

ग्राहक जागरूकता-सायबर धोके आणि फसवणूक

फसवणूक करणाऱ्या व्यक्ती समाज माध्यमे, मोबाइल फोन कॉल्स इत्यादींद्वारे आविष्कारी फसवणूक पध्दती वापरून सामान्य लोकांना फसवत आहेत आणि चुकीच्या दिशेला नेत आहेत. हे लक्षात घेऊन, भारतीय रिझर्व बँक (आरबीआय) सामान्य लोकांना फसवणूक करणारे संदेश, संशयास्पद कॉल्स, अनोळखी लिंक्स, नकली सूचना, अनाधिकृत क्यूआर कोड्स इत्यादींपासून सावध करत आहे. ज्याद्वारे सवलतीचे आश्वासन दिले जाते/बँकांकडून जलद प्रतिसाद दिला जातो आणि कोणत्याही प्रकारची आर्थिक सेवा दिली जात असल्याची भासवले जाते.

फसवणूक करणारे गोपनीय तपशील जसे की वापरकर्ता आयडी, लॉगिन/ट्रान्झॅक्शन पासवर्ड, ओटीपी (वन टाइम पासवर्ड), डेबिट/क्रेडिट कार्ड तपशील जसे की पिन, सीव्हीव्ही, एक्सपायरी डेट आणि इतर वैयक्तिक माहिती मिळविण्याचा प्रयत्न करतात. फसवणूक करणाऱ्यांद्वारे वापरल्या जाणाऱ्या काही ठराविक मोडस ऑपरेंडी आहेत -

- फिशिंग/विशिंग/एसएमएसिंग - बनावट ईमेल/फोन कॉल/एसएमएसद्वारे फसवणूक करण्याचे तंत्र अनुक्रमे ग्राहकांना त्यांच्या बँकेकडून/विश्वसनीय संस्थेकडून आहे असे भासवून फसवणे. बनावट ईमेल आणि एसएमएसमध्ये हानिकारक लिंक असू शकतात जे गोपनीय माहिती काढू शकतात किंवा मालवेअर लॉच करू शकतात. केव्हायसी-अपडेट, जॉब ॲप्लिकेशन, खाते/सिम-कार्ड अनब्लॉक करणे, इन्कम टॅक्स रिटर्न भरणे, रिवॉई पॉइंट लॅप्स करणे, कॅशबॅक ऑफर इ.च्या बहाण्याने ग्राहकांना गोपनीय तपशील शेअर करण्याचे आमिष दाखवले जाते.
- रिमोट ॲक्सेस - फसवणूक करणारा ग्राहकांना त्यांच्या मोबाईल फोन/कॉम्प्युटरवर एक ॲप्लिकेशन डाउनलोड करण्याचे आमिष देतो, जे ग्राहकांच्या डिवाइसद्वारे सर्व ग्राहकांच्या डेटामध्ये प्रवेश करू शकते.
- यूपीआयद्वारे फसवणूक - पैसे मिळवण्यासाठी 'एंटर यूआर यूपीआय पिन' सारख्या संदेशांसह बनावट पेमेंट विनंत्या पाठवून यूपीआयच्या 'कलेक्ट रिक्वेस्ट' वैशिष्ट्याचा गैरवापर केला जातो.
- बनावट हेल्लोलाइन/ग्राहक सेवा संपर्क तपशील-वेबपेजेस/सोशल मीडियावर बँका/ई-वॉलेट पुरवठादारांचे खोटे क्रमांक सर्च इंजिन इत्यादीद्वारे दाखवले जातात.

आरबीआय जनतेला आवाहन करते की कोणतेही डिजिटल (ऑनलाइन/मोबाईल) बँकिंग/पेमेंट व्यवहार करताना सर्व योग्य खबरदारी घेऊन सुरक्षित डिजिटल बँकिंगची पध्दत अवलंबावी.

सुरक्षित डिजिटल बँकिंगची पध्दत

- एटीएम/डेबिट कार्ड/क्रेडिट कार्ड तपशील यांसारखे खाते तपशील कधीही कोणालाही शेअर करू नका, अगदी बँक अधिकारी खरे असले तरीही शेअर करू नका.
- केव्हायसी अपडेट न करण्याच्या बहाण्याने तुमचे खाते ब्लॉक करण्याची धमकी देणारा कोणताही फोन कॉल/ईमेल आणि ते अपडेट करण्यासाठी लिंकवर क्लिक करण्याची सूचना ही फसवणूक करणाऱ्यांची सामान्य पध्दत आहे. केव्हायसी अद्ययावत करण्यासाठी/जलद मिळवण्यासाठी ऑफरला प्रतिसाद देऊ नका. तुमच्या बँक/एनबीएफसी/ई-वॉलेटदात्याच्या अधिकृत वेबसाइटचा उपयोग करा किंवा शाखेशी संपर्क साधा.
- पैशांच्या पावतीचा समावेश असलेल्या व्यवहारांसाठी बारकोड/क्यूआर कोड स्कॅन करणे किंवा एमपिन एंटर करणे आवश्यक नाही. त्यामुळे असे करण्यास सांगितले असल्यास सावधगिरी बाळगा.
- संपर्काच्या तपशीलांसाठी नेहमी बँक/एनबीएफसी/ई-वॉलेटदात्याच्या अधिकृत वेबसाइटचा उपयोग करा. इंटरनेट सर्च इंजिनवरील संपर्क क्रमांक फसवे असू शकतात.
- तुम्ही सुरू न केलेल्या व्यवहारासाठी तुमचे खाते डेबिट करण्यासाठी ओटीपी मिळाल्यास, तुमच्या बँक/ई-वॉलेटदात्याला ताबडतोब कळवा. न केलेल्या व्यवहारासाठी तुम्हाला डेबिट एसएमएस प्राप्त झाल्यास, तुमच्या बँक/ई-वॉलेटदात्याला ताबडतोब कळवा आणि यूपीआय सह डेबिटचे सर्व मोड ब्लॉक करा. तुम्हाला तुमच्या खात्यामध्ये फसवणूक झाल्याचा संशय आल्यास, इंटरनेट/मोबाइल बँकिंगसाठी सक्षम केलेल्या लाभार्थी यादीमध्ये कोणतीही भर पडली आहे का ते तपासा.
- तुमच्या आर्थिक सेवादात्याकडून सूचनांसाठी तुमचे ईमेल आणि फोन संदेश नियमितपणे तपासा. कार्ड/खाते/वॉलेट ब्लॉक करण्यासाठी तुमच्या बँक/एनबीएफसी/सेवादात्याला आढळलेल्या कोणत्याही अनधिकृत व्यवहाराची त्वरित तक्रार करा, जेणेकरून पुढील नुकसान टाळता येईल.
- तुमचे कार्ड सुरक्षित करा आणि व्यवहारांसाठी दैनिक मर्यादा सेट करा. तुम्ही मर्यादा सेट करू शकता आणि देशांतर्गत/आंतरराष्ट्रीय वापरासाठी सक्रिय/निष्क्रिय देखील करू शकता. हे फसवणुकीमुळे होणारे नुकसान मर्यादित करू शकते.

अधिक माहितीसाठी भेट द्या: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=5318