ऑनलाइन सुरक्षा

जग अधिक डिजिटल सॅवी बनत असताना, आपल्या बँकिंगच्या पद्धती सुद्धा बदलत आहेत. जरी हे बदल सोयिस्कर आहेत, मात्र असे गुन्हेगार सुद्धा आहेत जे आपल्या ऑनलाइन जीवनाचा गैरफायदा घेण्यासाठी उत्सुक आहेत आणि आपल्या पैशांच्या बाबतीत आपली फसवणूक करण्यासाठी तयार आहेत.

आरबीएल बँकेमध्ये, आम्ही खात्री करतो की आमच्या ग्राहकांना प्रत्येक वेळी एक सुरक्षित बँकिंग अनुभव मिळेल. तुमच्या बँकेने अनेक मार्गदर्शक तत्वे आणि साधनं एकत्र ठेवलेली आहेत जी फसवणूक रोखण्यात मदत करतील.

मोबाइल बँकिंग

- **तुमचा फोन लॉक ठेवा:** तुमच्या हँडसेटसाठी पासवर्ड/पिन सेट करून ठेवा जेणेकरून तो कुणीही सहजपणे ॲक्सेस करु शकणार नाही.
- **महत्त्वाची माहिती तुमच्या फोनमध्ये ठेवू नका.** बँकिंगची माहिती मिळवण्यासाठी मोबाइल फोन वापरला जाण्याची शक्यता असते. जर तुम्ही ही फोनमध्ये सेव करून ठेवता तर मॅलवेयर किंवा छुपे स्पायवेअर असलेले ईमेल्स किंवा ॲप्स वापरुन, गुन्हेगार ही माहिती ॲक्सेस करु शकतात.
- **ऑटो-फिल सुरु करू नका:** फॉर्ममध्ये कंटाळवाणे तपशील पटकन भरण्याची ही एक सोयिस्कर पद्धत असू शकते परंतु ऑटो-फिल फीचर बंद ठेवणे चांगले जर तुम्हाला मोबाइल बँकिंग वापरताना सुरक्षित आणि बिनधोक बँकिंग अनुभव घ्यायचा असेल.
- **असुरक्षित वाय-फाय नेटवर्क्स टाळा:** सार्वजनिक वाय-फाय किंवा शेयर्ड इंटरनेट नेटवर्क्स वापरताना तुमचे बँक खाते वापरू नका.
- **लॉग आउट करा:** तुमचा व्यवहार झाल्यानंतर, तुमच्या स्मार्टफोनद्वारे ॲक्सेस केलेल्या ॲप किंवा वेबसाइटवरून तुम्ही लॉग आउट केल्याची खात्री करा.

इंटरनेट बँकिंग

- **क्लिक करण्याआधी विचार करा:** बँका आपल्या ऑनलाइन बँकिंग पेजेसच्या लिंक्सचा समावेश असलेले ईमेल्स किंवा टेक्स्ट मेसेजेस कधीच पाठवणार नाही. जर तुम्हाला तुमच्या तपशीलांची विचारणा करणारा असा ईमेल मिळाला आहे, तर त्यातील लिंक्सवर क्लिक करू नका कारण हा फिशिंगचा प्रयत्न असू शकतो. जगभरातील बँकांना ही समस्या भेडसावत आहे आणि त्यांच्या ग्राहकांना संशयास्पद वाटणाऱ्या ईमेल/एसएमएसवर पाठवलेल्या कोणत्याही लिंकवर क्लिक करण्याबाबत अत्यंत सावधगिरी बाळगण्याचा सल्ला देतात.
- **मॅलवेयरकडे लक्ष ठेवा:** अनेकदा संशयास्पद दिसणाऱ्या ईमेलमध्ये कंप्युटर व्हायरस किंवा ट्रोजन व्हायरस असतात जे तुमची संवेदनशील माहिती चोरण्यासाठी गुन्हेगारांकडून ठेवले जातात. अशा ईमेल्सवर क्लिक करण्याविषयी किंवा त्यातील अटॅचमेंट्स डाउनलोड

करण्याविषयी सावधगिरी बाळगा. फक्त विश्वसनीय स्रोतांकडूनच ॲप्स आणि अटॅचमेंट्स डाउनलोड करा.

- **इंटरनेट बँकिंगसोबत जोखीम कमी करा:** पेपरलेस पर्यायांचा वापर करा. चेक वापरण्याऐवजी ऑनलाइन पैसे ट्रांसफर करा. ऑनलाइन बिल मिळवा आणि भरा. फोन बँकिंगसाठी नोंदणी करुन सूचना आणि अपडेट्स वेळेवर प्राप्त करा.
- **तुमचा पासवर्ड नियमितपणे अपडेट करा:** गुन्हेगार तुमची बँकिंगची माहिती मिळवण्यासाठी फिशिंग, विशिंग, स्किमिंग, स्पूफिंग, सायबर स्टॉकिंग इत्यादी सारख्या विभिन्न मार्गांचा उपयोग करतात. म्हणून, फसवणूकीपासून स्वत:ला सुरक्षित ठेवण्यासाठी तुम्ही तुमचे तपशील नियमितपणे अपडेट करणे अत्यावश्यक आहे.
- **युआरएल ब्राउजरमध्ये टाईप करा:** इंटरनेट बँकिंग द्वारे लॉग-इन करण्यासाठी ईमेल्समध्ये मिळालेल्या लिंक्सवर कधीच क्लिक करू नका. ऑनलाइन सुरक्षा आणि सुरक्षिततेची खात्री करण्याचा सर्वोत्तम मार्ग आहे ब्राउजर विंडोमध्ये युआरएल टाईप करणे.
- **अवघड पासवर्ड तयार करा.** आपली जन्मतारीख किंवा सर्वसामान्य पासवर्ड्स वापरू नका जे हॅक करण्यासाठी सोपे असतात. तुमचा पासवर्ड शक्य तितका किचकट बनवण्यासाठी तुम्ही अक्षरं, संख्या आणि विशेष वर्ण वापरत असल्याची खात्री करा.
- **फसवणूकीची त्वरित तक्रार करा:** तुमच्या खात्यात लॉग-इन किंवा पैसे ट्रांसफर करण्यासारख्या काही संशयास्पद हालचाली तुम्हाला दिसल्यास, त्याची त्वरित बँकेला तक्रार करा.
- **ओळख चोरण्याकडे लक्ष द्या:** कागदाचा असा कोणताही तुकडा लगेचच नष्ट करा ज्यावर तुमचे लॉगइन तपशील आहेत. अनोळखी व्यक्ती किंवा तिसऱ्या पक्षासोबत तुमची वैयक्तिक माहिती कधीच शेयर करू नका आणि तुमचे तपशील बँकेकडे नियमितपणे अपडेट करा.

फोन बँकिंगची सुरक्षा

- **तुमचे तपशील सुरक्षित करा:** पहिली आणि सर्वात महत्त्वाची गोष्ट जी तुम्हाला माहित असायला हवी ती म्हणजे कुणीही बँक अधिकारी तुम्हाला तुमचा पासवर्ड, पिन, ओटीपी, सीव्हीव्ही किंवा कार्ड नंबर कधीच विचारणार नाही. हे अपराधी असतील जे तुमच्या खात्याचा ॲक्सेस मिळवण्यासाठी संवेदनशील तपशील उघड करण्यास तुम्हाला प्रवृत्त करतील. तुमचे तपशील नेहमी गोपनीय ठेवा.
- **तुमचा पिन लपवा:** जेव्हा तुम्हाला तुमचा पिन (वैयक्तिक ओळख क्रमांक) टाईप करण्यासाठी सांगितले जाते, तेव्हा डिव्हाइसमध्ये एंटर करताना तुमचा पिन कुणीही पाहत नसल्याची खात्री करा.
- **सार्वजनिक ठिकाणं टाळा:** तुम्ही फोन बँकिंग वापरताना, तुम्ही सार्वजनिक ठिकाणाी नसल्याची खात्री करा कारण तुम्हाला पडताळणीचे तपशील विचारले जाऊ शकतात. संवेदनशील माहिती कुणीही ऐकत नसल्याची खात्री करण्यासाठी अशा गोष्टी सार्वजनिक ठिकाणी करणे टाळणे सर्वात योग्य आहे.
- **थर्ड पार्टी कॉलर नाही:** फोन बँकिंग सुविधेचा लाभ फक्त खातेधारकांनाच मिळेल.

क्रेडिट आणि डेबिट कार्डच्या सुरक्षेसाठी टिप्स

- **हे सुरक्षित ठेवा:** तुम्ही तुमचे क्रेडिट आणि डेबिट कार्ड्स सुरक्षित ठिकाणी ठेवता याची नेहमी खात्री करा.
- **कार्डवर सही करा:** तुम्हाला तुमचे कार्ड मिळाल्यावर, तुम्ही त्यावर सही केल्याची खात्री करा.
- **पिन लक्षात ठेवा:** पिन नंबर कुठेही लिहू नका. पिन पाठ करणे आणि तो नेहमी स्वतःकडे ठेवणे सर्वात चांगले आहे.
- **पिन लेटर नष्ट करा:** तुम्हाला तुमच्या कार्ड पिनचे तपशील मिळाल्यावर, पत्र नष्ट करा ज्यात पिनचा उल्लेख आहे.

एटीएम सुरक्षा

- **तपशील शेयर करण्यास नाही म्हणा:** तुमच्या एटीएम कार्डचे तपशील आणि पिन कुणासोबतही शेयर करू नका.
- **तुमच्याकडे तुमचे कार्ड आहे का?** तुम्ही तुमचा व्यवहार पूर्ण केल्यावर तुमचे कार्ड घेण्यास कधीही विसरू नका.
- **संशयास्पद वस्तूंवर लक्ष ठेवा:** तुम्ही व्यवहार करत असताना एटीएमला कोणताही कॅमेरा किंवा इतर संशयास्पद उपकरण जोडलेले नाहीत याची खात्री करा. एक हाताने कीबोर्ड झाकून दुसऱ्या हाताने पिन एंटर करणे नेहमीच योग्य आहे, जेणेकरून तुमचा पिन दिसण्यापासून सुरक्षित राहतो.
- **अनोळखी धोका:** तुम्ही एटीएम वापरत असताना अनोळखी व्यक्तींना तुमची मदत करू देऊ नका किंवा तुम्हाला पाहू देऊ नका.
- **तुमचे पैसे मोजा:** मशिनमधून निघालेल्या नोटा आठवणीने मोजा आणि तपासा.
- **व्यवहाराची पावती मागे सोडू नका:** तुम्ही तुमचा व्यवहार पूर्ण केल्यावर, व्यवहाराची पावती तुम्ही मागे सोडत नसल्याची खात्री करा (जर तुम्ही पावतीची निवड केली आहे).
- **तुमचा पिन नियमितपणे बदला:** तुमचा एटीएम पिन नियमितपणे बदलणे योग्य आहे.

रोख आणि चेक व्यवहाराची सुरक्षा

- **नोटांची कधीच घडी घालू नका किंवा दुमडू नका:** त्या नेहमीच शक्य तितके सरळ आणि व्यवस्थित ठेवण्याचा प्रयत्न करा.
- **नोटांना स्टॅपल करू नका:** किंवा त्यांच्यावर लिहू किंवा खरडू नका. कोणत्याही प्रकारे नोटा खराब करण्यास मनाई आहे.
- **काळजीपूर्वकपणे हाताळा:** नोटा नेहमी स्वच्छ आणि कोरड्या हातांनी हाताळा.
- **चेकचे तपशीलांची नोंद करा:** प्रत्येक वेळी जेव्हा तुम्ही चेक जारी करता, तेव्हा तुम्ही ज्या व्यक्तीला तो देत आहात त्याचे तपशील, तारीख, रक्कम इत्यादीची नोंद केल्याची खात्री करा.
- **चेकबूक सुरक्षित ठेवा:** तुमचे चेकबूक नेहमी तुमच्या जवळ ठेवा. ते कधीही दुर्लक्षितपणे सोडू नका किंवा अशा ठिकाणी ठेवू नका जिथे इतर लोकं ते घेऊ शकतात.
- **चेकची संख्या मोजा:** तुम्हाला नवीन चेकबूक मिळाल्यावर लगेचच, त्यातील चेक्सची संख्या तुम्हाला खात्री देण्यात आलेल्या संख्येच्या इतकीच आहेच आहे हे तपासणे सर्वात

योग्य आहे. चेक्सच्या संख्येमध्ये तुम्हाला तफावत आढळल्यास, त्याची त्वरित बँकेकडे तक्रार करा.

- **कोऱ्या चेकवर कधीच सही करू नका:** जेव्हा कधीही तुम्ही चेक जारी करता, तेव्हा तुम्ही त्यावर व्यक्तीचे नाव आणि व्यवहाराची अचूक रक्कम टाकल्याची खात्री करा.
- **गरज असल्यास चेक क्रॉस करा:** जर तुम्ही दुसऱ्या खात्यात पैसे ट्रांसफर करत आहात, तर तुम्ही चेक क्रॉस केल्याची खात्री करणे आवश्यक आहे. अशा प्रकारे, चेकवर नमूद केलेली रक्कम केवळ प्राप्तकर्त्याच्या बँक खात्यात ट्रांसफर केली जाते, ज्याचे नाव चेकवर नमूद केले आहे. त्यामुळे, गैरवापर होण्याची शक्यता कमी होते.

तुम्हाला प्रत्येक वेळेस एक सुरक्षित आणि बिनधोक बँकिंगचा अनुभव मिळण्याची खात्री करण्यासाठी आम्ही काय करतो?

आरबीएल बँकेमध्ये, आम्ही ऑनलाइन सुरक्षा गांभीर्याने घेतो. म्हणूनच आम्ही तुमचे ऑनलाइन बँकिंग व्यवहार शक्य तितके सुरक्षित आणि बिनधोक करण्यासाठी वेगवेगळ्या पद्धती लागू केलेल्या आहेत. हे साध्य करण्यासाठी आम्ही वापरत असलेल्या काही पद्धती खाली नमूद केलेल्या आहेत.

- **ओटीपी (वन-टाईम पासवर्ड):** तुमच्या खात्यात होत असलेला व्यवहार तुमच्या द्वारे केला जात आहे याची खात्री करण्यासाठी, आम्ही तुमच्या नोंदणीकृत मोबाइल क्रमांकवर ओटीपी किंवा वन-टाईम पासवर्ड पाठवतो. व्यवहार सुरु ठेवण्यासाठी, तुम्हाला हा ओटीपी क्रमांक प्रविष्ट करण्यास सांगितला जाईल. जर तुम्हाला एखादा वन-टाईम पासवर्ड प्राप्त होतो ज्याची तुम्हाला अपेक्षा नाही, तर त्याविषयी त्वरित बँकेला कळवा.
- **नोटिफिकेशन्स आणि अलर्ट्स:** आम्हाला तुमच्या खात्यात संशयास्पद हालचाल होत असल्याचे दिसून आल्यास, आम्ही ताबडतोब कॉल द्वारे तुम्हाला कळवू. हा मेसेज कदाचित एक सूचना असू शकते, परंतु तो तुम्हाला कधीही लिंकवर क्लिक करण्यास किंवा अटॅचमेंट्स डाउनलोड करण्यास सांगणार किंवा पुढे जाण्यासाठी तुमच्या सुरक्षा प्रश्नांची उत्तरे विचारणार नाही.
- **सिस्टमची सुरक्षा:** अत्याधुनिक तंत्रज्ञानाचा वापर करून, आम्ही प्रत्येक ऑनलाइन बँकिंग व्यवहार शक्य तितका सुरक्षित आणि बिनधोक करण्याचा प्रयत्न करतो. आम्ही फायरवॉल्स, इंट्रुजन डिटेक्शन कॅपेबिलिटी (घुसखोरी शोधण्याची क्षमता) आणि अँटी-मॅलवेयर प्रोग्राम युक्त आधुनिक संगणक प्रणाली वापरतो.
- **शेवटचे लॉगइन तपशील:** प्रत्येक वेळी जेव्हा तुम्ही लॉगइन करता, तुम्हाला तुमच्या खात्यात दिसणारे शेवटच्या लॉगइनचे तपशील तपासा. जर ते तुमच्या शेवटच्या लॉगइन हालचालीशी जुळतात, तर याचा अर्थ होतो कि तुमचे खाते शक्य तितके सुरक्षित आणि बिनधोक आहे. मात्र, शेवटचे लॉगइन तपशील तुमच्या हालचालीशी जुळत नसेल आणि संशयास्पद हालचालींची चिन्ह दाखवते, तर याची त्वरित बँकेला तक्रार करा.

ऑनलाइन आणि ऑफलाइन फसवणूकीपासून तुम्ही स्वतःचे संरक्षण कसे कराल?

- **घोटाळ्यांकडे लक्ष द्या:** फिशिंग, विशिंग, सायबर स्टॉकिंग, स्किमिंग इत्यादी अशा अनेक घोटाळ्यांपैकी काही आहेत, ज्यांचा वापर गुन्हेगार तुमचे वैयक्तिक तपशील शेयर

करण्यासाठी तुम्हाला फसवण्यासाठी करतात. या घोटाळ्यांकडे लक्ष द्या आणि संशयास्पद दिसणाऱ्या लिंक्स, ईमेल्स आणि अटॅचमेंट्सवर क्लिक करू नका.

- **पासवर्ड्स नियमितपणे अपडेट करा:** तुमचे युजरनेस आणि पासवर्ड हे एकमेव घटक आहेत जे गुन्हेगारांना तुमचा डेटा ॲक्सेस करण्यापासून रोखतात. तुम्ही ते नियमितपणे, कमीत कमी दोन महिन्यातून एकदा अपडेट करत असल्याची खात्री करा. अक्षरं, आकडे आणि विशेष वर्णांचा समावेश असलेले रँडम पासवर्ड्स वापरा. अगदी सर्वसामान्य किंवा सहजसोपे पासवर्ड्स वापरू नका जे क्रॅक करण्यासाठी अगदी सोपे असतात.
- **सुरक्षित वेबसाइट्स वापरा:** ईमेलमध्ये एम्बेड केलेल्या कोणत्याही लिंकवर कधीच क्लिक करू नका; तुमच्या ब्राउजरमध्ये लिंक टाईप करणे अधिक सुरक्षित असते. युआरएल काळजीपूर्वकपणे वाचा कारण बहुतेक फिशर्स फसवणूकीच्या क्रियाकलापांसाठी एकसारख्याच वेबसाइट्स सेट अप करतात. जर तुम्हाला युआरएल मध्ये स्पेलिंगची चूक आढळते किंवा वेबसाइट असुरक्षित वाटत असते, तर जोखीम घेऊ नका. सर्व कृती तिथेच थांबवा.
- **वैयक्तिक माहिती सुरक्षित ठेवा:** जर तुम्ही तुमच्या माहितीची प्रत तुमच्या फोनमध्ये ठेवता, तर तुमचा फोन लॉक ठेवण्यासाठी नेहमी पिन/पासवर्ड सेट करा. जर तुम्ही तुमच्या खात्याची माहिती असलेले बँक मेलर्स/पत्र साठवून ठेवता, तर ते लॉकरमध्ये किंवा अशा ठिकाणी सुरक्षित ठेवा जे सहजपणे ॲक्सेस केले जाऊ शकत नाही.
- **सोशल इंजिनीयरिंग टाळा:** सोशल मीडियावर मौल्यवान माहिती शेयर करू नका कारण बहुतेक हल्लेखोर माहिती मिळवण्यासाठी मानवी संपर्काचा वापर करतात. तुमचे तपशील खाजगी ठेवा आणि तुम्हाला माहित नसलेल्या लोकांच्या कोणत्याही संपर्क/ फ्रेंड रिक्वेस्ट्स पासून सावध रहा. वैयक्तिक/कौटुंबिक माहिती विचारणाऱ्या व्यक्तींकडून आलेले अनपेक्षित फोन कॉल्स, एसएमएस किंवा ईमेल यांच्यावरील संशयामुळे तुम्ही सोशल इंजीनियरिंग हल्ल्याचा बळी होण्याचे टाळू शकता. वेबसाइटची सुरक्षा तपासण्याआधी इंटरनेटवर संवेदनशील माहिती पाठवणे टाळा. तुम्हाला अँटी-व्हायरस सॉफ्टवेयर इंस्टॉल करण्याचा सुद्धा सल्ला दिला जातो जे तुमच्या सिस्टमला फसव्या हालचालींपासून सुरक्षित ठेवू शकतात.
- **तुमचे इंटरनेट कनेक्शन सुरक्षित करा:** बँकिंग आणि आर्थिक व्यवहार करण्यासाठी सार्वजनिक नेटवर्क्स कधीही न वापरणे योग्य आहे. मात्र, तुम्ही याची सुद्धा खात्री करायला हवी की तुमचे वैयक्तिक किंवा घरगुती कनेक्शन पूर्णपणे सुरक्षित आहे. पासवर्ड सेटअप करता जेणेकरून अनोळखी व्यक्तींना तुमच्या इंटरनेट कनेक्शनचे ॲक्सेस मिळणार नाही.
- **कागदपत्रे टाकून देण्याआधी त्यांचे तुकडे करा:** जर तुम्ही अशी कोणतीही कागदपत्रे फेकून देत आहात ज्यामध्ये वैयक्तिक माहिती आहे, तर ते कागदपत्र फेकण्याआधी तुम्ही त्याचे तुकडे करत असल्याची खात्री करा. लोकांची ओळख चोरण्यासाठी गुन्हेगार लोकं पत्रांची चोरी करतात.
- **संशयास्पद ईमेल्स डीलीट करा:** लोकांची खाजगी माहिती ॲक्सेस करण्यासाठी ईमेल्स हे सर्वात जास्त वापरल्या जाणाऱ्या पद्धतींपैकी एक आहे. जर तुमच्या इनबॉक्समध्ये

तुम्हाला असे कोणतेही ईमेल्स आढळतात जे संशयास्पद वाटतात किंवा तुमच्या कॉन्टॅक्ट लिस्टमध्ये नसलेल्या व्यक्ती द्वारे पाठवलेले आहेत, तर ते ईमेल्स न उघडताच डीलीट करा. जर तुम्ही ते उघडता, तर त्यातील कोणत्याही लिंक्स किंवा अटॅचमेंट्सवर क्लिक करण्यापासून सावध रहा कारण अशा फाईल्समध्ये तुमच्या सिस्टममध्ये प्रवेश करून संवेदनशील माहिती स्कॅन करण्यासाठी तयार केलेले मॅलवेयर आणि व्हायरसेस असतात.

तुमच्या दैनंदिन जीवनात या टीप आणि युक्त्यांची अंमलबजावणी करून तुम्ही प्रत्येक वेळी एक सुरक्षित अनुभवाची खात्री करू शकाल. आजच्या डिजिटल युगात ऑनलाइन सुरक्षा राखणे सुद्धा महत्त्वाचे आहे कारण आपल्या जीवनाचा बराचसा भाग प्रत्येकाने पाहण्यासाठी आधीच जगात उपलब्ध आहे. ऑनलाइन सुरक्षा आणि सुरक्षिततेची खात्री करण्यासाठी या सुरक्षित बँकिंग टीपांचा सराव करा. कोणत्याही अतिरिक्त मदतीसाठी किंवा फसवणूकीची तक्रार करणअयासाठी, खाली दिलेल्या मार्गांनी ताबडतोब बँकेला संपर्क करा, आणि आम्हाला तुमची मदत करण्यात खुपच आनंद होईल!

बँकिंग आणि क्रेडिट काड्र्स : +91 22 6232 7777;

किंवा

संपूर्ण तपशीलांसोबत reportfraud@rbl.bank.in वर ईमेल करा.

सायबर फसवणूक झाल्यास तात्काळ तक्रार करा:

सायबर फसवणुकीचा बळी पडल्यास त्वरित कारवाई करा. राष्ट्रीय सायबर गुन्हे हेल्पलाइन 1930 वर संपर्कसाधा आणि https://cybercrime.gov.in/ या संकेतस्थळावर तक्रार नोंदवा. तसेच, तुम्ही Sancharsaathi Portal वरूनही तक्रार दाखल करू शकता. वेळेवर तक्रार केल्यास पुढील फसवणूक टाळता येते आणि इतरांनाही सतर्ककरता येते.