रिझर्व्ह बॅकेचे सायबर थ्रेटस् व फ्रॉडस्बाबतच्या सुचना

फसवुणक करणारे गोपनीय माहिती उदा . जसे की वापरकर्ता आयडी , लॉगिन /ट्रान्झॅक्शन पासवर्ड, ओटीपी (वन टाइम पासवर्ड), डेबिट / क्रेडिट कार्डचा पिन , सीव्हीव्ही नंबर, एक्सपायरी डेट आणि इतर वैयक्तिक माहिती मिळविण्याचा प्रयन्त करतात . फसवणूक करणा-यांद्वारे वापरल्या जाणा-या काही ठराविक कार्यप्रणाली खालीलप्रमाणे आहेत .

1. Vishing (विशिंग) - फोन कॉलद्वारे केवायसी अपडेट, खाती / सिम कार्ड अनब्लॉक करणे, डेबिट केलेली रक्कम जमा करणे इ . करण्याच्या बहाण्याने कस्टमरची गोपानीय माहिती गोळा करण्यासाठी आमिष देवून बॅक / नॉन-बॅक ई-वॉलेट प्राव्हाईडर /टेलीकॉम सर्व्हीस प्रोव्हाईडरकडील असल्याचे सांगतात .
2. Phishing (फिशिंग) - फसवणूक केलेले ई - मेल आणि / किंवा एसएमएस हे ग्राहकांना विचारात फसवण्यासाठी डिझाईन केलेले असतात व सदरचे ई - मेल्स किंवा एसएमएस हे त्यांच्या बॅका किंवा वॉलेट प्राव्हाईडर्सकडून आले असल्याचे दाखवितात आणि त्याचा गोपनीय तपशील काढण्यासाठी लिंक्स आहेत .
3. Remote Access (रिमोट ऍक्सेस) - कस्टमरना त्यांच्या मोबाईल फोनवर / कॉम्प्युटरवर एक ॲप्लिकेशन डाउनलोड करण्याचे आमिष दाखवून त्या कस्टमरच्या डिव्हाइसवरील सर्व कस्टमरच्या डेटाचा ॲक्सेस करण्याचा प्रयन्त करतात .
4. पैसे मिळवण्यासाठी 'Enter Your UPI Pin' सारख्या मेसेजसह बनावट पेमेंट विंनत्या पाठवुन UPI च्या 'Collect Request' फिचरचा गैरवापर करतात .
5. बॅका / ई -वॉलेट प्रोव्हाईडरचे फेक नंबर आणि सर्च इंजिनं इ . द्वारे वेबपेजेस / सोशल मीडियावर डिस्पेले केले जातात .

सुरक्षित डिजिटल बॅकिंगचा सराव

1. तुमची वैयक्तिक माहिती शेअर करू नका.

- खाते क्रंमाक , लॉगिन आयडी, पासवर्ड , पिन् , यूपीआय - पिन ,ओटीपी ,सीव्हीव्ही नंबर, एक्सपायरी डेट, एटीएम / डेबिट कार्ड / क्रेडिट कार्ड डिटेल्स, मोबाईल आणि इंटरनेट बॅंकीग पासवर्ड, मपीन, टीपीन आणि कुपीन, आधार कार्ड आणि पॅन कार्ड डिटेल्स कधीही कोणाशीही शेअर करू नका, अगदी बॅंक अधिका-यांसोबतही नाही , जरी ते खरे वाटले तरी. फोन / एसएमएस / ई-मेलवर माहिती कधीही कुणालाही शेअर करू नका.

2. कोणत्याही बनावट कॉल किंवा कोणत्याही ऑफरला प्रतिसाद देऊ नका.

- KYC अपडेट न करण्याच्या बहाण्याने तुमचे खाते ब्लॉक करण्याचा कोणताही फोन कॉल / ई-मेल आणि ते अपडेट करण्यासाठी लिंकवर सुचना ही फसवणूक करणा-याची सामान्य पद्धत आहे. KYC अपडेट / जलद मिळवण्यासाठी ऑफरला प्रतिसाद देऊ नका. नेहमी अधिकृत वेबसाइट्चाच वापर करावा.

3. कोणतेही अज्ञात ॲप डाउनलोड करू नका.

- तुमच्या फोन/डिव्हाइसवर अज्ञात ॲप डाउनलोड करू नका. ॲप तुमचा कॉन्फेडेनशल डेटा ॲक्सेस करू शकतो.

4. आवश्यक नसेल तेथे बारकोड किंवा QR कोड स्कॅन करू नका.

- ऑनलाईन व्यवहारांसाठी बारकोड / QR कोड स्कॅन करणे किंवा MPIN देणे आवश्यक नाही. पण असे करण्यास सांगितले असल्यास सावधगिरी बाळगा.

5. नेहमी अधिकृत वेबसाईट वापरा.

- नेहमी बॅंक / ई-वॉलेट प्राव्हाईडरच्या अधिकृत वेबसाईट्च ॲक्सेस कराव्यात. इंटरनेट सर्च इंजिनवरील कॉन्टेक्ट डिटेल्स हे फसवे असू शकतात.

6. फक्त सुरक्षित आणि विश्वसनीय वेबसाईट वापर.

- स्पेलिंग जुटींसाठी ई-मेल / SMS मध्ये प्राप्त URL आणि डोमेन नेम चेक करण्यात यावे. ऑनलाईन बॅंकिगसाठी फक्त व्हेरिफाईड, सुरक्षित आणि विश्वासार्ह वेबसाईट/ ॲप्स वापरा, म्हणजे "https" ने सुरू होणारी वेबसाईट. संशय आल्यास तात्काळ स्थानिक पोलिसांना / सायबर गुन्हे शाखेला कळवा.

7 . कोणतेही संशयास्पद व्यवहार करू नका .

- तुम्ही न केलेल्या ट्रान्झक्शनसाठी तुमच्या खातेमधुन डेबिट करण्यासाठी OTP मिळाल्यास , तुमच्या बॅक / ई -वॉलेट प्राव्हाईडरला तोबडतोब कळवा . न केलेल्या ट्रान्झक्शनसाठी तुम्हाला डेबिट एसएमएस प्राप्त झाल्यास ,तुमच्या बॅक / ई -वॉलेट प्राव्हाईडरला तोबडतोब कळवा आणि यूपीआय सह डेबिटचे सर्व मोड ब्लॉक करण्यात यावे . तुम्हाला तुमच्या खात्यात फसवणूक झाल्याचा संशय आल्यास ,इंटरनेट /मोबाईल बॅकिंगमध्ये कोणती ॲडीशनल बेनिफिशीर नावाचे यादी दिसते का ते पण चेक करावे

8 . तुमचा पासवर्ड शेअर करू नका .

- तुमच्या बॅक / ई -वॉलेट खात्याशी लिंक केलेल्या तुमच्या ई-मेलचा पासवर्ड शेअर करू नका .ई-कॉमर्स / सोशल मिडिया साईट्स आणि तुमच्या बॅक खात्याशी लिंक असलेल्या तुमचे बॅक खाते /ई मेल चे पासवर्ड हे कॉमन नसावेत . पब्लीक, ओपन किंवा फ्रि नेटवर्क द्वारे बॅकिंग टाळा .
- कोणत्याही वेबसाईट / ॲप्लिकेशनमध्ये तुमचा ई-मेल आयडी म्हणून रजिस्टर करताना तुमच्या ई-मेलचा पासवर्ड "पासवर्ड" शब्द सेट करू नका .तुमचा ई-मेल ॲक्सेस करण्यासाठी वापरला जाणारा पासवर्ड, जर तुमच्या खात्याशी लिंक केलेला असल्यास तो युनिक असावा आणि फक्त ई -मेल ॲक्सेससाठी वापरण्यात यावा आणि इतर कोणत्याही वेबसाईट / ॲप्लिकेशन ॲक्सेस करण्यासाठी नाही .

9 . कोणत्याही सल्ल्याने दिशाभूल होवु नका .

- परकीय पैसे पाठवणे ,कमिशनी पावती किंवा लॉटरी जिंकणे यासाठी तुमच्या वतीन आरबीआयकडे पैसे जमा करण्या-या सुचनांना दिशाभूल होवू नका .

10 . कोणत्याही अनधिकृत व्यवहारासाठी त्वरित तक्रार करा .

- फायन्शीयल सर्व्हीस प्रोव्हाईडरच्या अर्लटसचे ई-मेल आणि फोन मेसेजस रेग्युलरली चेक करावे . कोणतेही अनधिकृत ट्रान्झक्शन तुमच्या बॅक/एनबीएफसी/सर्व्हीस प्रोव्हाईडरवरून आढळल्यास तात्काळ कार्ड/ खाते/वॉलेट ब्लॉक करा , जेणेकरून पुढील नुकसान टाळता येईल .

11 . तुमचे व्यवहार सुरक्षित करा .

- तुमचे कार्ड सुरक्षित करा आणि डेली ट्रान्झक्शन लिमीट सेट करा . तुम्ही लिमिटी देखील सेट करू शकता आणि देशांतर्गत/आंतरराष्ट्रीय वापरासाठी ॲक्टीव्हेट / डिॲक्टीव्हेट करू शकता .या फसवणुकीमुळे होणा-या नुकसानवर मर्याद घालता येतील .

12 . सोशल मीडियावर तुमची गोपनीय सेटिंग्ज लॉक करा .

- तुमचे पासवर्ड शोधण्यासाठी फसवणुक करणारे सोशल मीडिया प्रोफाइलचा वापर करू शकतात आणि तुमचा पासवर्ड रिसेट करण्यासाठी सिक्युरिटी प्रश्नांची उत्तर देऊ शकतात . सोशल मीडियावर तुमची प्रायव्हसी सेटिंग्ज लॉक करा आणि वाढदिवस ,पत्ता, आईचे नाव इ . पोस्ट करणे टाळा . अनोळखी व्यक्तीच्या विनंतीला उत्तर देऊ नका .

13 . तुमचे इंटरनेट कनेक्शन सुरक्षित आणि संरक्षित ठेवा

- स्ट्रॉग पासवर्डने तुमच्या घरचे आणि ऑफिसचे वायरलेस नेटवर्क नेहमी सुरक्षित ठेवा . सार्व जनिक वायफाय नेटवर्क वापरताना योग्य ती काळजी घ्या .

14 . तुमचा मोबाईल आणि कॉम्प्युटर अपडेट ठेवा .

- संगणक / लॅपटॉप/ टॅब /स्मार्ट फोन ऑपरेटिंग सिस्टीम ,ब्राउझर ,अँटी- व्हायरस सॉफ्टवेअर नेहमी अपडेट ठेवा .

15 . अँटी- व्हायरस सॉफ्टवेअर वापर करावा .

- तुमच्या डिव्हाईसमध्ये नेहमी चांगल्या दर्जाचे पेड अँटी- व्हायरस / मॅलेवेअर सॉफ्टवेअर इंस्टॉल करा .

16 . स्ट्रॉग पासवर्ड सेट करा .

- तुमच्या डिव्हाईससाठी नेहमी स्ट्रॉग पासवर्ड सेट करा . स्ट्रॉग पासवर्ड किमान **8** कॅरेक्टरचा असावा आणि त्यात कॅपिटल आणि लोअर केस लेटरचे मिक्स , किमान एक संख्या आणि किमान एक स्पशेल कॅरेक्टर असावा .