धोखाधड़ी वाली गतिविधियों से सुरक्षित रहने के लिए सलाह

पिछले दशक में, वित्तीय धोखाधड़ी, विशेष रूप से क्रेडिट कार्ड से जुड़ी धोखाधड़ी, बहुत अधिक बढ़ गई है। लोग कई बार धोखाधड़ी के तरीके का शिकार हो जाते हैं और व्यक्तिगत/ महत्वपूर्ण जानकारी का खुलासा करते हैं जिससे धोखेबाजों को आपकी व्यक्तिगत जानकारी के लिए तरीका मिलता है और वित्तीय गलतफहमी पैदा होती है। हालांकि, जानकारी के दौर में हमें इनका मुकाबला करने के लिए कई साधन मिले हैं, लेकिन हमें खुद को बचाने के लिए हर समय सतर्क और सूचित रहकर खुद को सशक्त बनाना चाहिए।

1. आरबीएल बैंक कभी भी व्यक्तिगत विवरण नहीं मांगता है!

अगर आपको कभी भी आरबीएल बैंक से कोई कॉल, टेक्स्ट मैसेज या ईमेल मिलता है जिसमें आपके व्यक्तिगत विवरण मांगे जा रहे हैं, जैसे कि 16 अंकों वाला क्रेडिट कार्ड नंबर, समाप्ति तिथि, सीवीवी, पैन नंबर, ओटीपी, एमपिन इत्यादि, तो उन्हें न बताएं। हम कभी भी निजी जानकारी नहीं मांगेंगे और आप इस तरह की जानकारी धोखेबाज को दे सकते हैं।

2. अनजान कॉलर पर भरोसा न करें!

आपसे आपके कार्ड या व्यक्तिगत विवरण के लिए पूछने वाले असत्यापित कॉल को पूरी तरह से अनदेखा किया जाना चाहिए। हमेशा इस बात को जानने का प्रयास करें कि आपसे संभावित गोपनीय जानकारी कैसे पूछी जा रही है। इन कॉल को आमतौर पर किसी प्रकार के प्रोत्साहन के साथ जोड़ा जाता है, जैसे कि "हम आपकी क्रेडिट सीमा बढ़ाएंगे" या "हमें लकी ड्रॉ में आपको शामिल करने के लिए आपके विवरण की आवश्यकता है", ये आपको विवरण देने के लिए मजबूर करने के उद्देश्य हैं जिससे धोखाधड़ी होगी।

3. ओटीपी संदेशों की दोबारा जांच करें!

हमेशा ओटीपी के उद्देश्य को सत्यापित करें और कभी भी कॉल, एसएमएस या ईमेल पर किसी के साथ ओटीपी या कार्ड विवरण साझा न करें। आरबीएल बैंक से लेनदेन के लिए मिलने वाले ओटीपी एसएमएस में हमेशा लेनदेन की राशि और व्यापारी का नाम होगा। ऑनलाइन खरीदारी करने से पहले आपको हर बार दोबारा जांच करनी चाहिए।

4. संदिग्ध प्रस्तावों से बचें!

अगर कोई प्रस्ताव इतना अच्छा लगता है कि उसका सही होना संभव नहीं है, तो सम्भावना है कि वह वैसा ही है। ऐसे प्रस्तावों को अनदेखा करें जो अवास्तविक लगते हैं क्योंकि उनमें आपसे स्कैम करने की संभावना है। उदाहरण के लिए, "आपने मुफ्त कार जीती है" या "इस लिंक पर क्लिक करें

और मुफ्त गिफ्ट वाउचर प्राप्त करें" जैसे प्रस्ताव में खाते के विवरण के लिए अनुरोध किया जाएगा, हालांकि, ये धोखाधड़ी करने वाले लोगों के लिए आपके विवरण तक पहुंचने के साधन हैं और इन्हें अनदेखा किया जाना है। कोई भी विवरण देने से पहले, विश्वसनीय स्रोतों से मिले प्रस्तावों को भी सत्यापित किया जाना चाहिए। कभी भी संदिग्ध लिंक और अटैचमेंट न खोलें।

5. असत्यापित ऐप्स से दूर रहें!

ऐप स्टोर पर असत्यापित ऐप्स से आपके मोबाइल डिवाइस से ही डेटा निकाला जा सकता है! ऐप डाउनलोड करते समय, सुनिश्चित करें कि यह विश्वसनीय स्रोत से है और अपने डिवाइस पर उन्हें अनुमतियां देने से पहले खोजबीन करें! बहुत ही आम स्कैम धोखाधड़ी वाले वे संचार है जिनमें आपसे "केवाईसी के लिए इस ऐप को डाउनलोड करें" या "जारी रखने के लिए इस लिंक को खोलें" कहा जाता है, हालांकि, किसी भी व्यक्ति को इन पर ध्यान देना चाहिए और केवल सत्यापित स्रोतों पर भरोसा करना चाहिए।

6. धोखा न खाएं!

नकली कॉल और ईमेल की घटना आज बढ़ती जा रही है और धोखाधड़ी करने वाले लोग उन लोगों को शिकार बनाते हैं जो इन बातचीत की प्रामाणिकता को सत्यापित नहीं करते हैं। सुनिश्चित करें कि आपके संपर्क वास्तविक हैं, न कि धोखाधड़ी वाले। यहां ध्यान रखने वाली कुछ बातें दी गई हैं::

- ग्राहक सेवा केंद्र के विवरण के लिए हमेशा आरबीएल बैंक की आधिकारिक वेबसाइट (www.rblbank.com) पर जाएं
- हमेशा प्रेषक के ईमेल पते की जांच करें, कभी-कभी छोटी-छोटी ग़लतियाँ होती हैं जो आँखों से लगभग अदृश्य होती हैं, जैसे कि 'Bnak' के बजाय 'Bank', जिसे आप तब तक पंजीकृत नहीं करेंगे जब तक कि स्पष्ट रूप से इसकी तलाश न हो। इसके अलावा, संदेह होने पर सीधे बैंक से संपर्क करें और हम आपके किसी भी संदेह को स्पष्ट करेंगे।
- जब आप अपने खाते के विवरण को ऑनलाइन दर्ज करते हैं/देखते हैं, तो हमेशा जांचें कि लिंक में "https://online.rblbank.com" है या नहीं।
- कभी भी किसी भी एसएमएस/ईमेल/सोशल मीडिया संदेशों का जवाब न दें जो आपकी व्यक्तिगत जानकारी चाहते हैं।

7. अज्ञात अटैचमेंट पर क्लिक करने से बचें!

अवैध स्रोत से मिले ईमेल या टेक्स्ट मैसेज में दिए गए अटैचमेंट को खोलने से आपके विवरण दिख सकते हैं। निम्नलिखित की जांच करें:

- क्या मुझे आमतौर पर इस स्रोत से अटैचमेंट मिलता है?
- क्या यह वैध स्रोत है?

ध्यान से सोचें। और अस्पष्ट या अविश्वसनीय स्रोतों से मिले अटैचमेंट को खोलने से बचें।

8. कभी भी व्यक्तिगत या वित्तीय जानकारी का खुलासा न करें!

आप वित्तीय धोखाधड़ी से सुरक्षा की अंतिम कड़ी हैं। आपके क्रेडिट कार्ड के साथ आने वाले सुरक्षा के सभी लेयर के बावजूद, असावधान रहने पर आपको परेशानी हो सकती है। हमेशा अपनी जानकारी को लेकर सतर्क रहें और धोखाधड़ी करने वाले व्यक्तियों का लक्ष्य न बनें।

9. अपने खाते पर धोखाधड़ी वाली गतिविधियों से सतर्क रहें!

- अपनी वित्तीय गतिविधियों पर नजर रखें।
- किसी भी फर्क को देखने के लिए अपने स्टेटमेंट की समीक्षा करें
- कुछ भी संदिग्ध लगने पर तुरंत बैंक से संपर्क करें और अपना कार्ड ब्लॉक करें।

हम हर दिन बैंकिंग को सुरक्षित बनाने का प्रयास कर रहे हैं।

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।