शरद सहकारी बँक लि.,मंचर

यांच्या डिजीटल बँकींग सुरक्षा ह्या उपक्रमातून

“सावध रहा आणि बँकेचे सुरक्षित व्यवहार करा.”

शरद सहकारी बँक लि.,मंचर

बँकिंगपेक्षाही खूप काही!

परिचय

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

प्रस्तावना

बँकिंग यंत्रणांचे डिजिटलायजेशन झाल्यामुळे ग्राहकांना आपल्या आर्थिक आवश्यकता सहजपणे आणि जलदपणे पूर्ण करण्यासाठी नवीन माध्यमं तयार झाली आहेत.

डिजीटल 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.

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

ह्या पुस्तिकेतून आम्ही जागरूकता निर्माण करत आहोत. सध्या चालू असलेल्या संशयास्पद आणि फसवणुवकीच्या प्रकारांचा तुम्हाला परिचय करून देत आहोत. त्यासाठी आम्ही काही फसवणुकीचे उदाहरण दिले आहे आणि त्या कशा ओळखायच्या ते सांगितले आहे. अशा कृती रोखण्यासाठी कोणती काळजी घ्यावी, त्यांची सुचना कशी द्यावी हे सुद्धा सूचवले आहे. तुम्ही सावध राहिलात तर तुम्ही बळी पड्ण्याची शक्यता कमी होईल आणि तुमचं आर्थिक नुकसान होणार नाही.

आम्हाला विश्वास आहे की ही माहिती तुम्हाला खूप उपयोगी पडेल.

सुरक्षित रहा!

सुरक्षित रहा!

आम्ही इथे काही सामान्य सावधगिरीच्या सूचना आणि चांगल्या कार्यपद्धतींची माहिती देत आहोत.

हे टाळा

- असुरक्षित वेबसाईट्सवर भेट देऊ नका किंवा अनोळखी ब्राऊजर्स वापरू नका.
- सार्वजनिक डिवाइसवर पासवर्ड सेव्ह करू नका.
- सार्वजनिक किंवा मोफत नेटवर्क्सवर आर्थिक / गोपनीय ई–मेल्सचा वापर करून नका.
- संशयास्पद वाटणाऱ्या पॉप अप्स, लिंक्स आणि अनोळखी स्त्रोतांकडून आलेल्या इ–मेल्सवर क्लिक करू नका.
- ई–मेल्स किंवा अनोळखी वेबसाईटस्वर सुरक्षित माहिती किंवा पासवर्डस् स्टोअर करू नका.
- समाज माध्यमांवरील अनोळखी व्यक्तींकडे खासगी माहिती देऊ नका.
- बँकिंग आणि इतर व्यवहारांसाठी समान / कॉमन पासवर्ड वापरू नका.
- अनोळखी ॲप्लिकेशन किंवा सॉफ्टवेअर इंस्टॉल करू नका.
- तुमचा मोबाईल किंवा इतर इलेक्ट्रॉनिक डिवाइसेस अथवा ॲप्स अनलॉक अवस्थेत ठेवू नका.

हे कधीही करू नका

- आपला पिन (वैयक्तिक ओळख क्रमांक), पासवर्ड किंवा डेबिट कार्डचे नंबर्स सीव्हीव्ही, चेक बुकची प्रत, के.वाय.सी. तपशील कोणालाही देऊ नका.
- अनोळखी डिव्हाईसेसवर संवेदनशील किंवा गोपनीय माहिती साठवू नका.

हे नेहमी करा

- (स्ट्राँग) स्क्रीन पासवर्ड वापरून तुमचा फोन सुरक्षित करा.
- जिथे शक्य असेल / उपलब्ध असेल तिथे टू–फॅक्टर अँथेटिकेशनचा वापर करा.
- वापर केल्यानंतर तात्काळ इंटरनेट बँकिंग सेशनमधून लॉग आऊट करा.
- एनॅबल किंवा डिसॅबल फिचर वापरा आणि तुमच्या वापरानुसार तुमच्या ए.टी.एम. कार्डावर किंवा खात्यावर व्यवहाराची मर्यादा सेट करा.
- पॅडलॉक्स किंवा https अशी सुरक्षित चिन्हे पाूसन वेबसाईटच्या सुरक्षितेची पडताळणी करा.
- ऑनलाईन पेमेंटस् करताना सुरक्षित पेमेंट गेटवेजचा वापर करा.
- आकडे शब्द आणि स्पेशल कॅरेक्टर्सच्या मिश्रणातून तयार झालेला सशक्त (स्ट्राँग) पासवर्ड वापरा आणि तो नियमित बदला.
- डिवाइसेसवर अँटीव्हायरस आणि अँटी स्पायवेअर इंस्टॉल करा, ते अद्यावत ठेवा आणि उपलब्ध असतील तेव्हा अपडेटस् इंस्टॉल करा.
- वापर करण्याआधी कोणताही यू.एसबी डिवाइस/स्टोरेज डिवाइस स्कॅन करा.
- तुमचे मोबाइल ॲप्स पासवर्डने सुरक्षित करा.

ऑनलाईन/वेबसाइटवरील फसवणुकीबाबत (१)

गुन्ह्याची पद्धत

तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

ऑनलाईन लूट करण्याची पद्धती

कसं लुटतात

- भ्रष्ट व्यक्ती एक वेबसाइट तयार करते, जी बँकेच्या खऱ्या वेबसाइटसारखी दिसते.
- ह्या वेबसाइट्सच्या लिंक एस.एम.एस., समाज माध्यमे (सोशल साईट), इ-मेल्स इत्यादीद्वारे पसरवल्या जातात.
- ह्या वेबसाइट अधिकृत वेबसाईट असल्याचे दाखवले जाते आणि अशी युक्ती केली जाते की लिंक पहाताच तुम्ही तपशीलावर युआरएल न पहाता तुमचा तपशील किंवा संवेदनशील आणि गोपनिय माहिती देता.
- तुम्ही ह्या वेबसाइटवर तपशील एंटर केल्यानंतर, भ्रष्ट व्यक्ती , त्या माहितीचा वापर करून त्याचा गैरवापर करतो.

सुरक्षिततेच्या सूचना

- अनोळखी लिंक्स अधिकृत वाटत असल्या तरी त्याचा वापर टाळा.
- आर्थिक तपशील देण्याआधी वेबसाइटची माहिती तपासून घ्या.

ऑनलाइन फसवूणक

कशी करतात

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

सुरक्षिततेच्या सूचना

- ऑनलाईन प्रॉडक्टस्चा आर्थिक व्यवहार करताना सावध रहा.
- पैसे प्राप्त करताना कधीही पिन किंवा पासवर्ड एंटर करायला सांगितले जात नाही./त्याची आवश्यकता नसते.

ऑनलाईन/वेबसाइटवरील फसवणुकीबाबत (२)

गुन्ह्याची पद्धत
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 (सोशल साईट) प्लॅटफॉर्म्सवर सर्च रिझल्टस्मध्ये ते वरच्या भागात आपला बनावट नंबर टाकतात.
- तुमच्या बँकेच्या कस्टमर केअरच्या संपर्काचा तपशील किंवा इतर आर्थिक माहिती/संस्था ऑनलाईन 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 / बदल केलेली असू शकते.
- बँका/कंपन्यांच्या संपर्काच्या खऱ्या तपशीलासाठी नेहमी अधिकृत वेबसाइटस् पहा.

स्क्रीन शेअरिंग/रिमोट ॲक्सेस

हे कसे केले जाते

? तुम्हाला स्क्रीन शेअरिंग ॲप्स डाऊनलोड करायला लावून फसवणुक करणारी 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 डाऊनलोड करायला सांगितलं तर तसं करू नका.
- बँकिंग किंवा आर्थिक ॲपवर अथवा वेबसाइटवर लॉगिन करण्याआधी तुम्ही सर्व स्क्रीन शेअरिंग ॲप्लिकेशन बंद केल्याची खात्री करा.

कॉल/मोबाइल फसवणुकी बाबत (१)

गुन्ह्याची पद्धत

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 तत्काळ खंडित होईल, केव्हायसी पूर्तता झाली नाही, खाते/कार्ड इत्यादी बंद होईल अशी आणीबाणीची किंवा अत्यंत तातडीने कर्यवाही करावी अशी विविध कारणे सांगते.
- ? ग्राहकाने दिलेल्या तपशीलाचा गैरवापर करून ग्राहकाच्या खात्यात अनधिकृत व्यवहार केला जातो.

सुरक्षिततेच्या सूचना

- ✓ **बँक तुम्हाला यूझरनेम, पासवर्ड, कार्डचा तपशील, पिन, सीव्हीव्ही, ओटीपी इत्यादी गोपनीय माहिती कधीही विचारत नाही.**

मोबाइल ॲपचा भ्रष्टाचार

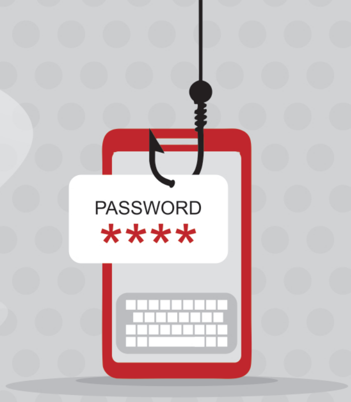
कसा केला जातो

- ? तुमच्या मोबाइल, लॅपटॉप किंवा डेस्कटॉपवर ॲप डाऊनलोड कराण्याचं अमिष दाखवलं जातं.
- ? ह्या ॲप्सच्या लिंक दिल्या जातात किंवा एसएमएस, सामाजिक माध्यमे इत्यादीद्वारे पुरवल्या जातात.
- ? हे फसवणूक करणारी ॲप्लिकेशन असतात, ज्यामुळे भ्ष्ट्र व्यक्तीला तुमच्या डिवाइसवर संपूर्ण नियंत्रण मिळतं.

सुरक्षिततेच्या सूचना

- ✓ खात्री न केलेल्या / अनोळखी स्त्रोतांकडून कधीही ॲप्लिकेशन डाऊनलोड करू नका.
- ✓ डाऊनलोड केलेल्या लिंकवर नकळत क्लिक होऊ नये ह्यासाठी अनोळखी स्त्रोतांकडून आलेले एसएमएस/इ-मेल डिलिट करा.

कॉल/मोबाइल फसवणुकी बाबत (२)



गुन्ह्याची पद्धत
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 डेबीट मर्यादा वाढवली जात असल्याचं सांगितलं जातं आणि मेसेजमध्ये दिलेल्या क्रमांकावर तुम्हाला संपर्क करायला सांगितलं जातं.
- ? तुम्ही त्या क्रमांकावर कॉल केल्यावर तुम्हाला काही फॉर्म्स (ऑनलाईनसुद्धा) भरायला सांगितलं जातं. ज्यामुळे तुमचा आर्थिक 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 पोर्टस्ला जोडला जातो तुमच्या डिवाइसवर विशिष्ट अनोळखी ॲप्स/मालवेअर इंस्टॉल केलेले असतील तर भ्रष्ट व्यक्ती संवेदनशील माहिती, इ-मेल एस.एम.एस. आणि सेव केलेला पासवर्ड चोरू शकते किंवा त्यावर नियंत्रण मिळवू शकते.

सुरक्षिततेच्या सूचना

- सार्वजनिक/अनोळखी चार्जिंग पोर्ट्स/केबल्स वापरू नका.

कॉल/मोबाइल फसवणुकी बाबत (३)

गुन्ह्याची पद्धत

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 रिप्लेसमेंट सिमकार्ड मिळवून ओटीपी आणि ॲलर्ट्स मिळवते व अर्थिक व्यवहार करते.
- भ्रष्ट व्यक्ती तुमच्या मोबाइल ऑपरेटरच्या रिटेल आउटलेला 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 सिमकार्ड अपडेट होत असल्याचं सांगते ज्यामुळे तुमचं सिम डिॲक्टिवेट होतं आणि तुमच्या मोबाइल नंबरसह सिमकार्ड चा ताबा मिळवतात.

सुरक्षिततेच्या सूचना

- तुमच्या 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 नसल्याचं खात्री करा.

इतर प्रकारच्या फसवणुकी बाबत (१)

गुन्ह्याची पद्धत

तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

समाज माध्यमांद्वारे भ्रष्टाचार

कसा केला जातो

- भ्रष्ट व्यक्ती तुम्ही स्वत: असल्याचं भासवून प्रसिद्ध समाज माध्यमांवर नकली खातं तयार करते.
- तुम्ही अनलॉक्ड फोन दिल्यावर (इमर्जन्सी कॉल करण्यासाठी किंवा दुरूस्तीसाठी) किंवा तो बेवारस अवस्थेत ठेवल्यावर तुमच्या मोबाईलवर आलेला ओटीपी भ्रष्ट व्यक्तीला मिळतो. त्यामुळे ती तुमचा प्रोफाइल ॲक्सेस करते आणि काही ॲप्लिकेशनचं डेस्कटॉप वर्जन तयार करते व तुमचे संपर्क क्रमांक, ऑनलाईन प्रोफाइल व चॅट मॅसेज 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 फसवणुकी बाबत (२)

गुन्ह्याची पद्धत

तुम्ही सतर्क आणि सुरक्षित कसे राहू शकता?

लॉटरी किंवा नोकरीसंबंधी भ्रष्ट घोटाळे

कसे केले जातात

- ? तुम्ही खूप मोठी लॉटरी/बक्षीस जिंकल्याचे किंवा प्रसिद्ध कंपनीचे पद तुम्हाला दिले जात असल्याचे भासवून भष्ट्र व्यक्ती तुम्हाला ई-मेल पाठवते किंवा फोन कॉल करते.
- ? पैसे/बक्षीस प्रप्त करण्यासाठी 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.
- अविश्वासनीय 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 कोणतेही अतिरिक्त डिवाइस जोडलं नसल्याची खात्री करा.
- तुमच्या जवळ कोणी उभं असेल तर त्याच्या उपस्थितीत कार्डचा तपशील एंटर करू नका.
- पिन एंटर करताना कीपॅड झाकून घ्या आणि तुमचं कार्ड किंवा पिन कोणालाही देऊ नका.
- तुम्हाला संशयास्पद वाटलं तर एटीएममधून लगेच बाहेर पडा.

कोणताही संशयास्पद किंवा भ्रष्ट व्यवहार दिसून आला तर शरद सहकारी बँकेला कळवा

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

फोन : ०२१३३-२२३१०३,२२५४५० टोल फ्री नं.: १८००२३३२१२४

आम्हाला इथे लिहा : https://sharadbank.com/contactus

शरद बँकेच्या कोणत्याही नजीकच्या शाखेत भेट द्या.

तुम्ही वेळ आणि लक्ष दिल्याबद्दल धन्यवाद.