अज्ञात ऐप्स/मालवेयर आपके डिवाइस में इस्टॉल कर दिए जाते हैं जिसके सहारे जालसाज संवेदनशील डाटा, ई-मे, एसएमएस या सेव किए गए पासवर्ड्स चुरा सकते हैं, नियंत्रित कर सकते हैं और उन तक ऐक्सेस प्राप्त कर सकते हैं

सुरक्षा संबंधी सुझाव

- सार्वजनिक/अज्ञत चार्जिंग पोर्ट्स/केबल्स का उपयोग हमेशा टालें

ऑन कॉल/मोबाइल फ्रॉड्स के बारे में (3)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

सिम स्वैप धोखाधड़ी

ये कैसे की जाती है

- आपके अकाउंट विवरण और ऑथेंटिकेशन को आपके पंजीकृत मोबाइल नंबर से जोडा जाता है. जालसाज लोग ओटीपी और एलर्ट्स तक ऐक्सेस प्राप्त करने की कोशिश करते हैं ताकि वे आपके नंबर का नया बदली सिम कार्ड लेकर फायनांशियल ट्रांजैक्शन्स कर सकें
- जालसाज आपका नकली पहचान पत्र बनाकर खुद को आप बताकर आपके मोबाइल ऑपरेटर के रिटेल आउटलेट पर जा सकते हैं और आपके असली सिम को ब्लॉक करवा सकते हैं और आपके मोबाइल नंबर वाला नया सिम ले सकते हैं
- या फिर, वे अपने द्वारा शेयर किया गया एसएमएस आपके ऑपरेटर को भेजते हुए सिम कार्ड को अपग्रेड करने के लिए डरा सकते हैं जो आपके सिम को डिऐक्टिवेट कर देता है और उनके कब्जे में रहे आपके मोबाइल नंबर वाले सिम कार्ड को ऐक्टिव कर देता है

सुरक्षा संबंधी सुझाव

- सोशल इंजीनियरिंग स्कैम्स से सावधान रहें जिनका लक्ष्य होता है आपका गोपनीय और निजी डाटा चुराना
- यदि आपका मोबाइल फोन अचानक कोई नेटवर्क कनेक्टिविटी नहीं दिखाता है तो तुरंत अपने मोबाइल सर्विस प्रोवाइडर से अपनी सेवा के बारे में पूछताछ करें ताकि सुनिश्चित हो कि आपके सिम के लिए कोई डुप्लिकेट सिम तो जारी नहीं किया गया है

अन्य प्रकार की फ्रॉड्स के बारे में (1)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

सोशल मीडिया के जरिए धोखाधड़ी

ये कैसे की जाती है

- जालसाज आप बनकर पॉपुलर सोशल मीडिया प्लेटफॉर्म पर नकली अकाउंट बनाता है
- जब आपका अनलॉक्ड फोन अनजाने में (इमरजेंसी कॉल करने के लिए या रिपेयर के लिए) सौंपा जाता है या अकेले में पड़ा रहता है तब जालसाज आपके मोबाइल पर भेजा गया ओटीपी प्राप्त कर लेता है और आपके प्रोफाइल तक ऐक्सेस प्राप्त करता है और कुछ एप्लिकेशन्स के डेस्कटॉप वर्जन निर्मित करते उन्हें आपके कॉन्टैक्ट्स, ऑनलाइन प्रोफाइल और चैट मैसेजेस तक ऐक्सेस देता है
- वे आपके दोस्तों को रिक्वेस्ट भेजकर तत्काल मेडिकल इलाज के लिए धन मांग सकते हैं

सुरक्षा संबंदी सुझाव

- फोन द्वारा या व्यक्तिगत रूप से कोई भी भुगतान करने से पहले अपने संपर्कितों से संपर्क करके निवेदन की प्रामाणिकता की पुष्टि कर लें
- अपना फोन लॉक किए बिना कभी अकेले न छोडें

क्यूआर स्कैन आधारित धोखाधड़ियाँ

ये कैसे की जाती हैं

- जालसाज कई बहाने बनाकर आपसे संपर्क कर सकते हैं और पेमेंट ऐप्स का उपयोग करके क्यूआर कोड्स स्कैन करने के लिए आपको ललचा सकते हैं और भुगतान की प्रक्रिया पूर्ण करवा सकते हैं.
- इन क्यूआर कोड्स में प्रीडिफाइंड (पूर्वनिर्धारित) अकाउंट विवरण होते हैं जिससे आप किसी विशिष्ट खाते में धन ट्रांसफर कर सकते हैं जहाँ जालसाज आपको झांसा देकर आपके खाते से धन ट्रांसफर पूर्ण करवा सकते हैं.

सुरक्षा संबंधी सुझाव

- पेमेंट ऐप्स का उपयोग करके कोई भी क्यूआर कोड स्कैन करते समय सावधानी बरतें

अन्य प्रकार की फ्रॉड्स के बारे में (2)

मोडस ऑपरांडी
आप कैसे सतर्क और सुरक्षित रह सकते हैं?

लॉटरी या नौकरी दिलाने की धोखाधडी भरे कांड

ये कैसे किया जाता है

- जालसाज आपको बडी लॉटरी/इनाम जीतने की जानकारी देनेवाले ई-मेल या फोन कॉल्स करते हैं या वे अपने आपको किसी प्रतिष्ठित कंपनी का अधिकारी बताते हैं जो नौकरी दे रही है
- लेकिन, धन/उपहार प्राप्त करने या चयन प्रक्रिया पूर्ण करने की दृष्टि से आपसे कुछ धन प्रत्यक्ष रूप से देने के लिए कह सकता है
- मांगी गई राशि लॉटरी/इनाम का एक बहुत ही छोटा सा प्रतिशत होती है या नौकरी पाने के लिए महत्वपूर्ण लगती है, इसीलिए आप वह भुगतान कर सकते हैं

सुरक्षा संबंधी सुझाव

- किसी भी लॉटरी कॉल्स/ईमेल्स के लिए भुगतान या अपने सुरक्षित विश्वसनीय डेटा साझा न करें
- किसी भी अविश्वसनीय लॉटरी या ऑफर्स की प्रमाणिकता पर हमेशा सवाल करें
- याद रहे, नौकरी देनेवाली कोई भी प्रामाणिक कंपनी पैसे कभी नहीं मांगेगी

एटीएम कार्ड स्किमिंग

ये कैसे किया जाता है

- डाटा चुराने, डुप्लिकेट कार्ड बनाने और आपके खाते से धन निकालने के लिए जालसाज एटीएम मशीनों में स्किमिंग डिवाइसेस लगा देते हैं
- वे आप द्वारा एंटर की गई जानकारी हासिल करने के लिए डमी कीपैड्स या छोटे कैमरे भी इंस्टॉल कर सकते हैं
- आपके प्रवेश करने पर वे एटीएम सेवाओं का उपयोग करते हुए वे ग्राहक का रूप भी बना सकते हैं ताकि वे आपके पिन को देख सकें या यदि आप धन निकालने में अक्षम रहते हैं तो वे आपका ट्रांजैक्शन पूर्ण करने के लिए मदद देने का दिखावा कर सकते हैं

सुरक्षा संबंधी सुझाव

- सतर्क रहें और सुनिश्चित करें कि कार्ड इनसर्शन स्लॉट या एटीएम मशीन के कीपैड के पास कोई अतिरिक्त डिवाइस न जुडा हो
- अपने पास किसी व्यक्ति की मौजूदगी में कार्ड के विवरण एंटर नहीं करें
- पिन एंटर करते समय कीपैड को ढंकें और अपना कार्ड या पिन किसी को न दें
- यदि आपको कुछ भी संदिग्ध लगता है तो तुरंत एटीएम परिसर से बाहर निकल जाएँ

#BankingDhyaanSe

किसी संदिग्ध या धोखाधडी भरे ट्रांजैक्शन की सूचना ऐक्सिस बैंक को दें

यदि आप कोई संदिग्ध ट्रांजैक्शन करते हैं या धोखाधडी में पडकर करते हैं तो आप नीचे वर्णित चैनल्स से संपर्क कर सकते हैं:

- हमारे फोन बैंकिंग नंबर्स पर कॉल करें: 1860 419 5555 / 1860 500 5555
- हमें यहाँ लिखें https://www.axisbank.com/support/
- किसी भी ऐक्सिस बैंक शाखा में जाएँ

अपना समय और ध्यान देने के लिए धन्यवाद.

#BankingDhyaanSe