



किसी को भी न बताएं

ओटीपी • कार्ड नंबर • यूपीआई पिन • बैंक संबंधी जानकारी

• कस्टमर आईडी और पासवर्ड

फिशिंग और स्मिशिंग लिंक्स

धोखाधड़ी

- जालसाज SMS, ई-मेल, सोशल मीडिया पोस्ट, इंस्टेंट मैसेंजर आदि के जरिए लिंक ट्रांसमिट करने के लिए थर्ड पार्टी वेबसाइट बनाते हैं।
- जब आप लिंक पर क्लिक करते हैं, तो आपको एक ऐसी फिशिंग वेबसाइट पर ले जाया जाता है जो देखने में बिलकुल असली जैसी लगती है। वहां आपको अपनी बैंक जानकारी दर्ज करने के लिए कहा जाएगा।
- एक बार जब आप यह प्रक्रिया पूरी कर लेते हैं, तो जालसाज आपकी जानकारियों का गलत इस्तेमाल करता है।



सुरक्षा के उपाय



- फिशिंग के खिलाफ सुरक्षा का पहला उपाय यह जानना है कि आपका बैंक कभी भी आपसे संबंधित जानकारियां नहीं मांगेगा या आपको अपनी वेबसाइट पर लिंक नहीं भेजेगा।
- जोखिम से बचने के लिए अपना कार्ड ब्लॉक करें या अपना पासवर्ड तुरंत बदलें।

विशिंग कॉल्स

धोखाधड़ी

- ऑनलाइन जानकारी प्राप्त करके एक धोखेबाज बैंकर, फ़र्म का कर्मचारी या बीमा एजेंट बनकर आपसे संपर्क कर सकता है।
- वे इसे एक बहुत ज़रूरी मामला बता सकते हैं और आपके बैंक और शाखा के बारे में बुनियादी तथ्यों को बताकर आपका भरोसा जीत सकते हैं।
- एक बार धोखेबाज जब आपका भरोसा हासिल कर लेता है, तो वो आपसे आपका KYC अपडेट करने के लिए कहेगा, जिसके लिए वो आपको आकर्षक छूट देगा, पेनेल्टी से बचने के लिए भुगतान करने जैसी बातें करके आपको धोखा देने की कोशिश करेगा।



सुरक्षा के उपाय



- अपने कार्ड को तुरंत ब्लॉक करें।
- अपना पासवर्ड अक्सर रीसेट करते रहें।

ऑनलाइन सेलिंग प्लेटफॉर्म का इस्तेमाल करके धोखाधड़ी

धोखाधड़ी

- जालसाज ऑनलाइन सेलिंग प्लेटफॉर्म पर खरीददार बनकर आते हैं और आपके प्रॉडक्ट में रुचि दिखाते हैं.
- पैसे का भुगतान करने के बजाय, वे UPI ऐप्स के माध्यम से 'पैसे का अनुरोध' करते हैं और आपसे कहते हैं कि अपने अकाउंट से पैसे निकालने के लिए आप इसे स्वीकार करें.



सुरक्षा के उपाय



- अपने वित्तीय संस्थान को अनधिकृत लेनदेन की घटनाओं की तुरंत जानकारी दे.
- अपनी शिकायत दर्ज करने के लिए राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 155260 से संपर्क करें.

आपकी जानकारियां चोरी करने के लिए नकली हेल्पलाइन और स्क्रीन शेयरिंग ऐप

धोखाधड़ी

- ग्राहक बिज़नेस हेल्पलाइन नंबर देखने के लिए सर्च इंजन का इस्तेमाल करते हैं, जहां स्कैमर्स फ़र्जी नंबर अपलोड करते हैं और ग्राहक को उन नंबरों पर कॉल करने के लिए प्रोत्साहित करते हैं.
- धोखेबाज बैंक का आदमी होने का दिखावा करता है और आपसे ऐप डाउनलोड करने और अपनी स्क्रीन साझा करने आपके डिवाइस का एक्सेस प्राप्त करता है या वेरिफिकेशन के लिए आपके कार्ड की जानकारियां मांगता है.
- हम उन्हें सच मानते हुए अपनी गुप्त जानकारियां उनके साथ शेयर करते हैं.
- इनकी मदद से वे आपकी बैंकिंग का एक्सेस प्राप्त करते हैं और बाद में पेमेंट ऐप या इंटरनेट बैंकिंग का उपयोग करके पैसे निकाल लेते हैं.



सुरक्षा के उपाय



- कभी भी ऐप्स डाउनलोड न करें और अपनी स्क्रीन किसी अज्ञान आदमी के साथ शेयर न करें.
- यदि आपको कोई परेशानी हो तो हमेशा अपनी शाखा में जाएं.

सोशल मीडिया के माध्यम से जालसाजी

धोखाधड़ी



- जालसाज जाने-माने सोशल मीडिया प्लेटफॉर्म पर फर्जी अकाउंट बनाते हैं और मेडिकल बिल या भुगतान के लिए पैसे मांगते हैं.
- वे समय के साथ आपका विश्वास हासिल करते हैं और बाद में निजी जानकारी का उपयोग करके ब्लैकमेल और पैसे निकालने के लिए करते हैं.

सुरक्षा के उपाय



- हमेशा ऑनलाइन अकाउंट की सत्यता की पुष्टि करें और गोपनीय जानकारी के बारे में पूछने पर संदेह ज़रूर करें.
- अपनी शिकायत दर्ज करने के लिए राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 155260 से संपर्क करें.

लॉटरी संबंधी धोखाधड़ी

धोखाधड़ी



- जालसाज आपको एक ई-मेल लिख सकते हैं या आपको कॉल कर सकते हैं, यह दावा करते हुए कि आपने लॉटरी में एक बहुत बड़ा इनाम जीता है. पर पैसे पाने के लिए, उनकी वेबसाइट पर बैंक अकाउंट या क्रेडिट कार्ड द्वारा पहचान का वेरिफिकेशन करना आवश्यक है, जहां पर डेटा एकत्र किया जाता है.
- कुछ परिस्थितियों में, धोखेबाज लॉटरी/सामान पाने के लिए टैक्स, शिपिंग फ़ीस, प्रोसेसिंग फ़ीस और अन्य फ़ीस के लिए एडवांस पेमेंट की मांग करते हैं.
- चूंकि मांगी गई रकम लॉटरी/सामान का एक बहुत ही छोटा सा प्रतिशत होता है, इसलिए लोग धोखेबाज की बातों में आकर भुगतान कर सकते हैं.

सुरक्षा के उपाय



- लॉटरी जीतने से संबंधित कॉल/ SMS /ई-मेल का कभी भी जवाब न दें.
- असुविधा से बचने के लिए अपने बैंक या क्रेडिट कार्ड के जारीकर्ता को सूचित करें

जालसाजों द्वारा लोन देने के लिए फ़र्जी विज्ञापन

- जालसाज बहुत आकर्षक ब्याज दरों पर, आसान पुनर्भुगतान विकल्पों आदि के साथ पर्सनल लोन्स के लिए नकली विज्ञापन बनाते हैं, और फिर ग्राहकों से उनसे संपर्क करने के लिए कहते हैं.
- ये ई-मेल आईडी भोले-भाले ग्राहकों के साथ विश्वसनीयता बनाने और उनमें भरोसा जगाने के लिए सीनियर बैंक ऑफिसर्स की ई-मेल आईडी जैसी दिखने वाली ई-मेल आईडी बनाते हैं.
- जब ग्राहक लोन के लिए धोखेबाजों से संपर्क करते हैं, तो वे प्रोसेसिंग फ़ीस, GST, इंटरस्टेट कॉस्ट जैसे अलग-अलग एडवांस फ़ीस की मांग करते हैं, और फिर बिना लोन दिए ही गायब हो जाते हैं.

धोखाधड़ी



सुरक्षा के उपाय



- बातचीत में निवेश करने से बचें और लोन लेने के लिए अपने रिलेशनशिप मैनेजर से संपर्क करें.
- सावधान रहें और कई ऐसे सवाल पूछें जिनका जवाब केवल वे ही जानते होंगे.

ऑनलाइन नौकरी संबंधी धोखाधड़ी

- नकली जॉब सर्च पोर्टल बना लिए जाते हैं, और जब ज़रूरतमंद लोग रजिस्ट्रेशन के लिए इन वेबसाइटों पर गुप्त बैंक अकाउंट, क्रेडिट कार्ड, या डेबिट कार्ड संबंधी जानकारियां दर्ज करते हैं, तो उन अकाउंट के साथ छेड़छाड़ की जाती है.
- कुछ परिस्थितियों में, धोखेबाज एक प्रतिष्ठित कॉर्पोरेशन के अधिकारी के रूप में खुदको बताता है और नकली इंटरव्यू करने के बाद आपके चुने जाने की पुष्टि करते हैं. इसके बाद उनसे एक महत्वपूर्ण ट्रेनिंग प्रोग्राम के लिए भुगतान करने का दबाव डाला जाता है.

धोखाधड़ी



सुरक्षा के उपाय



- हमेशा प्रमाणित जॉब पोर्टल का ही इस्तेमाल करें.
- किसी अज्ञान कंपनी के ई-मेल का जवाब न दें क्योंकि यह एक स्कैम हो सकता है.

ATM कार्ड स्किमिंग

- ATM मशीनों में स्किमिंग उपकरण पाए गए हैं, जिससे धोखेबाज़ आपके कार्ड से डेटा ले सकते हैं और एक डमी कीपैड और एक छोटा/ पिनहोल कैमरा स्थापित करके आपका पिन प्राप्त कर सकते हैं जो कुशलता के साथ छिपाए गए होते हैं।
- कई बार, धोखेबाज़ आम ग्राहकों के रूप में सामने आ सकते हैं और जब आप पिन दर्ज कर रहे हों तो वो उसे देख लेता है। फिर इस जानकारी की मदद से ड्युप्लीकेट कार्ड बनाने और ग्राहक के खाते से पैसे निकालने के लिए किया जाता है।

धोखाधड़ी



सुरक्षा के उपाय



- जांचें कि कहीं ATM में कोई छेड़छाड़ तो नहीं हुई है।
- अपने आसपास के संदिग्ध लोगों पर हमेशा नज़र रखें।

सिम स्वैप

- चूंकि आपका रजिस्टर्ड मोबाइल नंबर आपके अकाउंट की अधिकांश जानकारी और प्रमाणीकरण से जुड़ा हुआ है, इसलिए धोखेबाज़ आपके सिम कार्ड का एक्सेस पाने या ड्युप्लीकेट सिम प्राप्त करने का प्रयास करता है, ताकि उनके ड्युप्लीकेट सिम पर आए ओटीपी का उपयोग करके वे डिजिटल लेनदेन कर सकें।
- जालसाज आमतौर पर ग्राहकों को उनकी नेटवर्क कंपनी से होने का दावा करते हुए कॉल करते हैं, जो 3G से 4G में मुफ्त अपग्रेड या सिम कार्ड पर बोनस के बदले में जानकारी की मांग करते हैं।

धोखाधड़ी



सुरक्षा के उपाय



- यदि आपके फ़ोन में काफ़ी समय से मोबाइल नेटवर्क नहीं है तो आपको संदेह हो जाना चाहिए।
- आपके सिम के लिए कोई ड्युप्लीकेट सिम जारी नहीं किया जा रहा है यह सुनिश्चित करने के लिए कि अपने मोबाइल ऑपरेटर से संपर्क करें।

जाली दस्तावेज़ों के साथ धोखाधड़ी करके लोन

धोखाधड़ी



- ये धोखाधड़ी तब होती है जब कोई व्यक्ति या संस्था वित्तीय संस्थानों से किसी भी प्रकार की सेवाओं का लाभ उठाने के लिए जाली दस्तावेज़ों का उपयोग करती है।
- NBFC कर्मचारी / NBFC की ई-मेल आईडी की प्रामाणिकता की पुष्टि किए बिना वित्तीय संस्थाओं के साथ KYC से संबंधित दस्तावेज़ों को साझा करते समय ऐसी धोखाधड़ी हो सकती है।
- पीड़ित व्यक्ति की व्यक्तिगत जानकारियां, जैसे कि पहचान पत्र, बैंक अकाउंट संबंधी विवरण आदि की चोरी करके धोखाधड़ी वाले लोन पास किए जाते हैं और इन जानकारी का उपयोग किसी वित्तीय संस्थान से लाभ प्राप्त किया जाता है।

सुरक्षा के उपाय



- अपनी जानकारियों को शेयर करने से पहले हमेशा NBFC कर्मचारी/कंपनी की प्रामाणिकता की पुष्टि करें।
- पहचान संबंधी चोरी से बचने के लिए अपने पहचान पत्र, बैंक अकाउंट का विवरण आदि सुरक्षित रखें।

आधार ओटीपी से समझौता

धोखाधड़ी



- आधार आधारित ओटीपी से डिजिटल अकाउंट खोले जा सकते हैं।
- ऐसे कई उदाहरण हैं जहां ग्राहक अपने UIDAI ओटीपी को थर्ड पार्टी के वेंडर्स को शेयर करते हैं, और उनसे धोखेबाज़ों को गलत अकाउंट बनाने में मदद मिलती है।

सुरक्षा के उपाय



- अपने आधार ओटीपी को असत्यापित संस्थानों के साथ शेयर न करें।
- किसी भी जानकारी को शेयर करने से पहले हमेशा व्यक्ति की पहचान वेरिफ़ाई करें।



अधिक जानकारी के लिए,
एचडीएफसी बैंक के सिक्योर बैंकिंग पेज पर जाए

<https://www.hdfcbank.com/personal/useful-links/security>

*रिटेल लोन बुक साइज़ पर आधारित (मॉर्गेंजेस को छोड़कर). सोर्स: FY 19-20 वार्षिक रिपोर्ट्स.
मार्केट कैपिटलाइजेशन पर नं.1 आधारित है BSE आंकड़े पर 31 दिसंबर, 2020 के दिन.