ऑनलाइन सुरक्षा

दुनिया अधिक डिजिटल प्रेमी होती जा रही है जिससे बैंकिंग के हमारे तरीके भी बदल रहे हैं। हालांकि बदलाव सुविधा के लिए किए जाते हैं, लेकिन ऐसे भी अपराधी प्रवृत्ति के लोग हैं जो हमारी ऑनलाइन सुविधाओं का गलत तरीके से फायदा उठाना चाहते हैं और धोखा देकर हमारे पैसे निकालने के लिए तैयार हैं।

आरबीएल बैंक में, हम यह सुनिश्चित करते हैं कि अपने ग्राहकों को हर बार सुरक्षित बैंकिंग अनुभव मिले। आपके बैंक ने कई दिशानिर्देश और टूल साथ में दिए हैं जिनसे धोखाधड़ी को रोकने में मदद मिलेगी।

मोबाइल बैंकिंग

- **अपने फोन को लॉक रखें:** अपने हैंडसेट के लिए पासवर्ड/पिन सेट करें, ताकि कोई भी व्यक्ति आसानी से इसे एक्सेस न कर सके।
- **अपने फोन में महत्वपूर्ण जानकारी न रखें:** मोबाइल फोन का उपयोग बैंकिंग जानकारी प्राप्त करने के लिए किया जा सकता है। छिपे हुए स्पाइवेयर के साथ मैलवेयर या ईमेल या ऐप्स का उपयोग करके, अपराधी प्रवृत्ति वाले लोग इस जानकारी का एक्सेस तब कर सकते हैं जब आप इसे फोन में सहेजते हैं।
- **अपने-आप भरने की सुविधा चालू न करें:** यह फॉर्म में उबाऊ विवरण को जल्दी से भरने का सुविधाजनक तरीका हो सकता है, लेकिन अगर आप मोबाइल बैंकिंग का उपयोग करते समय सुरक्षित बैंकिंग अनुभव चाहते हैं, तो अपने-आप भरने की सुविधा को बंद रखना सबसे अच्छा होता है।
- **असुरक्षित वाई-फाई नेटवर्क से बचें:** सार्वजनिक वाई-फाई या साझा इंटरनेट नेटवर्क का उपयोग करते समय अपने बैंकिंग खाते का एक्सेस न करें।
- **लॉगआउट करें:** आपका लेनदेन पूरा होने के बाद, सुनिश्चित करें कि आप उस ऐप या वेबसाइट से लॉग आउट करें जिसे आप अपने स्मार्टफोन द्वारा एक्सेस करते हैं।

इंटरनेट बैंकिंग

- **क्लिक करने से पहले सोचें:** बैंक कभी भी ऐसे ईमेल या टेक्स्ट मैसेज नहीं भेजेंगे जिसमें हमारे ऑनलाइन बैंकिंग पेजों के लिंक शामिल हों। अगर आपको विवरण मांगने वाला इस तरह का ईमेल मिला है, तो लिंक पर क्लिक न करें क्योंकि यह फिशिंग का प्रयास हो सकता है। दुनिया भर के बैंक इस समस्या का सामना कर रहे हैं और अपने ग्राहकों को सलाह दे रहे हैं कि वे ईमेल/एसएमएस पर भेजे गए ऐसे किसी भी लिंक पर क्लिक करने के बारे में बेहद सावधान रहें जो संदिग्ध दिखते हैं।
- **मैलवेयर पर नजर रखें:** संदिग्ध दिखने वाले ईमेल में अक्सर कंप्यूटर वायरस या ट्रोजन वायरस होते हैं जो अपराधियों द्वारा आपकी संवेदनशील जानकारी चोरी करने के लिए

काम में लाए जाते हैं। ऐसे ईमेल पर क्लिक करने या उनमें शामिल अटैचमेंट डाउनलोड करने के बारे में सावधान रहें। केवल विश्वसनीय स्रोतों से ऐप्स और अटैचमेंट डाउनलोड करें.

- **इंटरनेट बैंकिंग के साथ जोखिम कम करें:** कागज रहित विकल्पों का उपयोग करें। चेक का उपयोग करने के बजाय ऑनलाइन पैसे ट्रांसफर करें। ऑनलाइन बिल प्राप्त करें और भुगतान करें। फोन बैंकिंग के लिए पंजीकरण करें और समय पर अलर्ट और अपडेट प्राप्त करें।
- **अपना पासवर्ड नियमित रूप से अपडेट करें:** अपराधी आपकी बैंकिंग जानकारी हासिल करने के लिए फिशिंग, विशिंग, स्किमिंग, स्पूफिंग, साइबर स्टॉकिंग इत्यादि जैसे विभिन्न तरीकों का उपयोग करते हैं। इसलिए, यह जरूरी है कि आप खुद को धोखाधड़ी से सुरक्षित रखने के लिए नियमित रूप से अपने विवरण अपडेट करें।
- **ब्राउजर में यूआरएल टाइप करें:** इंटरनेट बैंकिंग द्वारा लॉगिन करने के लिए ईमेल में प्राप्त लिंक पर कभी भी क्लिक न करें। ऑनलाइन सुरक्षा सुनिश्चित करने का सबसे अच्छा तरीका ब्राउजर विंडो में यूआरएल टाइप करना है।
- **मुश्किल पासवर्ड बनाएं:** अपनी जन्मतिथि या ऐसे सामान्य पासवर्ड का उपयोग न करें जिन्हें हैक करना आसान है। सुनिश्चित करें कि आप अपने पासवर्ड को अधिक से अधिक मुश्किल बनाने के लिए अक्षरों, संख्याओं और विशेष वर्णों का उपयोग करते हैं।
- **धोखाधड़ी की रिपोर्ट तुरंत करें:** अगर आपको अपने खाते से लॉगिन या पैसे का ट्रांसफर जैसी कुछ संदिग्ध गतिविधि दिखाई देती है, तो तुरंत बैंक को इसकी सूचना दें।
- **पहचान की चोरी पर नजर रखें:** हमेशा कागज के ऐसे किसी भी टुकड़े को नष्ट करें जिसमें आपका लॉगिन विवरण हो। कभी भी अजनबी या तीसरे पक्ष को अपनी व्यक्तिगत जानकारी न दें और नियमित रूप से बैंक के साथ अपना विवरण अपडेट करें।

फोन बैंकिंग सुरक्षा

- **अपने विवरण सुरक्षित रखें:** पहली और सबसे महत्वपूर्ण बात जो आपको पता होनी चाहिए वह यह है कि कोई भी बैंक अधिकारी आपसे कभी भी आपका पासवर्ड, पिन, ओटीपी, सीवीवी या कार्ड नंबर नहीं मांगेगा। वे अपराधी ही होंगे जो आपके खाते का एक्सेस पाने के लिए आपसे संवेदनशील विवरण मांगेंगे। अपने विवरण को हमेशा गोपनीय रखें।
- **अपना पिन छुपाएं:** जब आपको अपना पिन (व्यक्तिगत पहचान संख्या) टाइप करने के लिए कहा जाता है, तो सुनिश्चित करें कि डिवाइस में पिन डालते समय कोई भी व्यक्ति उसे नहीं देखता है।
- **सार्वजनिक स्थानों से बचें:** जब आप फोन बैंकिंग का उपयोग करते हैं, तो सुनिश्चित करें कि आप सार्वजनिक स्थान पर नहीं हैं क्योंकि आपसे सत्यापन विवरण मांगा जा सकता है। ऐसी चीजों के लिए सार्वजनिक स्थानों से बचना सबसे अच्छा है, ताकि यह सुनिश्चित हो सके कि कोई भी व्यक्ति संवेदनशील जानकारी न सुन सके।

- **कोई तृतीय पक्ष कॉलर नहीं:** फोन बैंकिंग सुविधा का लाभ केवल खाताधारकों को ही मिलता है।

क्रेडिट और डेबिट कार्ड सुरक्षा से जड़ी सलाह

- **इसे सुरक्षित रखें:** हमेशा सुनिश्चित करें कि आप अपने क्रेडिट और डेबिट कार्ड को सुरक्षित स्थान पर रखते हैं।
- **कार्ड पर हस्ताक्षर करें:** जैसे ही आप अपना कार्ड प्राप्त करते हैं, सुनिश्चित करें कि आप उस पर हस्ताक्षर करते हैं।
- **पिन याद रखें:** पिन नंबर कहीं भी न लिखें। इसे याद रखना और पिन को हमेशा अपने पास रखना सबसे अच्छा होता है।
- **पिन वाले लेटर को नष्ट करें:** जब आपको अपने कार्ड के पिन का विवरण प्राप्त होता है, तो उस मेलर को नष्ट कर दें जिसमें पिन का उल्लेख किया गया है।

एटीएम सुरक्षा

- **विवरण साझा करने के लिए "ना" कहें:** अपने एटीएम कार्ड का विवरण और पिन किसी भी व्यक्ति को न दें।
- **क्या आपके पास अपना कार्ड है?** अपना लेन-देन पूरा करने के बाद अपना कार्ड लेना कभी न भूलें।
- **संदिग्ध वस्तुओं पर नजर रखें:** सुनिश्चित करें कि जब आप लेनदेन कर रहे हों, तो एटीएम से कोई कैमरा या अन्य संदिग्ध डिवाइस जुड़ा हुआ न हो। कीबोर्ड को हमेशा एक हाथ से ढकने और किसी अन्य व्यक्ति के समक्ष अपना पिन दर्ज न करने की सलाह दी जाती है, ताकि आपका पिन दिखाई देने से सुरक्षित हो।
- **अजनबी का खतरा:** एटीएम का उपयोग करते समय अजनबियों को आपकी सहायता करने या की जाने वाले गतिविधियों को देखने की अनुमति न दें।
- **अपने पैसे की गिनती करें:** निकले हुए नोटों को गिनना और जांचना याद रखें।
- **लेनदेन की रसीद न छोड़ें:** आपका लेन-देन पूरा होने के बाद सुनिश्चित करें कि आप लेनदेन रसीद को न छोड़ें (अगर आपने इसका विकल्प चुना है)।
- **अपने पिन को नियमित रूप से बदलें:** नियमित रूप से अपना एटीएम पिन बदलने की सलाह दी जाती है।

नकद और चेक लेनदेन सुरक्षा

- **बैंक नोट को कभी न मोड़ें:** हमेशा उन्हें जितना संभव हो उतना सीधा और साफ रखने की कोशिश करें।
- **बैंक के नोट पर स्टैपल किया हुआ नहीं है:** या उन पर कुछ लिखा हुआ नहीं है। बैंक के नोटों को किसी भी तरीके से नुकसान पहुंचाने की सख्त मनाही है।
- **सावधानी से रखें:** बैंक के नोटों को हमेशा साफ और सूखे हाथों से हैंडल करें।
- **चेक का विवरण रिकॉर्ड करें:** चेक जारी करने पर हर बार यह सुनिश्चित करें कि आप उस व्यक्ति का विवरण रिकॉर्ड करते हैं जिसे आप इसे दे रहे हैं और तारीख, राशि इत्यादि को भी रिकॉर्ड करते हैं।

- **चेक बुक को सुरक्षित रखें:** अपनी चेक बुक को हमेशा अपने पास रखें। इसे कभी भी लावारिस या उन जगहों पर न छोड़ें जहां अन्य लोग इसे एक्सेस कर सकें।
- **चेक के नंबर की गणना करें:** जैसे ही आपको नई चेक बुक मिलती है, वैसे ही यह जांचना सबसे अच्छा होता है कि नंबर उस नंबर से मेल खाता है या नहीं जो आपके लिए बताया गया है। अगर आपको चेक के नंबर में फर्क मिलता है, तो तुरंत बैंक को इसकी सूचना दें।
- **कभी भी खाली चेक पर हस्ताक्षर न करें:** जब भी आप चेक जारी कर रहे हों, तो सुनिश्चित करें कि आप लेनदेन के लिए व्यक्ति का नाम और सटीक राशि डालते हैं।
- **आवश्यक होने पर चेक को क्रॉस करें:** अगर आप किसी अन्य खाते में पैसे ट्रांसफर कर रहे हैं, तो आपको चेक को क्रॉस करना सुनिश्चित करना होगा। इससे, केवल चेक पर लिखी राशि ही उस भुगतान वाले व्यक्ति के बैंक खाते में ट्रांसफर की जाती है जिसका नाम चेक पर लिखा है। इस प्रकार, इसके दुरुपयोग की संभावना कम हो जाती है।

हम यह सुनिश्चित करने के लिए क्या करते हैं कि आपको हर बार सुरक्षित बैंकिंग अनुभव मिले?

आरबीएल बैंक में, हम ऑनलाइन सुरक्षा को गंभीरता से लेते हैं। यही कारण है कि हमने अलग-अलग तरीकों को लागू किया है जिसमें हम आपके ऑनलाइन बैंकिंग लेनदेन को यथासंभव सुरक्षित बनाते हैं। नीचे सूचीबद्ध कुछ तरीके हैं जिनका उपयोग हम इसे प्राप्त करने के लिए करते हैं।

- **ओटीपी (वन-टाइम पासवर्ड):** यह सुनिश्चित करने के लिए कि आपके खाते में होने वाले लेनदेन आपके द्वारा किए गए हैं, हम आपके पंजीकृत मोबाइल नंबर पर ओटीपी या वन-टाइम पासवर्ड भेजते हैं। लेनदेन जारी रखने के लिए, आपको यह ओटीपी नंबर डालने के लिए कहा जाएगा। अगर आपको वन-टाइम पासवर्ड प्राप्त होता है जिसकी आप उम्मीद नहीं कर रहे थे, तो तुरंत बैंक को इसकी सूचना दें।
- **सूचनाएं और चेतावनी:** अगर हम आपके खाते में संदिग्ध गतिविधि देखते हैं, तो हम आपको कॉल करके तुरंत सूचित करेंगे। संदेश कोई सूचना हो सकती है, लेकिन इसमें आपको लिंक पर क्लिक करने या अटैचमेंट डाउनलोड करने या आगे बढ़ने के लिए अपने सुरक्षा प्रश्नों के उत्तर मांगने के लिए कभी नहीं कहा जाएगा।
- **सिस्टम सुरक्षा:** अत्याधुनिक तकनीक का उपयोग करके, हम हर ऑनलाइन बैंकिंग लेनदेन को यथासंभव सुरक्षित बनाने का प्रयास करते हैं। हम फायरवॉल, घुसपैठ का पता लगाने की क्षमताओं और एंटी-मैलवेयर प्रोग्राम के साथ उन्नत कंप्यूटर सिस्टम का उपयोग करते हैं।
- **अंतिम लॉगिन विवरण:** हर बार जब आप लॉगिन करते हैं, तो अपने खाते में दिखाई देने वाले अंतिम लॉगिन विवरण की जांच करें। अगर यह आपकी अंतिम लॉगिन गतिविधि से मेल खाता है, तो इसका मतलब है कि आपका खाता उतना ही सुरक्षित और सुरक्षित है जितना यह हो सकता है। हालांकि, अगर अंतिम लॉगिन विवरण आपकी गतिविधि से मेल नहीं खाता है और संदिग्ध गतिविधि के संकेत दिखाता है, तो तुरंत बैंक को इसकी सूचना दें।

आप ऑनलाइन और ऑफलाइन धोखाधड़ी से खुद को कैसे बचा सकते हैं?

- **स्कैम पर नज़र रखें:** फिशिंग, विशिंग, साइबरस्टॉकिंग, स्किमिंग इत्यादि कुछ ऐसे स्कैम हैं जिनका उपयोग अपराधी आपके व्यक्तिगत विवरण मांगने में आपको धोखा देने के लिए करते हैं। इन स्कैम पर नज़र रखें और उन लिंक, ईमेल और अटैचमेंट पर क्लिक न करें जो संदिग्ध दिखते हैं।
- **पासवर्ड नियमित रूप से अपडेट करें:** आपका उपयोगकर्ता नाम और पासवर्ड ही एकमात्र चीजें हैं जो अपराधियों को आपके डेटा का एक्सेस करने से रोकते हैं। सुनिश्चित करें कि आप दोनों को नियमित रूप से अपडेट करते हैं, कम से कम दो महीने में एक बार। अक्षरों, संख्याओं और विशेष वर्णों का उपयोग करते हुये यादृच्छिक पासवर्ड का उपयोग करें। सबसे आम या प्रासंगिक पासवर्ड न चुनें क्योंकि उन्हें क्रैक करना बहुत आसान होता है।
- **सुरक्षित वेबसाइटों का उपयोग करें:** कभी भी ईमेल में एम्बेड किए गए किसी भी लिंक पर क्लिक न करें; अपने ब्राउजर में लिंक टाइप करना सुरक्षित है। यूआरएल को ध्यान से पढ़ें क्योंकि अधिकांश फिशर धोखाधड़ी वाली गतिविधियों के लिए समान दिखने वाली वेबसाइट का सेटअप करते हैं। अगर आपको यूआरएल में वर्तनी की त्रुटि दिखाई देती है या आपको लगता है कि कोई वेबसाइट असुरक्षित दिखती है, तो जोखिम न लें। सभी गतिविधियों को वहीं रोक दें।
- **व्यक्तिगत जानकारी सुरक्षित रखें:** अगर आप अपने फोन में अपनी जानकारी की कॉपी रखते हैं, तो हमेशा अपने फोन को लॉक रखने के लिए पिन/पासवर्ड सेट करें। अगर आप अपने खाते की जानकारी वाले बैंक मेलर को संग्रहीत करते हैं, तो इसे लॉकर या किसी ऐसे स्थान पर सुरक्षित रखें जो आसानी से एक्सेस करने योग्य न हो।
- **सोशल इंजीनियरिंग से बचें:** सोशल मीडिया पर अहम जानकारी साझा न करें क्योंकि अधिकांश हमलावर जानकारी प्राप्त करने के लिए लोगों से बातचीत वाली विधि का उपयोग करते हैं। अपने विवरण को निजी रखें और उन लोगों के किसी भी कनेक्शन/मित्र अनुरोधों से सावधान रहें जिन्हें आप नहीं जानते हैं। आप व्यक्तिगत/आंतरिक जानकारी के बारे में पूछने वाले व्यक्तियों से अवांछित फोन कॉल, एसएमएस या ईमेल पर संदेह करके सोशल इंजीनियरिंग हमले का शिकार होने से बच सकते हैं। वेबसाइट की सुरक्षा की जांच करने से पहले इंटरनेट पर संवेदनशील जानकारी भेजने से बचें। ऐसा एंटी-वायरस सॉफ्टवेयर भी इंस्टॉल करने की सलाह दी जाती है जो आपके सिस्टम को धोखाधड़ी वाली गतिविधियों से बचा सकता है।
- **अपने इंटरनेट कनेक्शन को सुरक्षित करें:** यह सलाह दी जाती है कि बैंकिंग और वित्तीय लेनदेन करने के लिए कभी भी सार्वजनिक नेटवर्क का उपयोग न करें। हालांकि, आपको यह भी सुनिश्चित करना होगा कि आपका व्यक्तिगत या घरेलू कनेक्शन पूरी तरह से सुरक्षित है। पासवर्ड सेट करें, ताकि अजनबियों के पास आपके इंटरनेट कनेक्शन का एक्सेस न हो।

- **त्यागने से पहले दस्तावेजों के छोटे-छोटे टुकड़े करें:** अगर आप किसी भी दस्तावेज़ को फेंक रहे हैं जिसमें व्यक्तिगत जानकारी है, तो सुनिश्चित करें कि आप दस्तावेज़ को त्यागने से पहले उसके पूरी तरह से छोटे-छोटे टुकड़े करते हैं। अपराधियों को लोगों की पहचान चुराने के लिए संदेश चोरी के लिए उपयोग करने के लिए जाना जाता है।
- **संदिग्ध ईमेल हटाएं:** ईमेल लोगों की निजी जानकारी का एक्सेस करने के लिए सबसे अधिक इस्तेमाल किए जाने वाले तरीकों में से एक है। अगर आपको अपने इनबॉक्स में ऐसा कोई भी ईमेल मिलता है जो संदिग्ध दिखता है या किसी ऐसे व्यक्ति द्वारा भेजा गया है जो आपकी संपर्क सूची में नहीं है, तो ईमेल को खोले बिना हटा दें। अगर आप उन्हें खोलते हैं, तो किसी भी लिंक या अटैचमेंट पर क्लिक करने से सावधान रहें क्योंकि ऐसी फ़ाइलों में मैलवेयर और वायरस होते हैं जो आपके सिस्टम में जाने और संवेदनशील जानकारी स्कैन करने के लिए डिज़ाइन किए गए हैं।

अपने रोजमर्रा के जीवन में इन सलाहों और ट्रिक को लागू करने से यह सुनिश्चित होगा कि आपको हर बार सुरक्षित बैंकिंग अनुभव मिलता है। आज के डिजिटल युग में ऑनलाइन सुरक्षा बनाए रखना भी महत्वपूर्ण है क्योंकि हमारे जीवन का बहुत बड़ा हिस्सा पहले से ही दुनिया में हर व्यक्ति द्वारा देखे जाने के लिए मौजूद है। ऑनलाइन सुरक्षा और बचाव सुनिश्चित करने के लिए इन सुरक्षित बैंकिंग सलाहों को अपनाएं।

किसी भी अतिरिक्त सहायता के लिए या धोखाधड़ी की रिपोर्ट करने के लिए, नीचे बताए गए अनुसार तुरंत बैंक से संपर्क करें और हमें आपकी मदद करने में खुशी होगी!

बैंकिंग और क्रेडिट कार्ड : +91 22 6232 7777;

पूरी जानकारी के साथ reportfraud@rbl.bank.in पर ईमेल भेजें।

साइबर अपराध की शिकायत करें:

यदि आप साइबर अपराध का शिकार हो जाते हैं, तो तुरंत काररवाई करें। राष्ट्रीय साइबर अपराध हेल्पलाइन 1930 पर कॉल करें और अपनी शिकायत https://cybercrime.gov.in/ पर दजर करें। आप Sancharsaathi Portal के माध्यम से भी शिकायत दजर कर सकते हैं। समय पर की गई शिकायत से आगे की ठगी रोकी जा सकती है और दूसरों को भी सुरक्षित रखा जा सकता है।