अनुलग्नक 7: ग्राहक जागरूकता - साइबर धमकियां और धोखाधड़ी

यह देखा गया है कि कुछ अनैतिक तत्व सोशल मीडिया तकनीक, मोबाइल फोन कॉल, इत्यादि सहित नवकल्पनाशील तौर-तरीकों से जनता के साथ धोखाधड़ी और उन्हें भ्रमित कर रहे हैं। इसे देखते हुए, डीसीबी बैंक जनता को आगाह करता है कि वे ऐसे छलपूर्ण संदेशों, अवैध कॉल्स, अज्ञात लिंकों, भ्रामक सूचनाओं, अनधिकृत QR कोड्स, इत्यादि से सावधान रहें जो उन्हें किसी भी रूप में रियायत पाने/बैंक एवं वित्तीय सेवा-प्रदाताओं से शीघ्र उत्तर दिलाने का वचन देते हों।

धोखेबाज लोग यूज़र आईडी, लॉगिन/ट्रांजैक्शन पासवर्ड, वन-टाइम पासवर्ड (OTP), डेबिट/क्रेडिट कार्ड के विवरण जैसे पिन, CVV, समाप्ति तिथि एवं अन्य व्यक्तिगत सूचनाओं जैसे गोपनीय विवरणों को पाने का प्रयास करते हैं।

- विशिंग - बैंक/गैर-बैंक ई-वॉलेट प्रोवाइडर्स/टेलिकॉम सेवाओं के नाम पर भेजे जाने वाले झूठे फोन कॉल्स जिनके माध्यम से ग्राहकों को के.वाई.सी. अपडेटिंग, एकाउंट या सिम कार्ड को अनब्लॉक करने, डेबिट की गई राशि को क्रेडिट करने के बहाने लुभाया जाता है।
- फिशिंग - ग्राहकों को इस धोखे में रखने के लिए किए गए जाली ईमेल्स और/या एसएमएस कि वह संदेश उनके बैंक/ई-वॉलेट प्रोवाइडर से आया है और उसमें गोपनीय सूचनाओं को हथियाने के लिए लिंक बने होते हैं।
- रीमोट ऍक्सेस - ग्राहकों को अपने मोबाइल फोन/कंप्यूटर पर किसी ऍप्लीकेशन को डाउनलोड करने का लालच देना जिसके माध्यम से ग्राहक की डिवाइस पर डेटा ऍक्सेस किए जा सकते हैं।
- धन प्राप्त करने के लिए ''अपना UPI पिन डालें'' जैसे संदेशों के माध्यम से भुगतान के नकली निवेदन करके यूपीआई की ''निवेदन संग्रह'' (collect request) विशेषता का दुरुपयोग करना।
- वेबपेज़ों/सोशल मीडिया पर बैंकों/ई-वॉलेट प्रोवाइडरों के झूठे सम्पर्क नम्बर जिन्हें सर्च इंजिन इत्यादि के माध्यम से दिखाया जाता है।

डीसीबी बैंक जनता से अपील करता है कि कोई भी डिज़िटल (ऑनलाइन/भुगतान) लेनदेन करते समय वे सभी समुचित सावधानियां बरतते सुरक्षित डिज़िटल बैंकिंग प्रथा का पालन करें। इससे आर्थिक और/या अन्य नुकसानों से बचने में सहायता मिलेगी।

सुरक्षित डिज़िटल बैंकिंग प्रथाएं

- अपने एकाउंट (खाता) सम्बंधी विवरण जैसे खाता संख्या, लॉगिन आईडी, पासवर्ड, पिन, यूपीआई-पिन, ओटीपी, एटीएम/डेबिट कार्ड/क्रेडिट कार्ड के विवरण इत्यादि किसी को न बताएं, यहां तक कि बैंक के अधिकारियों को भी नहीं चाहे वे कितने ही भरोसेमंद क्यों न प्रतीत हों।
- केवाईसी को अपडेट न करने के कारण आपके एकाउंट को ब्लॉक कर देने की धमकी तथा उन्हें अपडेट करने के लिए दिए गए लिंक पर क्लिक करने का सुझाव देना धोखेबाज़ों के काम करने का एक सामान्य तरीका है। केवाईसी को अपडेट/त्वरित करने सम्बंधी किसी भी प्रस्ताव का उत्तर न दें। हमेशा अपने बैंक/गैर-बैंकिंग वित्तीय कम्पनी/ई-वॉलेट प्रोवाइडर की आधिकारिक वेबसाइट में जाएं या शाखा से सम्पर्क करें।
- अपने फोन या डिवाइस पर कोई भी अनजान ऍप डाउनलोड न करें। ये ऍप चुपके से आपके गोपनीय डेटा को ऍक्सेस कर सकते हैं।
- धन प्राप्ति के लिए किए गए लेनदेन में बारकोड या QR कोड को स्कैन करने या MPIN डालने की जरूरत नहीं होती है। अतः यदि ऐसा करने के लिए कहा जाए तो सावधानी बरतें।
- सम्पर्क सम्बंधी विवरण जानने के लिए हमेशा बैंक/गैर-बैंकिंग वित्तीय कम्पनी/ई-वॉलेट प्रोवाइडर की आधिकारिक वेबसाइट में जाएं। इंटरनेट सर्च इंजिन्स में दिए गए सम्पर्क नम्बर कपटपूर्ण हो सकते हैं।
- ईमेल्स और एसएमएस में प्राप्त यूआरएल और डॉमेन नेम्स की स्पेलिंग सम्बंधी त्रुटियों की जांच कर लें। ऑनलाइन बैंकिंग के लिए केवल सत्यापित, सुरक्षित, और विश्वसनीय वेबसाइटों एवं ऍपों का प्रयोग करें, यानी उन वेबसाइटों का जो ''https'' से अरंभ होती हों। किसी भी संदिग्ध URL या वेबसाइट की जानकारी तुरन्त पुलिस/साइबर अपराध शाखा को दी जानी चाहिए।

● यदि आपको ऐसे किसी लेनदेन के बारे में जिसे आपने आरंभ नहीं किया था, खाते से रकम निकालने के लिए जद्धझ प्राप्त होता है तो अपने बैंक/ई-वॉलेट प्रोवाइडर को तुरन्त सूचित करें। यदि आपको किसी लेनदेन के बारे में डेबिट एसएमएस प्राप्त होता है जिसे आपने नहीं किया था तो अपने बैंक/ई-वॉलेट प्रोवाइडर को तुरन्त सूचित करें और UPI सहित हर प्रकार की डेबिट को ब्लॉक कर दें। यदि आपको अपने खाते में किसी भी कपटपूर्ण क्रियाकलाप का संदेह होता है तो उसे इंटरनेट/मोबाइल बैंकिंग के लिए सक्षमकृत हितग्राही सूची में शामिल करने की जाच करें।

● अपने बैंक/ईमेल वॉलेट खाते से लिंक किए गए अपने ईमेल का पासवर्ड किसी के साथ साझा न करें। ई-कॉमर्स/सोशल मीडिया साइटों और अपने बैंक खाते के लिए एक समान पासवर्डों का इस्तेमाल न करें। सार्वजनिक, ओपन या फ्री वाई-फाई या इंटरनेट नेटवर्क्स के माध्यम से बैंकिंग कार्य करने से बचें।

● किसी भी वेबसाइट/ऍप्लीकेशन में यूज़र आईडी के रूप में रजिस्टर करते समय ''पासवर्ड'' शब्द को अपने ईमेल का पासवर्ड न बनाएं। आपके ईमेल - खास तौर पर यदि वह आपके बैंक खाते से लिंक किया हुआ हो - को ऍक्सेस करने के लिए प्रयुक्त पासवर्ड अनूठा होना चाहिए और उसका उपयोग केवल ईमेल ऍक्सेस करने के लिए किया जाना चाहिए न कि अन्य किसी वेबसाइट या ऍप्लीकेशन को ऍक्सेस करने के लिए।

● विदेश से प्राप्त धनों, कमीशन की रसीद, या लॉटरी जीतने इत्यादि के लिए आपकी ओर से भारतीय रिज़र्व बैंक में धन जमा किए जाने सम्बंधी सूचनाओं से भ्रमित न हों।

● अपने वित्तीय सेवाप्रदाता से प्राप्त चेतावनियों (एलर्ट्स) के लिए नियमित रूप से अपने ईमेल और फोन संदेशों की जांच करते रहें। अपने खाते में किसी भी अनधिकृत लेनदेन के बारे में अपने बैंक/गैर-बैंकिंग वित्तीय कम्पनी/ई-वॉलेट प्रोवाइडर को तुरन्त सूचित करके कार्ड, एकाउंट, वॉलेट को ब्लॉक करने का निवेदन करें ताकि आगे और कोई नुकसान न हो।

● अपने एटीएम, डेबिट और क्रेडिट कार्डों को सुरक्षित रखें और लेनदेन के लिए एक दैनिक सीमा तय करें। आप घरेलू/अंतर्राष्ट्रीय उपयोग के लिए भी सीमाएं तय कर सकते हैं और उसे सक्रिय/निष्क्रिय कर सकते हैं। इससे धोखाधड़ी के कारण होने वाले नुकसानों को सीमित किया जा सकेगा।