**परिशिष्ट 7: ग्राहक जागृती- सायबर धोके व फसवणूक**

असे आढळून आले आहे की काही तत्त्वशून्य घटक हे सोशल मीडिया तंत्रे, मोबाइल फोन कॉल्स, इत्यादींचा समावेश असणाऱ्या नावीन्यपूर्ण कार्यपद्धतींचा वापर करून सर्वसामान्य जनतेची फसवणूक व दिशाभूल करत आहेत. हे लक्षात घेता, बँकेकडून आणि वित्तीय सेवा प्रदात्यांकडून कोणत्याही प्रकारे सलवत /शीघ्र प्रतिसाद मिळवून देण्यास मदत करण्याचे वचन देणारे फसवणुकीचे संदेश, बनावट कॉल्, अज्ञात लिंक्स, खोट्या नोटिफिकेशन्स, अप्राधिकृत क्यूआर कोड्स यांपासून जनतेने सावध राहावे असा डीसीबी बँक सावधगिरीचा इशारा देत आहे.

घोटाळेबाज व्यक्तींनी यूज़र आयडी, लॉगिन/ट्रान्झॅक्शन पासवर्ड, वन टाइम पासवर्ड (ओटीपी), तसेच पिन, सीव्हीव्ही, मुदतसमाप्ती तारीख यांसारखा डेबिट/क्रेडिट कार्ड तपशील व इतर व्यक्तिगत माहिती यांसारखा गोपनीय तपशील प्राप्त करण्याचा प्रयत्न करणे. घोटाळेबाज व्यक्तींकडून वापरण्यात येणारी सर्वसामान्य कार्यपद्धती पुढीलप्रमाणे आहे:

- व्हिशिंग- केवायसी अद्ययावत करणे, खाते/सिम कार्ड अनब्लॉक करणे, डेबिट झालेली रक्कम पुन्हा क्रेडिट (जमा करणे) इत्यादीच्या बहाण्याने गोपनीय तपशीलाची देवाणघेवाण करण्यास ग्राहकाला भाग पाडण्यासाठी बँकेकडून/नॉन-बँक ई-वॉलेट प्रदात्याकडून/टेलिकॉम सेवा प्रदात्याकडून बोलत असल्याचे भासवणे.
- फिशिंग- ग्राहकाला त्याच्या बँकेकडून/ई-वॉलेट प्रदात्याकडून संपर्कव्यवहार आलेला आहे असे भासवण्याच्या दृष्टीने तयार करण्यात आलेले बनावट ईमेल्स आणि/किंवा एसएमएस आणि त्यामध्ये गोपनीय तपशील प्राप्त करण्यासाठी लिंक्स समाविष्ट असतात.
- दुरस्थ ॲक्सेस- ग्राहकाला त्याच्या मोबाइल फोनमध्ये/कॉम्प्युटरमध्ये ॲप्लिकेशन डाउनलोड करण्याचे आमिष दाखवणे, असे ॲप्लिकेशन्स ग्राहकाच्या डिव्हाइसमधील डेटा प्राप्त करू शकतात.
- पैसे प्राप्त करण्यासाठी 'तुमचा यूपीआय पिन दाखल करा' यांसारख्या संदेशासह बनावट पेमेन्ट विनंती पाठवून यूपीआयच्या 'कलेक्ट रिक्वेस्ट' वैशिष्ट्याचा गैरवापर करणे.
- वेबपेजेसवर/सोशल मीडियावर बँकांचे/ई-वॉलेट प्रदात्यांचे बनावट संपर्क क्रमांक देणे आणि सर्च इंजिन्स इत्यादींवर ते प्रदर्शित करण्यात येणे.

कोणतेही डिजिटल बँकिंग/पेमेन्ट व्यवहार (ऑनलाइन/मोबाइल) पार पाडताना, सार्वजनिक यथोचित खबरदारी घेऊन सुरक्षित डिजिटल व्यवहार करण्याची विनंती डीसीबी बँकेद्वारे जनतेला करण्यात येत आहे. यामुळे वित्तीय आणि/किंवा इतर नुकसानाला प्रतिबंध करण्यास मदत होईल.

सुरक्षित डिजिटल बँकिंग कार्यपद्धती

- कधीही खाते क्रमांक, लॉगिन आयडी, पासवर्ड, पिन, यूपीआय-पिन, ओटीपी, एटीएम/डेबिट कार्ड, क्रेडिट कार्ड तपशील अशा तुमच्या खाते तपशीलाची कोणासोबतही, अगदी बँकेच्या अधिकाऱ्यांसोबतही, ते कितीही खरे वाटत असले तरीही, देवाणघेवाण करू नका.
- केवायसी अद्ययावत केली नाही या बहाण्याने तुमचे खाते ब्लॉक करण्याची धमकी देणारा कोणतेही दूरध्वनी संपर्क/ईमेल आणि त्यामध्ये केवायसी अद्ययावत करण्यासाठी लिंकवर क्लिक करण्याची सूचना करण्यात येते ही घोटाळेबाजांची सर्वसामान्य कार्यपद्धती आहे. केवायसी अद्ययावत करण्याच्या/ती जलद करून घेण्याच्या ऑफर्सना प्रतिसाद देऊ नका. नेहमी तुमच्या बँकेच्या एनबीएफसी/ई-वॉलेट प्रदात्याच्या अधिकृत वेबसाइटवर जा किंवा शाखेशी संपर्क साधा.
- तुमच्या फोनवर किंवा डिव्हाइसवर कोणतेही अज्ञात ॲप डाउनलोड करू नका. असे ॲप्स तुमची गोपनीय माहिती गुप्तपणे पाहू शकतात.
- पैसे प्राप्त करण्याच्या व्यवहारांमध्ये बारकोड्स किंवा क्यूआर कोड्स स्कॅन करण्याची किंवा एमपिन दाखल करण्याची आवश्यकता नाही. म्हणून, असे करण्यास सांगितल्यास खबरदारी घ्या.
- संपर्क तपशीलासाठी नेहमी तुमच्या बँकेच्या/ एनबीएफसीच्या/ई-वॉलेट प्रदात्याच्या अधिकृत वेबसाइटवर जा. इंटरनेट सर्ज इंजिन्सवरील संपर्क क्रमांक हे फसवे असू शकतात.
- ईमेल्स व एसएमएस यामध्ये आलेल्या यूआरएल्सच्या व डोमेन नावांच्या स्पेलिंगमध्ये कोणतीही चूक आहे का ते तपासा. ऑनलाइन बँकिंगसाठी केवळ पडताळणी केलेल्या, सुरक्षित, आणि विश्वासार्ह वेबसाइट्सचा आणि ॲप्सचा वापर करा, म्हणजेच ''https'' ने सुरू होणाऱ्या वेबसाइट्स. संशयास्पद यूआरएलबाबत किंवा वेबसाइटबाबत लगेचच स्थानिक पोलिसांना/सायबरक्राइम शाखेला कळवायला हवे.

- तुम्ही न केलेल्या व्यवहारासाठी तुमच्या खात्यातून डेबिट करण्यासाठी तुम्हाला ओटीपी प्राप्त झाल्यास, लगेचच तुमच्या बँकेला/ई-वॉलेट प्रदात्याला त्याबाबत कळवा. तुम्ही न केलेल्या व्यवहारासाठी तुम्हाला डेबिटचा एसएमएस प्राप्त झाल्यास, लगेचच तुमच्या बँकेला/ई-वॉलेट प्रदात्याला कळवा आणि यूपीआयसह, डेबिटचे सर्व प्रकार अवरोधित करा. तुमच्या खात्यामध्ये कोणतेही फसवणुकीचे कृत्य होत असल्याची तुम्हाला शंका असल्यास, इंटरनेट/मोबाइल बँकिंगसाठी कार्यान्वित लाभार्थी यादीमधील समावेशाची तपासणी करा.
- तुमच्या बँकेशी/ई-वॉलेट खात्याशी जोडलेल्या तुमच्या ईमेलच्या पासवर्डची देवाणघेवाण करू नका. ई-कॉमर्स/सोशल मीडिया साइट्ससाठी आणि तुमच्या बँक खात्यासाठी आणि तुमच्या बँक खात्याशी जोडलेल्या ईमेलसाठी सामाईक पासवर्ड्स ठेवू नका. सार्वजनिक, खुल्या किंवा मोफत वाय-फायद्वारे किंवा इंटरनेट नेटवर्क्सद्वारे बँकिंग करणे टाळा.
- यूजर आयडीच्या स्वरुपात तुमच्या ईमेलसोबत कोणत्याही वेबसाइटची/ॲप्लिकेशनची नोंद करताना 'पासवर्ड' हा शब्द तुमचा ईमेल पासवर्ड म्हणून ठेवू नका. तुमचा ईमेल हाताळण्यासाठी वापरण्यात येणारा पासवर्ड, विशेषतः तुमच्या बँक खात्याशी जोडलेला, विशेष असायला हवा आणि त्याचा वापर केवळ ईमेल हाताळणीसाठी करावा आणि इतर कोणतीही वेबसाइट किंवा ॲप्लिकेशन हाताळणीसाठी करू नये.
- विदेशी वित्तप्रेषणे, कमिशन प्राप्त करणे, किंवा लॉटरी जिंकणे अशा कारणांसाठी तुमच्या वतीने आरबीआयकडे पैसे जमा करण्यात आल्याची सूचनेद्वारे स्वतःची दिशाभूल होऊ देऊ नका.
- तुमच्या वित्तीय सेवा प्रदात्याकडून येणाऱ्या अलर्ट्ससाठी नियमितपणे तुमचे ईमेल व फोन संदेश तपासा. तुमच्या खात्यामधील कोणत्याही अप्राधिकृत व्यवहाराबाबत ताबोडतोब तुमच्या बँकेला/एनबीएफसीला/सेवा प्रदात्याला कळवा, जेणेकरून पुढील नुकसान टाळण्यासाठी कार्ड, खाते, वॉलेट ब्लॉक करता येईल.
- तुमचे एटीएम, डेबिट व क्रेडिट काड्र्स सुरक्षित करा आणि व्यवहारासाठी दैनंदिन मर्यादा स्थापित करा. तुम्ही मर्यादादेखील स्थापित करू शकता आणि देशीय/आंतरराष्ट्रीय वापरासाठी कार्यान्वित/अकार्यान्वित करू शकता. याद्वारे फसवणुकीमुळे होणारे नुकसान मर्यादित होऊ शकते.