सावधान रहें, जागरूक

BE(A)WARE

वित्तीय धोखेबाजों की कार्यप्रणाली पर बुकलेट

भारतीय रिज़र्व बैंक

विषय वस्तु

आमुख

हाल के वर्षों में भुगतान के डिजिटल साधनों/तरीकों के प्रयोग में काफी वृद्धि हुई है। इसने कोविद-19 के कारण लगे लॉकडाउन के दौरान और गति प्राप्त की है। इससे न केवल ग्राहकों की सुलभता बढ़ी है, अपितु वित्तीय समावेशन के राष्ट्रीय उद्देश्य को काफी हद तक हासिल करने में मददगार साबित हुआ है। जैसे ही वित्तीय लेनदेन करने में आसानी हुई, खुदरा वित्तीय लेनदेनों की धोखाधड़ी के मामलों में वृद्धि हुई। धोखेबाज आम/जनसाधारण एवं मासूम/भोले-भाले लोगों, के मेहनत से कमाए गए धन को ठगने/हड़पने के लिए नवीनतम तरीकों का उपयोग कर रहे हैं, खासकर नए लोगों/सहभागियों को जो टेक्नो – फाइनेंशियल इको सिस्टम से भलीभांति : परिचित नहीं हैं।

इस बुकलेट के संकलन में, इसका एकमात्र उद्देश्य वास्तविक मूल्य की यथासंभव व्यावहारिक जानकारी को इसमें समाहित करना है, विशेषत: उनके लिए जो वित्तीय लेनदेन में अनुभवहीन हैं। यह केवल विभिन्न स्त्रोतों से यादृच्छिक रूप से एकत्रित घटनाओं का संकलन मात्र नहीं है, अपितु बैंकिंग लोकपाल में प्राप्त विभिन्न प्रकार की शिकायतों का बहुत सावधानी से संकलित दस्तावेज़ है। यह बुकलेट धोखेबाज लोगों की कार्यप्रणाली के बारे में आमजन में जागरूकता लाने का एक प्रयास मात्र है, इसके अतिरिक्त वित्तीय लेनदेन के समय बरती जाने वाली सावधानियों के विषय में कुछ जानकारी भी प्रदान करती है। यह बुकलेट व्यक्तिगत जानकारी को सुरक्षित, अनजान कॉल / ईमेल मैसेज से सावधान रहने, वित्तीय लेनदेन करते समय समुचित सावधानी रखने, समय – समय पर सुरक्षित निजी जानकारी / पासवर्ड को बदलने पर ज़ोर देती है। इस प्रकार इसका शीर्षक अंग्रेजी में BE(A)WARE है इसीलिए हिन्दी में इसे कहा जा सकता है – सावधान रहें और जागरूक बने।

यह बुकलेट उपभोक्ता शिक्षण और संरक्षण विभाग, भारतीय रिज़र्व बैंक की जन जागरूकता पहल का एक भाग है। इसकी परिकल्पना लोकपाल, मुंबई II के कार्यालय द्वारा की गई है।

धोखाधड़ीपूर्ण लेनदेन की कार्यप्रणाली और उसके विरुद्ध बरती जाने वाली सावधानियाँ - बैंक

1. फिशिंग संबंधी लिंक

कार्यप्रणाली

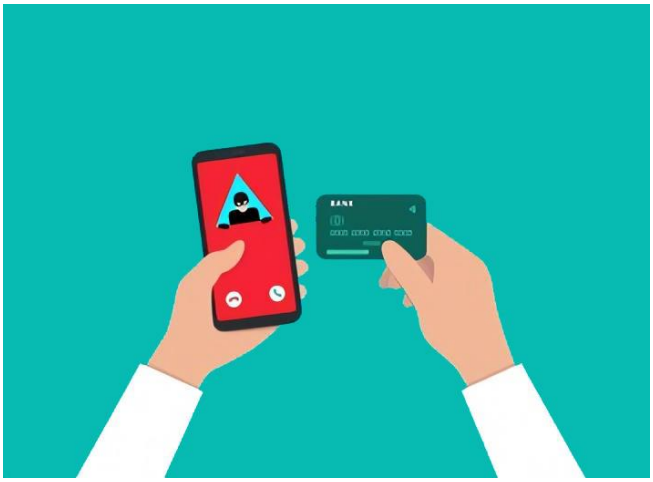
- धोखेबाज एक तृतीय पक्षकार (थर्ड पार्टी) वेबसाइट बनाते हैं, जो कि वास्तविक वेबसाइट्स की तरह ही प्रतीत होती है, जैसे कि बैंक की वेबसाइट्स या ई-कॉमर्स वेबसाइट्स या सर्च इंजन इत्यादि।
- धोखेबाजों द्वारा सामान्यत: ये लिंक एसएमएस / सोशल मीडिया / ईमेल / इंसटेंट मैसेजिंग आदि के द्वारा भेजे जाते हैं।
- अधिकांश समय, ग्राहक विस्तृत यूआरएल को जाँचे बिना, सिर्फ एक नजर डालकर और लिंक को क्लिक करके सुरक्षित निजी जानकारी जैसे व्यक्तिगत पहचान संख्या (पिन), वन टाइम पासवर्ड (ओटीपी), पासवर्ड आदि प्रविष्ट करते हैं, जिसे धोखेबाजों द्वारा कैप्चर कर उपयोग किया जाता है।

- यह लिंक वेबसाइटों के प्रमाणिक दिखने वाले नामों जैसे दिखाई देतें हैं, किंतु , वास्तव में, ग्राहक फिशिंग वेबसाइट्स की ओर पुनर्निर्देशित (रिडायरेक्ट) हो जाता है।
- जब ग्राहक इन वेबसाइट्स पर अपनी सुरक्षित निजी जानकारी डालते हैं, तो उसको हथिया लिया जाता है और धोखेबाजों द्वारा प्रयोग में लाया जाता है।

सावधानियाँ

- ✓ अनजान लिंक को क्लिक नहीं करना चाहिए तथा एसएमएस / ईमेल को तत्काल ही डिलीट कर देना चाहिए ताकि भविष्य में उस तक पहुँच से बचा जा सके।
- ✓ बैंक/ई-कॉमर्स/सर्च इंजन वेबसाइट का लिंक प्रदान करने वाली मेल को अनसब्सक्राइब करें और इस प्रकार के ई-मेल को डिलीट करने से पूर्व प्रेषक की ई-मेल आईडी को ब्लॉक कर दें।
- ✓ हमेशा अपने बैंक/सेवा प्रदाता की आधिकारिक वेबसाइट पर जाएँ। वेबसाइट्स डिटेल्स के सत्यापन के समय सावधानी बरतनी चाहिए, विशेषत: जब निजी वित्तीय जानकारी प्रविष्ट करनी हो। सुरक्षित निजी जानकारी प्रविष्ट करने से पूर्व वेबसाइट पर सुरक्षित चिन्ह (पैडलॉक चिन्ह के साथ https) की जांच करें।
- ✓ वर्तनी संबंधी त्रुटियों के लिए ई-मेल में प्राप्त यूआरएल और डोमेन नामों की जांच करें। संदेह होने पर सूचित करें।

2. टेलीफोन पर छद्म कॉल (विशिंग)



कार्यप्रणाली

- बहुरूपिए व्यक्ति बैंकर्स / कंपनी कार्यपालक / बीमा एजेंट / सरकारी अधिकारी इत्यादि के रूप में ग्राहक से टेलीफोन कॉल / सोशल मीडिया / के माध्यम से संपर्क करते हैं और विश्वास कायम करने के लिए नाम या जन्म तिथि जैसे कुछ विवरण साझा करते हुए सुरक्षित जानकारी की पुष्टि कराते हैं।

- कुछ कुछ मामलों में, बहुरूपिए व्यक्ति लेनदेन को ब्लॉक करने के लिए, दंड को रोकने हेतु भुगतान बाबत, आकर्षक छूट प्राप्त करने इत्यादि हेतु आकस्मिकता बताकर ग्राहक को अत्यावश्यक / तत्काल निजी जानकारी जैसे पासवर्ड/ओटीपी/पिन/सीवीवी आदि साझा करने के लिए दबाव डालते हैं / चाल में फँसाते हैं। बाद में ये निजी जानकारियाँ धोखेबाजों द्वारा ग्राहक के साथ छल करने के लिए प्रयुक्त होती हैं।

सावधानियाँ

- ✓ बैंक अधिकारी / वित्तीय संस्थाएं / कोई अन्य वास्तविक संस्था ग्राहक से गोपनीय जानकारी जैसे यूज़रनेम / पासवर्ड / कार्ड विवरण / सीवीवी / ओटीपी इत्यादि साझा करने के लिए कभी नहीं कहते।
- ✓ ऐसी गोपनीय जानकारी किसी के साथ साझा न करें। यहाँ तक कि आपके अपने परिवार के सदस्यों और मित्रों के साथ भी नहीं।

3. ऑनलाइन बिक्री प्लेटफॉर्म के प्रयोग से धोखाधड़ी

कार्यप्रणाली

- धोखेबाज ऑनलाइन बिक्री प्लेटफॉर्म पर खरीददार होने का दिखावा करते हैं और विक्रेता के उत्पाद/उत्पादों में रुचि दिखाते हैं।
- विक्रेता को धन का भुगतान करने के बजाए, वे यूपीआई ऐप के माध्यम से "धन अनुरोध"(Request money) विकल्प का प्रयोग करते हैं और यूपीआई पिन दर्ज कर अनुरोध को अनुमोदित करने का दबाव बनाते हैं। जैसे ही विक्रेता पिन दर्ज करता है धन धोखेबाज के खाते में अंतरित हो जाता है।

सावधानियाँ

- ✓ जब आप ऑनलाइन बिक्री प्लेटफार्मों का उपयोग करके उत्पादों को खरीद या बेच रहे हों तो हमेशा सावधान रहें।
- ✓ हमेशा याद रखें, धन प्राप्त करने के लिए कहीं भी अपना पिन / पासवर्ड डालने की आवश्यकता नहीं होती है। यदि यूपीआई या कोई अन्य ऐप आपसे लेनदेन पूरा करने के लिए आपका पिन डालने के लिए निर्देश देते हैं, तो इसका मतलब है कि आप धन प्राप्त करने की जगह धन भेजने की ओर अग्रसर हो रहे हैं।

4. अनजान / गैर सत्यापित मोबाइल ऐप्स के कारण धोखाधड़ी

कार्यप्रणाली

- धोखेबाज द्वारा एसएमएस/सोशल मीडिया / इंसटेंट मेसेंजर इत्यादि के माध्यम से कुछ लिंक साझा किए जाते हैं, ये लिंक अधिकृत संस्थाओं के मौजूदा ऐप जैसे ही दिखते हैं।
- धोखेबाज ग्राहक को ऐसे लिंक पर क्लिक करने की चाल चलता है जिसके परिणामस्वरूप ग्राहक के मोबाइल/लैपटॉप/डेस्कटॉप, आदि पर अज्ञात/असत्यापित ऐप्स डाउनलोड होते हैं।
- एक बार दुर्भावनापूर्ण एप्लिकेशन डाउनलोड होने के बाद धोखेबाज ग्राहक के डिवाइस तक पूर्ण पहुंच प्राप्त करता है। इसमें डिवाइस पर संग्रहित गोपनीय जानकारी और ऐप इंस्टॉल करने से पहले/बाद में प्राप्त संदेश/ओटीपी शामिल हैं।

डाउनलोड !! डाउनलोड !!

सावधानियाँ

- ✓ अनजान / गैर सत्यापित स्त्रोतों या अनजान व्यक्ति के कहने/बताने से कभी भी एप्लिकेशन डाउनलोड डाउनलोड नहीं करें।
- ✓ डाउनलोड करने से पहले एक विवेकपूर्ण अभ्यास के रूप में डाउनलोड किए जा रहे ऐप के प्रकाशकों/मालिकों के साथ-साथ इसकी उपयोगकर्ता रेटिंग आदि की जाँच करें।
- ✓ किसी एप्लिकेशन को डाउनलोड करते समय उसके द्वारा अपेक्षित अनुमति/आपके डेटा तक पहुँच जैसे संपर्क, फोटो आदि का एक्सेस की जाँच करें। केवल वही अनुमति प्रदान करें जो वांछित एप्लिकेशन का उपयोग करने के लिए बिल्कुल आवश्यक हैं।

5. एटीएम कार्ड स्किमिंग (डाटा चोरी करने की डिवाइस)

कार्यप्रणाली

- धोखेबाज एटीएम मशीन में स्किमिंग डिवाइस (डाटा चोरी करने की डिवाइस) इंसटॉल करते हैं और आपके कार्ड से डाटा चोरी करते हैं।
- धोखेबाज एटीएम पिन कैप्चर करने के लिए नकली दिखावटी की-बोर्ड , साधारण नज़र से दिखाई न देने वाला अति सूक्ष्म कैमरा भी लगा सकते हैं।
- कभी - कभार, धोखेबाज अन्य ग्राहक का बहाना करके आपके पास में खड़े हो जाते हैं तथा जब आप पिन प्रविष्ट करते हैं, तो वे आपके पिन तक पहुँच प्राप्त कर लेते हैं।
- यह डेटा बाद में नकली कार्ड बनाने के लिए प्रयुक्त होता है एवं ग्राहक के खाते से राशि निकाल ली जाती है।

सावधानियाँ

- ✓ लेनदेन करते समय इस बात की जाँच करें कि कार्ड प्रविष्ट करने के स्लॉट के पास या एटीएम मशीन के की - पैड में कोई अतिरिक्त उपकरण नहीं लगा हुआ है।
- ✓ अपना पिन डालते समय की-पैड को अपने हाथ से कवर करें/ढँक लें।
- ✓ अपने एटीएम कार्ड पर पिन कभी न लिखें।
- ✓ जब आपके एकदम पास में कोई अन्य/अनजान व्यक्ति खड़ा हो, तो उसकी उपस्थिति में अपना पिन नहीं डालें।
- ✓ नकदी निकालने के लिए अपना एटीएम कार्ड किसी को न दें।
- ✓ किसी भी अज्ञात व्यक्ति द्वारा दिए गए निर्देशों का पालन न करें या एटीएम पर अजनबियों/अज्ञात व्यक्तियों से सहायता/मार्गदर्शन न लें।
- ✓ यदि एटीएम से नकदी नहीं निकल रही है, तो, 'रद्द करें' (केंसिल) बटन दबाएं और एटीएम से बाहर निकलने से पहले होम स्क्रीन के प्रदर्शित होने की प्रतीक्षा करें।

6. स्क्रीन शेयरिंग ऐप/रिमोट एक्सेस के प्रयोग से धोखाधड़ी

कार्यप्रणाली

- धोखेबाज ग्राहक को स्क्रीन शेयरिंग ऐप्स डाउनलोड करने के लिए आपको युक्ति सुझाएंगे।
- इस प्रकार के ऐप का उपयोग करके, धोखेबाज ग्राहक के मोबाइल/लैपटॉप को देख/नियंत्रित कर सकते हैं और ग्राहक की वित्तीय जानकारी तक पहुँच प्राप्त कर सकते हैं।
- धोखेबाज इस जानकारी का उपयोग धन के अनधिकृत हस्तांतरण या ग्राहक की इंटरनेट बैंकिंग / भुगतान ऐप्स का उपयोग करके भुगतान करने के लिए करते हैं।

सावधानियाँ

- ✓ यदि आपके उपकरण में कोई तकनीकी गड़बड़ी होती है और आपको कोई स्क्रीन शेयरिंग ऐप डाउनलोड करने की आवश्यकता होती है, तो अपने उपकरण से भुगतान संबंधी सभी ऐप निष्क्रिय/लॉग आउट करें।
- ✓ ऐसे ऐप तभी डाउनलोड करें जब कंपनी की आधिकारिक वेबसाइट पर प्रदर्शित हो रहे कंपनी के आधिकारिक टोल-फ्री नंबर के माध्यम से आपको सलाह दी जाए। यदि कंपनी का कोई कार्यकारी अपने व्यक्तिगत संपर्क नंबर के माध्यम से आपसे संपर्क करता है तो ऐसे ऐप डाऊनलोड न करें।
- ✓ जैसे ही काम पूरा हो जाए, यह सुनिश्चित करें कि स्क्रीन शेयरिंग ऐप आपके उपकरण से हटा दिया गया है।

7. सिम अदला - बदली / नकली सिम बनाना (सिम क्लोनिंग)

कार्यप्रणाली

- धोखेबाज ग्राहक के सब्सक्राइबर आइडेंटिटी माड्यूल (सिम) कार्ड तक पहुँच प्राप्त करते हैं या ग्राहक के बैंक खाते से जुड़े पंजीकृत मोबाइल नंबर का डुप्लीकेट सिम कार्ड (इलेक्ट्रॉनिक-सिम सहित) प्राप्त कर सकते हैं।
- धोखेबाज ऐसे नकली सिम कार्ड पर प्राप्त ओटीपी का प्रयोग अनधिकृत लेनदेन के लिए करते हैं।
- धोखेबाज सामान्यत: स्वयं को टेलीफोन / मोबाइल नेटवर्क स्टाफ के रूप में प्रस्तुत करते हुए ग्राहक को फोन करते हैं तथा सिम कार्ड को 3जी से 4जी में अपग्रेड करने या सिम कार्ड पर अतिरिक्त लाभ प्रदान करने हेतु जानकारी का अनुरोध करते हैं।

सावधानियाँ

- ✓ सिम कार्ड से संबंधित जानकारी कभी साझा नहीं करें।
- ✓ अपने फोन में मोबाइल नेटवर्क एक्सेस के बारे में सतर्क रहें। यदि सामान्य हालात में काफी समय तक आपके मोबाइल में नेटवर्क नहीं है, तो आप यह सुनिश्चित करने के लिए तुरंत मोबाइल ऑपरेटर से संपर्क करें कि आपके मोबाइल नंबर के लिए कोई डुप्लीकेट सिम जारी नहीं किया जा रहा है/जारी किया गया है ।

8. सर्च इंजन के माध्यम से प्राप्त परिणामों के आधार पर क्रेडेंशियल (निजी जानकारी) से छेड़छाड़ करके धोखाधड़ी कार्यप्रणाली

- ग्राहक अपने बैंक, बीमा कंपनी, आधार अपडेशन सेंटर इत्यादि की संपर्क जानकारी/कस्टमर केयर नंबरप्राप्त करने हेतु सर्च इंजन का प्रयोग करते हैं। सर्च इंजन पर मौजूद ये विवरण अक्सर संबंधित संस्था से संबंधित नहीं हैं, लेकिन धोखेबाजों द्वारा इस रूप में प्रदर्शित किए जाते हैं।
- ग्राहक सर्च इंजन पर बैंक/कंपनी के संपर्क नंबर के रूप में प्रदर्शित धोखेबाजों के अज्ञात/गैर सत्यापित संपर्क नंबर से संपर्क कर बैठते हैं।
- जब ग्राहक इन संपर्क नंबरों पर कॉल करते हैं, तो बहुरूपिए ग्राहकों से सत्यापन के लिए उनके कार्ड के ब्योरे / विवरण मांगते हैं।
- धोखेबाज को विनियमित संस्था (आरई) का वास्तविक प्रतिनिधि मानते हुए, लोग अपनी सभी सुरक्षित जानकारियाँ साझा कर लेते हैं एवं इस प्रकार धोखे का शिकार होते हैं।

सावधानियाँ

- ✓ कस्टमर केयर का संपर्क विवरण हमेशा बैंक/कंपनियों की आधिकारिक वेबसाइट से प्राप्त करें।
- ✓ सर्च इंजन परिणाम पृष्ठ पर प्रदर्शित होने वाले नंबरों पर सीधे कॉल न करें क्योंकि ये अक्सर धोखेबाजों के छद्म आवरण में रहते हैं।
- ✓ यह भी ध्यान रखें कि कस्टमर केयर नंबर कभी भी मोबाइल नंबर के रूप में नहीं होते हैं।

9. क्यूआर कोड स्कैन के द्वारा घोटाला

कार्यप्रणाली

- धोखेबाज अक्सर विभिन्न प्रकार के बहानों के साथ ग्राहकों से संपर्क करते हैं एवं ग्राहकों के फोन पर ऐप्स का उपयोग करके त्वरित प्रतिक्रिया (क्यूआर)कोड स्कैन करने के लिए उन्हें धोखा देते हैं।
- ऐसे क्यूआर कोड को स्कैन करके ग्राहक अनजाने में धोखेबाजों को अपने खाते से पैसे निकालने के लिए अधिकृत कर सकते हैं।

सावधानियाँ

- ✓ भुगतान ऐप्स के माध्यम से कोई भी क्यूआर कोड स्कैन करते समय सावधानी बरतें। क्यूआर कोड में किसी विशिष्ट खाते में राशि अंतरित करने हेतु खाता विवरण अंतर्निहित होता है।
- ✓ पैसे प्राप्त करने के लिए कभी भी किसी भी क्यूआर कोड को स्कैन नहीं करें। पैसे की प्राप्ति से जुडे लेन-देन में बारकोड/क्यूआर कोड को स्कैन करने या मोबाइल बैंकिंग पिन (एम-पिन), पासवर्ड आदि दर्ज करने की आवश्यकता नहीं होती है।

10. सोशल मीडिया के माध्यम से नकली पहचान धारण करना

कार्यप्रणाली

- धोखेबाज सोशल मीडिया प्लेटफार्मों जैसे फेसबुक व इंस्टाग्राम आदि के उपयोगकर्ताओं के विवरण का उपयोग करके जाली अकाउंट बनाते हैं।
- फिर धोखेबाज उपयोगकर्ताओं के मित्रों को अत्यावश्यक मेडिकल उद्देश्यों,भुगतानों इत्यादि के लिए धन हेतु अनुरोध भेजते हैं।
- धोखेबाज नकली विवरण का उपयोग करते हुए उपयोगकर्ताओं से संपर्क भी करते हैं और एक समय के बाद विश्वास हासिल कर लेते हैं। जब उपयोगकर्ता अपनी व्यक्तिगत या निजी जानकारी साझा करते हैं तो धोखेबाज ऐसी जानकारी का उपयोग उपयोगकर्ताओं को ब्लैकमेल करने या जबरन वसूली के लिए करते हैं।

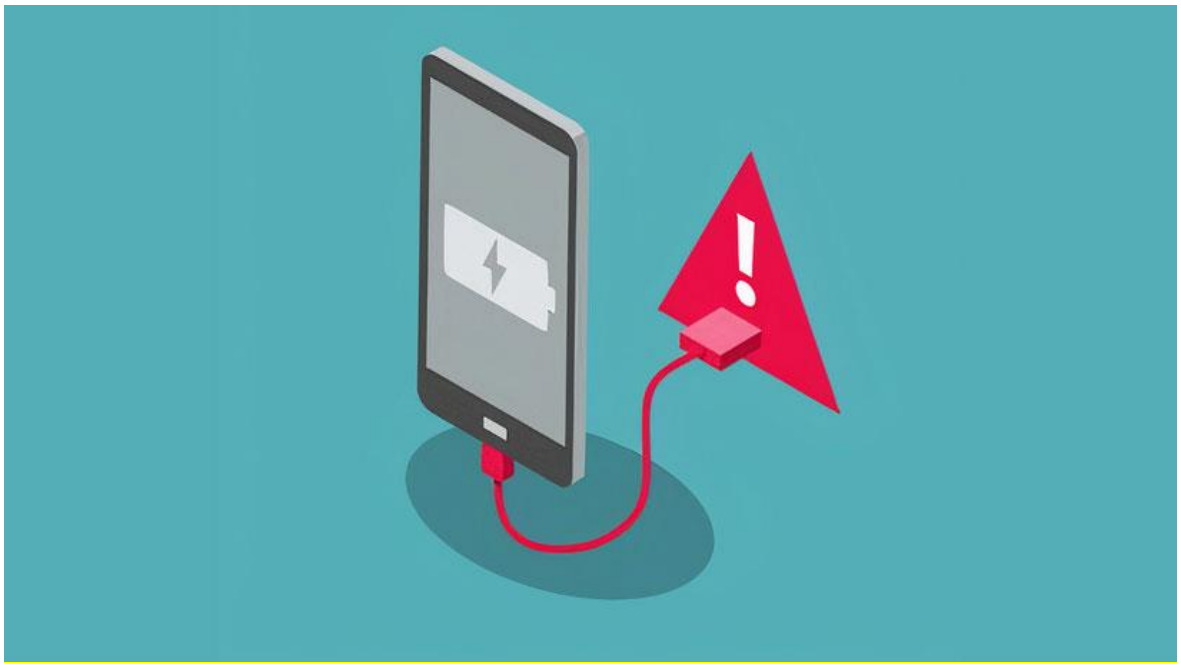
सावधानियाँ

- ✓ मित्र / संबंधी से प्राप्त धन आदि के अनुरोध की वास्तविकता को सत्यापित करने के लिए हमेशा फोन कॉल या भौतिक मीटिंग के माध्यम से पुष्टि करें ताकि यह पुष्ट हो सके कि प्रोफाइल नकली नहीं है।
- ✓ अनजान व्यक्तियों को ऑनलाइन भुगतान न करें।
- ✓ सोशल मीडिया प्लेटफार्म्स पर निजी एवं गुप्त जानकारी साझा न करें।

11. ज्यूस जैकिंग (चार्जिंग पोर्ट के माध्यम से साइबर क्राइम)

कार्यप्रणाली

- मोबाइल मोबाइल का चारजिंग पोर्ट, फाइल / डाटा ट्रांसफर करने के लिए भी प्रयुक्त हो सकता है।
- धोखेबाज सार्वजनिक चार्जिंग पोर्ट का उपयोग वहाँ से जुड़े ग्राहक के फोन में मैलवेयर स्थानांतरित करने के लिए करते हैं और ग्राहकों के मोबाइल फोन (ज्यूस जैकिंग) के , संवेदनशील डेटा जैसे ईमेल,एसएमएस, सहजे गए पासवर्ड्स आदि को नियंत्रित /एक्सेस/ चोरी करते हैं। हैं।



सावधानियाँ

- ✓ हमेशा पब्लिक / अनजान चार्जिंग पॉर्ट्स / कैबल्स का प्रयोग करने से बचें।

12. लॉटरी धोखाधड़ी

कार्यप्रणाली

- धोखेबाज ईमेल भेजते हैं / फोन करते हैं कि ग्राहक ने एक बहुत बड़ी लॉटरी जीती है। यद्यपि, धन प्राप्त करने के लिए धोखेबाज ग्राहकों से अपने बैंक खाते/क्रेडिट कार्ड का विवरण वेबसाइट पर दर्ज करके अपनी पहचान की पुष्टि करने के लिए कहते हैं, जहां से धोखाधड़ी करने वालों द्वारा डेटा कैप्चर किया जाता है।
- धोखेबाज लॉटरी / उत्पाद प्राप्त करने हेतु ग्राहकों को कर/विदेशी मुद्रा प्रभार/अग्रिम भुगतान या शिपिंग प्रभार, प्रोसेसिंग / संचालन शुल्क इत्यादि का भुगतान करने के लिए भी कहते हैं।
- कुछ मामलों में धोखेबाज आरबीआई या विदेशी बैंक/कंपनी/अंतरराष्ट्रीय वित्तीय संस्थान के प्रतिनिधि के रूप में भी पेश आ सकते हैं और उस संस्था से विदेशी मुद्रा में बड़ी राशि प्राप्त करने के लिए ग्राहक को अपेक्षाकृत कम राशि अंतरित करने के लिए कह सकते हैं।
- चूंकि, अनुरोधित धन आम तौर पर वादा किए गए लॉटरी/पुरस्कार का बहुत कम प्रतिशत होता है, ग्राहक धोखेबाज के जाल में फंस सकता है और भुगतान कर सकता है।

सावधानियाँ

- ✓ ऐसी अविश्वसनीय लॉटरी या प्रस्तावों से सावधान रहें। कोई भी मुफ्त पैसा नहीं डेटा है, विशेष रूप से इतनी बड़ी मात्रा में।
- ✓ किसी भी लॉटरी कॉल/ई-मेल के उत्तर में भुगतान न करें या सुरक्षित जानकारी साझा न करें।
- ✓ आरबीआई कभी भी जन सामान्य के खाते नहीं खोलता है या उनसे जमा राशियाँ स्वीकार नहीं करता है। इस प्रकार के संदेश धोखाधड़ी वाले होते हैं।
- ✓ आरबीआई कभी भी लोगों के व्यक्तिगत/बैंक विवरण की मांग नहीं करता है। नकली आरबीआई लोगो और संदेशों से सावधान रहें।
- ✓ बैंकों, संस्थानों आदि से पुरस्कार राशि प्राप्त हेतु पुरस्कार राशि, सरकारी सहायता और अपने ग्राहक को जाने (केवाईसी) अपडेशन की पेशकश/वादा करने वाले संदेशों का कभी भी जवाब न दें।

13. ऑनलाइन जॉब धोखाधड़ी

कार्यप्रणाली

- धोखेबाज नौकरी ढूंढने वाली जाली वेबसाइट बनाते हैं और जब नौकरी चाहने वाले पंजीकरण के दौरान इन वेबसाइट्स पर अपने बैंक खाते / डेबिट कार्ड / क्रेडिट कार्ड की सुरक्षित निजी जानकारी साझा करते हैं, तब खाते में सेंध लगा दी जाती है। (उनके खाते से छेड़छाड़ हो जाती है)
- धोखेबाज स्वयं को प्रतिष्ठित कंपनी(कंपनियों) के अधिकारियों के तौर पर प्रस्तुत करते हैं और जाली साक्षात्कार के पश्चात रोजगार की पेशकश करते हैं। फिर नौकरी चाहने वाले को पंजीकरण, अनिवार्य प्रशिक्षण कार्यक्रम, लैपटॉप इत्यादि के लिए धन अंतरित करने हेतु उकसाया जाता है।

सावधानियाँ

- ✓ विदेशी संस्थानों से प्राप्त प्रस्तावों सहित किसी भी नौकरी के प्रस्ताव के लिए सर्वप्रथम रोजगार कंपनी/उसके प्रतिनिधि की पहचान और संपर्क विवरण की पुष्टि करें।
- ✓ हमेशा याद रखें कि एक वास्तविक कंपनी, जो नौकरी दे रही है, कभी भी धन की मांग नहीं करेगी।
- ✓ अनजान जॉब सर्च वेबसाइट पर भुगतान नहीं करें।

14. मनी म्यूल

कार्यप्रणाली

- मनी म्यूल एक ऐसा शब्द है जिसका प्रयोग उन निर्दोष पीड़ितों का वर्णन करने के लिए किया जाता है, जिन्हें धोखेबाजों द्वारा उनके बैंक खाते/खातों के माध्यम से चोरी/अवैध धन को वैध बनाने हेतु धोखा दिया जाता है।
- धोखेबाज ई-मेल, सोशल मीडिया आदि के माध्यम से ग्राहकों से संपर्क करते हैं और उन्हें आकर्षक कमीशन के बदले में अपने बैंक खातों (मनी म्यूल) में धन प्राप्त करने हेतु रजामंद करते हैं।
- मनी म्यूल को फिर दूसरे मनी म्यूल के खाते में पैसा अंतरित करनेके लिए निर्देशित किया जाता है। इस प्रकार एक श्रृंखला प्रारम्भ होती है जिसके परिणामस्वरूप अंतत: धोखेबाज के खाते में पैसा अंतरित हो जाता है।
- वैकल्पिक रूप से, धोखेबाज मनी म्यूल को नकदी निकालने और इसे किसी को सौंपने हेतु निर्देशित कर सकता है।
- जब इस प्रकार की धोखाधड़ी रिपोर्ट की जाती है तो मनी लॉन्ड्रिंग के लिए मनी म्यूल पुलिस जांच का लक्ष्य बन जाता है।

सावधानियाँ

- ✓ किसी शुल्क/भुगतान के एवज में धन प्राप्त करने या अंतरित करने हेतु दूसरों को अपने खाते का उपयोग करने की अनुमति न दें।
- ✓ आपके बैंक खाते का विवरण मांगने वाले ई-मेल का जवाब न दें।
- ✓ आकर्षक प्रस्तावों /कमीशन के बहकावे में न आएं और आकर्षक शुल्क के एवज में अधिकृत धन प्राप्त करने और उसे दूसरों को अंतरित करने के लिए सहमति या धन की नकद निकासी कर दूसरों को न दें।
- ✓ यदि धन का स्त्रोत वास्तविक नहीं है या अंतर्निहित लेन-देन का औचित्य अधिकारियों के साने साबित नहीं होता है तो धन प्राप्त करने वाला पुलिस और अन्य विधि प्रवर्तन एजेंसियों के समक्ष गंभीर संकट में पड़ सकता है।

गैर बैंकिंग वित्तीय कंपनियों में कपटपूर्ण लेनदेन की कार्य प्रणाली और बरती जाने वाली सावधानियाँ

1. धोखेबाजों द्वारा ऋण प्रदान करने के लिए जाली विज्ञापन

- धोखेबाज अत्यंत आकर्षित कम ब्याज दरों या आसान पुनर्भुगतान तरीकों या बिना किसी प्रतिभूति की आवश्यकता इत्यादि पर पर्सनल लोन प्रदान करने का जाली विज्ञापन जारी करते हैं।
- धोखेबाज ऐसे प्रस्तावों वाले ई-मेल भेजते हैं एवं ग्राहकों से उनसे संपर्क करने के लिए कहते हैं।
- भोले-भाले ग्राहकों की साख हासिल करने तथा विश्वास हासिल करने के लिए, ये ई मेल आईडी, सु-ज्ञात / वास्तविक गैर बैंकिंग वित्तीय कंपनियों के वरिष्ठ अधिकारियों की ईमेल आईडी की तरह बनाया जाता है।
- जब ग्राहक लोन लेने के लिए धोखेबाज से संपर्क करते हैं, तो धोखेबाज विभिन्न प्रकार के पूर्व शुल्क यथा प्रोसेसिंग फीस, वस्तु और सेवा कर(जीएसटी), अन्तर नगर प्रशुल्क, अग्रिम ईएमआई, इत्यादि लेते हैं और ऋण संवितरित किए बिना भाग जाते हैं।
- धोखेबाज सर्च इंजन पर दर्शाने के लिए जाली वेबसाइट्स लिंक भी बनाते हैं, जिन्हें लोग लोन इत्यादि की तलाश में खोजते हैं।

सावधानियाँ

- ✓ बैंक / गैर बैंकिंग वित्तीय कंपनियाँ द्वारा प्रभारित ऋण प्रोसेसिंग शुल्क ऋण राशि में से काटा जाता है और उधारकर्ता से नकद में अग्रिम शुल्क की मांग नहीं की जाती है।
- ✓ कभी भी किसी भी प्रोसेसिंग शुल्क का अग्रिम भुगतान न करें क्योंकि गैर बैंकिंग वित्तीय कंपनियाँ / बैंक ऋण आवेदन की प्रोसेसिंग के पहले कभी भी अग्रिम शुल्क की मांग नहीं करते।
- ✓ कम ब्याज दरों इत्यादि पर ऑनलाइन ऋण प्रस्ताव पर वास्तविक स्त्रोत से विवरण जाँचे बगैर भुगतान नहीं करें या अपनी सुरक्षित निजी जानकारी प्रविष्ट नहीं करें।

2. एसएमएस / ईमेल / इंस्टेंट मैसेजिंग / कॉल स्कैम

- धोखेबाज आकर्षक ऋणों की उपलब्धता के संबंध में इंस्टेंट मैसेजिंग ऐप /एसएमएस/सोशल मीडिया के माध्यम से फर्जी संदेश प्रसारित करते हैं और विश्वसनीयता बढ़ाने के लिए उनके द्वारा साझा किए गए मोबाइल नंबर के प्रोफाइल पिक्चर के रूप में किसी भी ज्ञात एनबीएफसी के लोगो का उपयोग करते हैं।
- धोखेबाज अपना आधार कार्ड/पैन कार्ड और नकली एनबीएफसी पहचान पत्र (आईडी कार्ड) भी साझा कर लेते हैं।
- ऋण चाहने वालों को ऐसे बल्क संदेश/एसएमएस/ईमेल भेजने के बाद, धोखेबाज यादृच्छिक लोगों को कॉल करते हैं और नकली मंजूरी पत्र, नकली चेक की प्रतियां, आदि साझा करते हैं, और विभिन्न शुल्कों की मांग करते हैं। यदि एक बार ग्राहक इन शुल्कों का भुगतान कर देते हैं, तो जालसाज पैसे लेकर फरार हो जाते हैं ।

सावधानियाँ

- ✓ एसएमएस/ईमेल के माध्यम से भेजे गए लिंक पर कभी भी क्लिक न करें या विज्ञापन संबंधी ऐसे एसएमएस/ईमेल का जवाब न दें।
- ✓ संदिग्ध अटैचमेंट या फ़िशिंग लिंक भेजने वाले अज्ञात स्रोतों के ईमेल को कभी भी न खोलें/उनका जवाब न दें।
- ✓ कभी भी लोगों द्वारा टेलीफोन/ईमेल आदि के माध्यम से दिए गए ऋण प्रस्तावों पर विश्वास न करें।
- ✓ इस तरह के प्रस्तावों के लिए कभी भी कोई भुगतान न करें अथवा ऐसे प्रस्तावों के लिए किसी भी व्यक्तिगत / वित्तीय जानकारी को अन्य स्रोतों के माध्यम से उसके वास्तविक होने के के बारे में क्रॉस-चेक किए बिना साझा न करें।

3. ओटीपी आधारित धोखाधड़ी

कार्यप्रणाली

- धोखेबाज एनबीएफसी के रूप में प्रतिरूपण करते हैं और एनबीएफसी / बैंक ग्राहकों को ऋण देने या ऋण खातों पर क्रेडिट सीमा में वृद्धि की पेशकश करने वाले एसएमएस / संदेश भेजते हैं, और ग्राहकों को मोबाइल नंबर पर उनसे संपर्क करने के लिए कहते हैं।

- जब ग्राहक उक्त नंबर पर कॉल करते हैं, तो धोखेबाज उनसे वित्तीय विवरण वाले कुछ फॉर्म भरने के लिए कहते हैं। इसके बाद धोखेबाज उन्हें ओटीपी या पिन विवरण साझा करने के लिए भी उकसाते / मनाते हैं और ग्राहक के खाते से अनधिकृत अंतरण करते हैं।

सावधानियाँ

- ✓ अपने मित्रों और परिवार के सदस्यों सहित किसी के भी साथ किसी भी रूप में ओटीपी / पिन / व्यक्तिगत विवरण आदि को कभी भी साझा न करें।
- ✓ आपकी जानकारी के बिना कोई ओटीपी जनरेट नहीं हुआ है, यह सुनिश्चित करने के लिए नियमित रूप से अपने एसएमएस / ईमेल की जांच करें।
- ✓ बैंक / एनबीएफसी / ई-वॉलेट प्रदाता की सेवाओं का लाभ उठाने और / या उत्पाद और सेवाओं से संबंधित जानकारी और स्पष्टीकरण प्राप्त करने के लिए हमेशा उनकी आधिकारिक वेबसाइट को एक्सेस करें या शाखा से संपर्क करें।

4. नकली (फर्जी) ऋण वेबसाइट / ऐप धोखाधड़ी (फ्रॉड) कार्यप्रणाली

- धोखेबाज फर्जी ऋण ऐप बनाते हैं, जो तत्काल और अल्पकालिक ऋण प्रदान करते हैं। ये ऐप उधारकर्ताओं को ठगते हैं और काफी अधिक दर पर ब्याज भी वसूल सकते हैं।

  भोले-भाले ग्राहकों को आकर्षित करने के लिए, ये धोखेबाज "सीमित अवधि ऑफ़र" का विज्ञापन करते हैं और दबाव की रणनीति का उपयोग करके उधारकर्ताओं को तत्काल निर्णय लेने के लिए उकसाया जाता है।

सावधानियाँ

- सत्यापित करें कि क्या ऋणदाता सरकार / नियामक / अधिकृत एजेंसियों के साथ पंजीकृत है।
- जाँच करें कि क्या ऋणदाता ने कोई भौतिक पता या संपर्क जानकारी प्रदान की है ताकि यह सुनिश्चित हो सके कि बाद में उनसे संपर्क करना मुश्किल नहीं होगा।
- यदि ऋणदाता क्रेडिट स्कोर की जांच करने के बजाय व्यक्तिगत विवरण जानने में अधिक रुचि रखता है तो सावधान रहें।
- याद रखें कि कोई भी प्रतिष्ठित एनबीएफसी / बैंक ऋण आवेदन को संसाधित करने से पहले कभी भी भुगतान नहीं मांगेगा।
- वास्तविक ऋण प्रदाता कभी भी दस्तावेजों तथा अन्य जानकारियों की पुष्टि किए बिना पैसे की पेशकश नहीं करते हैं।
- सत्यापित करें कि क्या ये एनबीएफसी-समर्थित ऋण ऐप्स वास्तविक हैं अथवा नहीं।

5. मनी सर्कुलेशन/पोंजी/मल्टी लेवल मार्केटिंग (एमएलएम) योजनाएं धोखाधड़ी

कार्यप्रणाली

- एमएलएम/श्रृंखलाबद्धविपणन (चेन मार्केटिंग) /पिरामिड संरचना योजनाएं नामांकन/ सदस्यों को जोड़ने पर आसान या त्वरित धन का वादा करती हैं।
- ऐसी योजनाओं द्वारा न केवल उच्च रिटर्न का आश्वासन दिया जाता है बल्कि भोले-भाले लोगों का विश्वास हासिल करने के लिए अपने वादे के अनुसार पहली कुछ किश्तों का भुगतान भी करते हैं और मौखिक प्रचार के माध्यम से अधिक निवेशकों को आकर्षित करते हैं।
- ऐसी योजनाएँ अधिक से अधिक लोगों को श्रृंखला / समूह में शामिल होने के लिए प्रोत्साहित करती हैं, जिसके लिए उत्पादों की बिक्री से कमीशन के बजाय नामांकनकर्ता को कमीशन का भुगतान किया जाता है।
- इस मॉडल के कारण, कुछ समय बाद जब योजना में शामिल होने वाले लोगों की संख्या कम होने लगती है तो यह योजना अस्थिर हो जाती है। इसके बाद, धोखेबाज योजना को बंद कर देते हैं और लोगों द्वारा निवेश किए गए धन को लेकर गायब हो जाते हैं।

सावधानियाँ

- प्रतिफल जोखिम के समानुपाती होता है। जितना अधिक रिटर्न, उतना अधिक जोखिम। लगातार असामान्य रूप से उच्च रिटर्न (प्रति वर्ष 40-50 %) की पेशकश करने वाली कोई भी योजना संभावित धोखाधड़ी का पहला संकेत हो सकती है और सावधानी बरतने की जरूरत है ।
- हमेशा ध्यान दें कि माल/सेवा की वास्तविक बिक्री के बिना प्राप्त होने वाला कोई भुगतान/ कमीशन/ बोनस/ लाभ का प्रतिशत संदेहास्पद है और इससे धोखाधड़ी हो सकती है।
- मल्टी-लेवल मार्केटिंग / चेन मार्केटिंग / पिरामिड स्ट्रक्चर स्कीम चलाने वाली संस्थाओं द्वारा दिए जाने वाले उच्च रिटर्न के वादों के बहकावे में न आएं। प्राइज चिट एंड मनी सर्कुलेशन (प्रतिबंध) अधिनियम, 1978 के तहत मनी सर्कुलेशन / मल्टी-लेवल मार्केटिंग / पिरामिड संरचनाओं के तहत धन की स्वीकृति एक संज्ञेयअपराध है।
- ऐसे प्रस्तावों या ऐसी योजनाओं की जानकारी होने पर तुरंत राज्य पुलिस में शिकायत दर्ज की जानी चाहिए।

6. जाली दस्तावेज़ों के साथ धोखाधड़ी युक्त ऋण कार्यप्रणाली

- धोखेबाज वित्तीय संस्थानों से सेवाओं का लाभ उठाने के लिए जाली दस्तावेजों का उपयोग करते हैं।
- धोखेबाज पहचान की चोरी करते हैं, ग्राहकों की व्यक्तिगत जानकारी जैसे पहचान पत्र, बैंक खाता विवरण आदि की चोरी करते हैं, और वित्तीय संस्थान से लाभ प्राप्त करने के लिए इस जानकारी या क्रेडेंशियल का उपयोग करते हैं।
- धोखेबाज एनबीएफसी के कर्मचारियों के रूप में पेश होते हैं और ग्राहकों से केवाईसी से संबंधित दस्तावेज एकत्र करते हैं।

सावधानियाँ

- ✓ ऋण स्वीकृति / किसी भी संस्था से ऋण सुविधा का लाभ उठाने के लिए राष्ट्रीय स्वचालित समाशोधन गृह (NACH) फॉर्म सहित केवाईसी और अन्य व्यक्तिगत दस्तावेज प्रदान करते समय समुचित सावधानी और सतर्कता बरतें, विशेष रूप से ऐसे व्यक्ति से जो इन संस्थाओं के प्रतिनिधि होने का ढोंग करते हैं।
- ✓ ऐसे दस्तावेज़ केवल इकाई के अधिकृत कर्मियों या संस्थाओं के अधिकृत ईमेल आईडी के साथ साझा किए जाने चाहिए।
- ✓ यह सुनिश्चित करने के लिए संबंधित संस्थाओं के साथ अनुवर्ती कार्रवाई करें कि ऋण की स्वीकृति न होने और/या ऋण खाते को बंद करने की स्थिति में आपके द्वारा साझा किए गए दस्तावेज़ उनके द्वारा तुरंत वापस कर दिए गए जाएं।

वित्तीय लेनदेन करते समय बरती जाने वाली सामान्य सावधानियां

सामान्य सावधानियाँ

- ✓ आपके ब्राउज़िंग सत्र के दौरान दिखाई देने वाले संदिग्ध लगने वाले पॉप अप से सावधान रहें।
- ✓ ऑनलाइन भुगतान करने से पहले हमेशा एक सुरक्षित भुगतान गेटवे (https:// - पैड लॉक सिंबल वाला यूआरएल) की जांच करें ।
- ✓ अपना पिन (व्यक्तिगत पहचान संख्या), पासवर्ड, और क्रेडिट अथवा डेबिट कार्ड नंबर, सीवीवी, आदि निजी रखें और गोपनीय वित्तीय जानकारी को बैंकों/वित्तीय संस्थानों, मित्रों या यहां तक कि परिवार के सदस्यों के साथ भी साझा न करें।
- ✓ वेबसाइटों/उपकरणों/सार्वजनिक लैपटॉप/डेस्कटॉप पर कार्ड विवरण सहेजने (सेव करने) से बचें।
- ✓ जहां सुविधा उपलब्ध हो वहां टू-फैक्टर ऑथेंटिकेशन ऑन करें।
- ✓ अज्ञात स्रोतों से आने वाले ईमेल को कभी भी नहीं खोलें / उनका जवाब नहीं दें क्योंकि इनमें संदिग्ध अटैचमेंट या फ़िशिंग लिंक हो सकते हैं।

- ✓ चेकबुक, केवाईसी दस्तावेजों की प्रतियां कभी भी अजनबियों के साथ साझा न करें।

उपकरण (डिवाइस) / कंप्यूटर की सुरक्षा के लिए

- ✓ नियमित अंतराल पर पासवर्ड बदलें।
- ✓ डिवाइस पर एंटीवायरस इंस्टॉल करें और जब भी उपलब्ध हो अपडेट इंस्टॉल करें।
- ✓ उपयोग करने से पहले हमेशा अज्ञात यूनिवर्सल सीरियल बस (यूएसबी) ड्राइव/डिवाइस को स्कैन करें।
- ✓ अपने डिवाइस को खुला न छोड़ें।
- ✓ निर्दिष्ट समय के बाद डिवाइस के ऑटो लॉक को कॉन्फ़िगर करें।
- ✓ आपके फोन / लैपटॉप पर कोई भी अज्ञात एप्लिकेशन या सॉफ़्टवेयर इंस्टॉल न करें।
- ✓ उपकरणों पर पासवर्ड या गोपनीय जानकारी संचित (सेव) न करें।

सुरक्षित इंटरनेट ब्राउज़िंग के लिए

- ✓ अरक्षित /असुरक्षित / अज्ञात वेबसाइटों पर जाने से बचें।
- ✓ अनजान ब्राउजर के इस्तेमाल से बचें।
- ✓ सार्वजनिक उपकरणों पर पासवर्ड सहेजने (सेव करने) से बचें।
- ✓ अज्ञात वेबसाइटों / सार्वजनिक उपकरणों पर सुरक्षित क्रेडेंशियल डालने से बचें।
- ✓ किसी के साथ निजी जानकारी साझा न करें, विशेष रूप से सोशल मीडिया पर अज्ञात व्यक्तियों के साथ।
- ✓ किसी भी वेबपेज (https:// - पैड लॉक सिंबल के साथ यूआरएल) की सुरक्षा को हमेशा सत्यापित करें, खास तौर पर जब किसी ईमेल या एसएमएस लिंक द्वारा ऐसे पृष्ठों पर पुनर्निर्देशित (रीडायरेक्ट) किया जाता है।

सुरक्षित इंटरनेट बैंकिंग के लिए

- ✓ सार्वजनिक उपकरणों पर हमेशा वर्चुअल कीबोर्ड का उपयोग करें क्योंकि कीस्ट्रोक्स को कॉमप्रोमाइज़ किए गए उपकरणों, कीबोर्ड आदि के माध्यम से भी कैप्चर किया जा सकता है।
- ✓ उपयोग के तुरंत बाद इंटरनेट बैंकिंग सत्र से लॉग आउट करें।
- ✓ समय-समय पर पासवर्ड अपडेट करते रहें।
- ✓ ईमेल और इंटरनेट बैंकिंग के लिए एक जैसे पासवर्ड का इस्तेमाल न करें।
- ✓ वित्तीय लेनदेन के लिए सार्वजनिक टर्मिनलों (जैसे साइबर कैफे, आदि) का उपयोग करने से बचें।

- ✓ फोन का गर्म होना बैकग्राउंड में स्पाइवेयर चलाकर किसी के द्वारा जासूसी करने का संकेत हो सकता है।
- ✓ डेटा खपत की मात्रा में असामान्य वृद्धि कभी-कभी इस बात का संकेत हो सकती है कि बैकग्राउंड में स्पाइवेयर चल रहा है।
- ✓ स्पाइवेयर ऐप्स कभी-कभी फ़ोन की शटडाउन प्रक्रिया में हस्तक्षेप कर सकते हैं ताकि डिवाइस ठीक से बंद होने में विफल रहे या ऐसा करने के लिए असामान्य रूप से लंबा समय लगे।
- ✓ ध्यान दें कि डेटा भेजने और प्राप्त करने के लिए स्पाइवेयर और मैलवेयर द्वारा टेक्स्ट संदेशों का उपयोग किया जा सकता है।

धोखाधड़ी की घटना के बाद की जाने वाली कार्रवाई

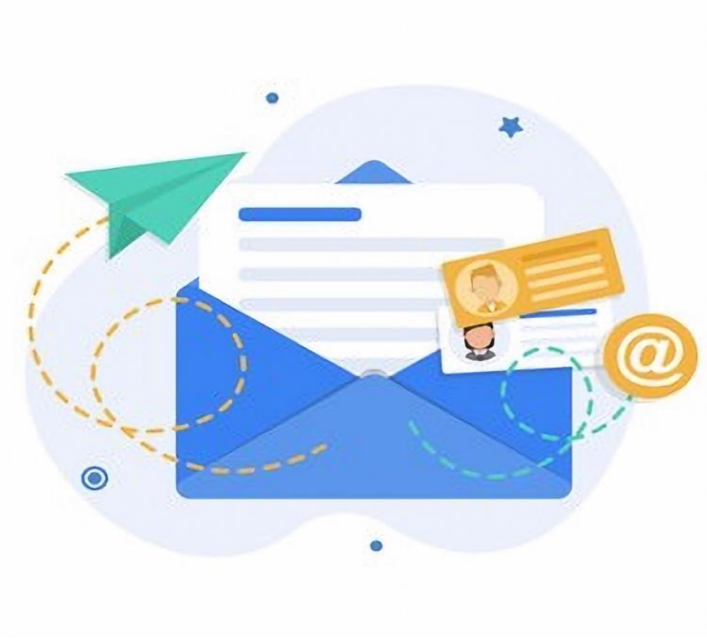
- ✓ न केवल डेबिट कार्ड / क्रेडिट कार्ड को ब्लॉक करें बल्कि अपनी शाखा में जाकर या बैंक की वेबसाइट पर उपलब्ध **आधिकारिक कस्टमर केयर नंबर** पर कॉल करके कार्ड से जुड़े बैंक खाते में डेबिट को भी फ्रीज कर दें। साथ ही, अन्य बैंकिंग चैनलों जैसे नेट बैंकिंग, मोबाइल बैंकिंग आदि की जांच करें और उनकी सुरक्षा सुनिश्चित करें, ताकि धोखाधड़ी के बाद डेबिट/क्रेडिट कार्ड आदि के अवरुद्ध हो जाने पर धोखाधड़ी को रोका जा सके।
- ✓ हेल्पलाइन नंबर 155260 या 1930 डायल करें या घटना की रिपोर्ट राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) पर करें।
- ✓ मोबाइल रीसेट करें: मोबाइल से डेटा लीक होने के कारण धोखाधड़ी होने पर मोबाइल रीसेट करने के लिए (सेटिंग-रीसेट-फ़ैक्टरी डेटा) का उपयोग करें।

डेबिट/क्रेडिट कार्ड से संबंधित सावधानियाँ

- ✓ यदि आप कुछ समय के लिए कार्ड का उपयोग नहीं करने जा रहे हैं, तो आपको क्रेडिट/डेबिट कार्ड की विभिन्न विशेषताओं, जैसे घरेलू और अंतर्राष्ट्रीय लेनदेन दोनों के लिए ऑनलाइन लेनदेन को निष्क्रिय कर देना चाहिए और कार्ड के उपयोग की आवश्यकता होने पर ही इसे सक्रिय करना चाहिए।
- ✓ इसी प्रकार, यदि कार्ड का उपयोग नहीं करना है, तो नियर फील्ड कम्युनिकेशन (एनएफसी) सुविधा को निष्क्रिय कर देना चाहिए।
- ✓ किसी भी प्वाइंट ऑफ सेल (पीओएस) साइट पर या एनएफसी रीडर पर कार्ड का उपयोग करते समय पिन दर्ज करने से पहले, आपको पीओएस मशीन की स्क्रीन और एनएफसी रीडर पर प्रदर्शित राशि की सावधानीपूर्वक जांच करनी चाहिए।
- ✓ लेन-देन करते समय स्वाइप करने के लिए व्यापारी को कार्ड को आपकी दृष्टि से दूर न ले जाने दें।
- ✓ पीओएस साइट/एटीएम पर पिन डालते समय कीपैड को अपने दूसरे हाथ से ढक लें।

ई-मेल अकाउंट की सुरक्षा के लिए

- ✓ अनजान पतों (एड्रेस) / नामों से प्राप्त लिंकों पर क्लिक न करें।
- ✓ सार्वजनिक या मुफ्त नेटवर्क पर ईमेल का उपयोग करने से बचें।
- ✓ ईमेल में सुरक्षित क्रेडेंशियल/बैंक पासवर्ड आदि को संचित न करें।



पासवर्ड सुरक्षा के लिए

- ✓ अपने पासवर्ड में अक्षरांकीय (अल्फान्यूमेरिक) और विशेष वर्णों (स्पेशल करेक्टर) के संयोजन का उपयोग करें।
- ✓ सुविधा उपलब्ध होने पर अपने सभी खातों के लिए टू फैक्टर ऑथेंटिकेशन रखें ।
- ✓ समय-समय / आवधिक आधार पर पासवर्ड बदलें।
- ✓ आपकी जन्मतिथि, जीवनसाथी का नाम, कार नंबर आदि को पासवर्ड के रूप में रखने से बचें।

आपको कैसे पता चलेगा जमाराशि स्वीकार करने वाली एनबीएफसी असली है या नहीं?

- ✓ जमाकर्ता को यह सत्यापित करना चाहिए कि https://rbi.org.in पर उपलब्ध जमाराशि स्वीकार करने के लिए पात्र एनबीएफसी की सूची में एनबीएफसी का नाम है या नहीं, और यह सुनिश्चित करें कि इस एनबीएफ़सी का नाम जमाराशिस्वीकार करने से प्रतिबंधित कंपनियों की सूची में नहीं दिख रहा है।
- ✓ एनबीएफसी द्वारा अपनी साइट पर / अपने कार्यालय में रिज़र्व बैंक द्वारा जारी पंजीकरण प्रमाणपत्र (सीओआर) को प्रमुखता से प्रदर्शित करना आवश्यक है। इस प्रमाणपत्र में यह भी दर्शाया जाना चाहिए कि एनबीएफसी को आरबीआई द्वारा विशेष रूप से जमाराशि स्वीकार करने के लिए अधिकृत किया गया है। उक्त को सुनिश्चित करने के लिए जमाकर्ताओं को प्रमाणपत्र की जांच करनी चाहिए कि एनबीएफसी जमा स्वीकार करने के लिए अधिकृत है अथवा नहीं।
- ✓ एनबीएफसी 12 महीने से कम और 60 महीने से अधिक की अवधि के लिए जमाराशि स्वीकार नहीं कर सकती हैं और एनबीएफसी द्वारा जमाकर्ता को दी जाने वाली अधिकतम ब्याज दर 12.5% से अधिक नहीं होनी चाहिए।
- ✓ रिजर्व बैंक द्वारा ब्याज दरों में बदलाव को https://rbi.org.in → साइटमैप → एनबीएफसी सूची → अक्सर पूछे वाले प्रश्न पर प्रकाशित किया जाता है।

जमाकर्ताओं द्वारा बरती जाने वाली सावधानियाँ

- ✓ जमाकर्ता द्वारा बैंक/एनबीएफसी/कंपनी के पास जमा की गई प्रत्येक जमा राशि के लिए एक उचित रसीद प्रदान करने पर जोर देना चाहिए।
- ✓ रसीद कंपनी द्वारा अधिकृत अधिकारी द्वारा विधिवत हस्ताक्षरित होनी चाहिए और अन्य बातों के साथ-साथ उसमें जमा करने की तारीख, जमाकर्ता का नाम, शब्दों और अंकों में राशि, देय ब्याज दर, परिपक्वता तिथि और राशि का उल्लेख होना चाहिए।
- ✓ गैर-बैंकिंग वित्तीय कंपनियों की ओर से जनता से जमाराशियां एकत्रित करने वाले दलालों/एजेंटों आदि के मामले में, जमाकर्ताओं को स्वयं को संतुष्ट करना चाहिए कि दलाल/एजेंट एनबीएफसी द्वारा विधिवत रूप से अधिकृत हैं।याद रखें कि एनबीएफसी के जमाकर्ताओं के लिए जमा बीमा सुविधा उपलब्ध नहीं है।

शिकायत दर्ज करें

आरबीआई लोकपाल को शिकायत

- ✓ ऑनलाइन शिकायत दर्ज करने के लिए कृपया https://cms.rbi.org.in/ लिंक पर जाएं।
- ✓ ईमेल द्वारा शिकायत crpc@rbi.org.in पर भेजी जा सकती है।
- ✓ भौतिक रूप / पेपर फॉर्म में शिकायतें सीआरपीसी, भारतीय रिजर्व बैंक, सेंट्रल विस्टा, सेक्टर -17, चंडीगढ़ -160 017 को भेजी जा सकती हैं।

भारतीय प्रतिभूति और विनिमय बोर्ड (सेबी) को शिकायत

- ✓ कृपया https://www.sebi.gov.in/ लिंक पर जाएं।

भारतीय बीमा नियामक और विकास प्राधिकरण (aआईआरडीएआई) को शिकायत

- ✓ कृपया https://www.irdai.gov.in/ लिंक पर जाएं।

राष्ट्रीय आवास बैंक (एनएचबी) को शिकायत

- ✓ कृपया https:// nhb.org.in/ लिंक पर जाएं।

साइबर पुलिस स्टेशन में शिकायत

- ✓ कृपया https://cybercrime.gov.in/ देखें ।
- ✓

****

शब्दावली

- ✓ **अग्रिम शुल्क/प्रसंस्करण शुल्क/टोकन शुल्क:** इनमें प्रारंभिक भुगतान जैसे दस्तावेज़ीकरण शुल्क, बैठक व्यय, प्रसंस्करण शुल्क, अन्य शुल्क शामिल हैं जो एक उधारकर्ता को ऋण के वितरण के लिए लागू हो सकते हैं।
- ✓ **टू-फैक्टर ऑथेंटिकेशन (दो-कारक प्रमाणीकरण) :** प्रमाणीकरण पद्धतियों में तीन बुनियादी 'कारक' शामिल होते हैं- कुछ ऐसा जो उपयोगकर्ता जानता है (जैसे, पासवर्ड, पिन- या तो स्थिर या एक बार उत्पन्न); उपयोगकर्ता के पास कुछ है (उदाहरण के लिए, एटीएम/स्मार्ट कार्ड नंबर, समाप्ति तिथि और कार्ड पर मुद्रित सीवीवी); और उपयोगकर्ता कुछ ऐसा है (जैसे, बायोमेट्रिक विशेषता, जैसे कि एक फिंगरप्रिंट)। दो-कारक प्रमाणीकरण (2FA के रूप में भी जाना जाता है) उपयोगकर्ताओं को दो अलग-अलग घटकों के संयोजन के माध्यम से स्पष्ट पहचान प्रदान करता है - उपयोगकर्ता के पास क्या है और लेन-देन पूरा करने के लिए उपयोगकर्ता क्या जानता/जानता है। और -
- ✓ **प्राधिकरण:** कार्ड जारी करने वाले बैंक की ओर से व्यापारी के लेन-देन प्राधिकरण अनुरोध पर प्रतिक्रिया यह दर्शाती है कि भुगतान जानकारी मान्य है और ग्राहक के क्रेडिट कार्ड पर फंड उपलब्ध हैं।
- ✓ **कार्ड नंबर:** क्रेडिट कार्ड एसोसिएशन या कार्ड जारी करने वाले बैंक द्वारा किसी कार्ड को दिया गया नंबर। क्रेडिट कार्ड से भुगतान करने के लिए ग्राहक द्वारा यह जानकारी व्यापारी को प्रदान की जानी चाहिए, लेकिन किसी अन्य के साथ साझा नहीं की जानी चाहिए। कार्ड पर अंकों की स्ट्रिंग छपी होती है।
- ✓ **क्रेडिट कार्ड:** एक कार्ड जो किसी वित्तीय संस्थान से असुरक्षित/सुरक्षित क्रेडिट का लाभ उठाकर उत्पादों या सेवाओं के लिए भुगतान करने की अनुमति देता है।
- ✓ **क्रेडिट सीमा:** यह शब्द एक वित्तीय संस्था द्वारा ग्राहक को दिए जाने वाले ऋण की अधिकतम राशि को प्रदर्शित करता है। ऋण प्रदान करने वाली संस्था क्रेडिट कार्ड की मांग करने वाले आवेदक द्वारा दी गई जानकारी के विश्लेषण के आधार पर क्रेडिट कार्ड पर क्रेडिट सीमा उपलब्ध कराती है। क्रेडिट सीमा ग्राहक के क्रेडिट स्कोर और भविष्य में क्रेडिट प्राप्त करने की उनकी क्षमता को प्रभावित कर सकती है।
- ✓ **सीवीवी:** यह कार्ड सत्यापन मान को दर्शाता है। यह कार्ड पर छपी 3 अंकों की संख्या है जो अधिकांश ऑनलाइन लेनदेन को पूरा करने के लिए अनिवार्य है। ये विवरण गोपनीय हैं और इन्हें किसी के साथ कभी भी साझा नहीं किया जाना चाहिए।
- ✓ **डेबिट कार्ड:** वह कार्ड जो कार्डधारक के बैंक खाते में उपलब्ध धन की कटौती करके उत्पादों या सेवाओं के लिए भुगतान करने की अनुमति देता है।

- ✓ **ई-कॉमर्स प्लेटफॉर्म:** यह एक ऐसा प्लेटफॉर्म/वेबसाइट है जो डिजिटल और इलेक्ट्रॉनिक नेटवर्क पर डिजिटल उत्पादों सहित वस्तुओं और सेवाओं की खरीद और बिक्री को सक्षम बनाता है।
- ✓ **ईएमआई:** यह समान मासिक किश्तों को दर्शाता है। यह एक निश्चित मासिक भुगतान है (मूलधन और ब्याज सहित), जो एक उधारकर्ता द्वारा अपने ऋणदाता/लेनदार (जैसे बैंक/एनबीएफसी) को हर माह तब तक किया जाता है, जब तक कि उधारकर्ता द्वारा ऋणदाता/लेनदार से लिए गए ऋण/क्रेडिट का ब्याज सहित पूर्ण रूप से भुगतान नहीं कर दिया जाता है।
- ✓ **एन्क्रिप्शन:** प्रसंस्करण सूचना को इलेक्ट्रॉनिक कोड में बदलने की प्रक्रिया ताकि इसकी गोपनीयता बनाए रखी जा सके।**समाप्ति तिथि:** वह तिथि जिस पर कार्ड, संविदा, करार, दस्तावेज़ आदि की वैधता समाप्त हो जाती है। लेन-देन केवल उन कार्डों या दस्तावेजों के लिए स्वीकृत किए जाएंगे जो अभी तक समाप्त नहीं हुए हैं।
- ✓ **गेटवे:** यह एक मध्यस्थ है जो सीधे तौर पर शामिल हुए बिना लेनदेन आधार प्रबंधन, जोखिम प्रबंधन आदि सेवाओं के प्रसंस्करण को सुगम बनाने के लिए प्रौद्योगिकी अवसंरचना प्रदान करता है। पेमेंट गेटवे ऐसी संस्थाएं हैं जो फंड के संचालन में किसी भी तरह की भागीदारी के बिना ऑनलाइन भुगतान लेनदेन को रूट करने और प्रसंस्करण की सुविधा प्रदान करने के लिए बुनियादी प्रौद्योगिकी अवसंरचना प्रदान करती हैं।
- ✓ **तत्काल भुगतान सेवाएं (आईएमपीएस):** यह भारतीय राष्ट्रीय भुगतान निगम (एनपीसीआई) द्वारा मोबाइल फोन के माध्यम से प्रदान की जाने वाली एक तत्काल इंटरबैंक इलेक्ट्रॉनिक फंड ट्रांसफर सेवा (एक सीमा तक) है।
- ✓ **(केवाईसी):** इसका आशय है अपने ग्राहक को जानें। यह वह प्रक्रिया है जिसमें वित्तीय संस्था दस्तावेजों का एक सेट प्राप्त करके और समुचित सावधानी से ग्राहक के साथ संबंध बनाए रखने में शामिल पहचान, उपयुक्तता और जोखिमों को सत्यापित करने का प्रयास करती है।
- ✓ **मनी म्यूल:** यह उन पीड़ितों का वर्णन करने के लिए इस्तेमाल किया जाने वाला शब्द है, जिनका शोषण धोखेबाजों द्वारा उनके बैंक खाते के माध्यम से चोरी / अवैध धन को वैध बनाने के लिए किया जाता है
- ✓ **मल्टी लेवल मार्केटिंग:** सिस्टम में मौजूद किसी कंपनी और साथ ही उनके द्वारा भर्ती किए गए किसी भी प्रतिभागी की ओर से माल या सेवाओं को बेचने की प्रथा जिसके तहत प्रतिभागियों को उनकी बिक्री पर कमीशन प्राप्त होता है।

- ✓ **राष्ट्रीय स्वचालित समाशोधन गृह (एनएसीएच):**यह भारतीय राष्ट्रीय भुगतान निगम (एनपीसीआई) द्वारा संचालित एक केंद्रीकृत इलेक्ट्रॉनिक समाशोधन सेवा (ईसीएस) प्रणाली है।
- ✓ **नियर फील्ड कम्युनिकेशन (एनएफसी):** यह एक संचार तकनीक है जिसका उपयोग एनएफसी से लैस डिवाइस से एक सक्षम टर्मिनल तक डेटा संचारित करने के लिए किया जाता है। एनएफसी तकनीक का उपयोग संपर्क रहित भुगतान करने के लिए किया जाता है जो स्मार्टफोन/कार्ड को एनएफसी सक्षम मशीन के पास रखकर किया जाता है।
- ✓ **एनईएफटी:** यह एक राष्ट्रव्यापी केंद्रीकृत भुगतान प्रणाली है जिसका स्वामित्व और संचालन भारतीय रिजर्व बैंक के पास है, जो भारत में बैंक ग्राहकों को किन्हीं दो एनईएफटी-सक्षम बैंक खातों के बीच धन अंतरित करने में सक्षम बनाता है।
- ✓ **ओटीपी:** वन टाइम पासवर्ड प्रमाणीकरण पद्धति के कारकों में से एक है, जिसे ग्राहक जानता है और अक्सर ऑनलाइन लेनदेन करने के लिए इसका उपयोग किया जाता है। यह गोपनीय है और इसे किसी के साथ साझा नहीं किया जाना चाहिए।
- ✓ **फ़िशिंग –** यह नकली ईमेल और / या एसएमएस को दर्शाता है, जो ग्राहकों को यह सोचने हेतु धोखा देने के उद्देश्य से डिज़ाइन किया गया है कि संचार उनके बैंक / ई-वॉलेट प्रदाता से उत्पन्न हुआ है और इसमें गोपनीय विवरण निकालने के लिए लिंक शामिल हैं।
- ✓ **पॉइंट ऑफ़ सेल डिवाइस टर्मिनल (पीओएस)/स्वीकृति उपकरण(एमपीओएस):** यह व्यापारिक प्रतिष्ठानों में स्थापित किसी भी उपकरण / टर्मिनल / मशीन को दर्शाता है, जो व्यापारियों को भुगतान कार्ड (क्रेडिट कार्ड, डेबिट कार्ड, उपहार कार्ड आदि) के माध्यम से भुगतान स्वीकार करने में सक्षम बनाता है।
- ✓ **त्वरित प्रतिक्रिया (क्यूआर) कोड:** क्यूआर कोड एक प्रकार का द्वि-आयामी बार कोड है। इसमें एक सफेद पृष्ठभूमि पर एक वर्ग ग्रिड में काले वर्ग व्यवस्थित होते हैं। इन कोड्स को पढ़ने और उसका अर्थ पता करने के लिए स्मार्टफोन कैमरों जैसे इमेजिंग उपकरणों का उपयोग किया जा सकता है। क्यूआर कोड में आदाता(पाने वाले) के बारे में जानकारी होती है और इसका उपयोग ग्राहकों के खाते को डेबिट करके बिक्री के बिंदु पर मोबाइल भुगतान की सुविधा के लिए किया जाता है।
- ✓ **रिमोट एक्सेस:** यह ग्राहक को अपने मोबाइल फोन / कंप्यूटर पर एक एप्लिकेशन डाउनलोड करने के लिए लुभाने को दर्शाता है, जो उस ग्राहक के डिवाइस पर सभी ग्राहकों के डेटा को एक्सेस करने में सक्षम है।

- ✓ **यूनिफाइड पेमेंट इंटरफेस (यूपीआई):** यूनिफाइड पेमेंट इंटरफेस एक ऐसा प्लेटफॉर्म है जो इंटरनेट एक्सेस वाले मोबाइल फोन का उपयोग करके एक बैंक / वॉलेट खाते से दूसरे में पैसे अंतरित करने की अनुमति देता है। एक बार जब ग्राहक बैंक के साथ यूपीआई के लिए पंजीकरण कर लेता है, तब वह एक अद्वितीय आभासी पहचानकर्ता बनाया जाता है और भुगतान शुरू करने के लिए उसे ग्राहक के मोबाइल फोन से मैप किया जाता है। यह यूपीआई-पिन के रूप में प्रमाणीकरण का उपयोग करता है, जो गोपनीय है और इसे किसी के साथ साझा नहीं किया जाना चाहिए।
- ✓ **विशिंग:** यह बैंक/गैर-बैंक ई-वॉलेट प्रदाताओं/दूरसंचार सेवा प्रदाताओं से होने का दिखावा करने वाले फोन कॉलों को दर्शाता करता है जो ग्राहकों को केवाईसी-अपडेशन, खाते/सिम-कार्ड को अनब्लॉक करने, डेबिट की गई राशि जमा करने,आदि के बहाने गोपनीय विवरण साझा करने के लिए लुभाते हैं।
- ✓ **बटुआ (वॉलेट) :** वॉलेट एक खाते की तरह होता है जिसका उपयोग इसमें संचित मूल्य के विरुद्ध वस्तुओं और सेवाओं की खरीद के लिए किया जा सकता है। वॉलेट वर्चुअल हो सकता है (जैसे मोबाइल वॉलेट) अथवा फिजिकल हो सकता है (जैसे प्रीपेड कार्ड)।

****

भारतीय रिज़र्व बैंक

Design by M Muralidhar, Anupam Sharma