बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

Integrated Risk Management Department

Head Office, Pune - 411005

प्रिय मूल्यवान ग्राहक, 12.12.2019

बैंक ऑफ महाराष्ट्र के साथ बैंकिंग के लिए धन्यवाद!

आपके खाते की सुरक्षा हमारे लिए अत्यंत महत्वपूर्ण है। अपने ग्राहकों को सुरक्षा के बारे में शिक्षित करना जारी रखने के हमारे प्रयास में, हम ग्राहक जागरूकता - 9 का प्रकाशन कर रहे हैं। कृपया इसे नीचे संलग्न पाएं। आशा है कि आप इसे उपयोगी और जानकारीपूर्ण पाएंगे।

ग्राहक जागरूकता - 9

सोशल इंजीनियरिंग धोखाधड़ी से स्वयं को बचाएं

केवाईसी अपडेशन, बैंक खातों को लिंक करना, ग्राहकों की गोपनीय जानकारी मांगना आदि विषय पर धोखाधड़ीपूर्ण यूआरएलवाले एसएमएस और धोखाधड़ीपूर्ण फोन कॉल्स आजकल बहुत प्रचलित हैं।

ये धोखेबाजों द्वारा निर्दोष व्यक्तियों के बैंक खातों से पैसे निकालने के लिए किए गए प्रयास हैं। इसलिए, अपने आप को बैंकिंग धोखाधड़ी से सुरक्षित रखें और सोशल इंजीनियरिंग धोखाधड़ी से बचने के तरीके सीखें।

फ़िशिंग:

• फ़िशिंग एक प्रकार का सोशल इंजीनियरिंग हमला है जिसका उपयोग अक्सर उपयोगकर्ता के डेटा, जिसमें लॉगिन क्रेडेंशियल और क्रेडिट कार्ड नंबर शामिल हैं, की चोरी करने के लिए किया जाता है।

विशिंग:

• विशिंग भी एक प्रकार का सोशल इंजीनियरिंग हमला है, जिसमें साइबर क्राइम करने वाला व्यक्ति फोन पर ग्राहक से संपर्क करता है, किसी व्यक्ति को प्राधिकारप्राप्त व्यक्ति के रूप में प्रस्तुत करता है। विशिंग, फ़िशिंग के ही समान है, लेकिन इसमें हमले को ई-मेल की बजाय फोन द्वारा प्रसारित किया जाता है।

सुरक्षा टिप्स:

1. किसी भी कॉलर से बहुत सतर्क रह कर बात करें, जो फोन / ई-मेल पर लॉग-इन जानकारी साझा करने के लिए कहता है।

2. यदि कोई कॉलर खाता डेटा या व्यक्तिगत पहचान योग्य जानकारी प्रदान करने के लिए कहता है, तो ऐसा करने से मना करें।

3. अज्ञात स्रोत से प्राप्त किसी भी मेल अटैचमेंट को डाउनलोड और एक्जिक्यूट न करें।

4. अज्ञात / अवैध स्रोत के साथ खाते के विवरण साझा न करें या धनराशि अंतरित न करें।

5. किसी भी गोपनीय निजी जानकारी की मांग करता हुआ और बैंक से आया हुआ होने का दावा करने वाले ई-मेल / एसएमएस का जवाब न दें।

6. छद्म रूपित या संदिग्ध ई-मेल या किसी भी संदिग्ध कॉल की रिपोर्ट करें।

7. अद्यतन और लाइसेंस प्राप्त एंटी-वायरस सॉफ़्टवेयर का ही उपयोग करें।

8. इंटरनेट पर धोखाधड़ी की गतिविधियों के प्रति सतर्क रहें।

यदि आपको केवाईसी अपडेशन से संबंधित एसएमएस प्राप्त होता है, तो कृपया उसका जवाब न दें। यह धोखाधड़ीपूर्ण हो सकता है। जालसाज आम तौर पर एसएमएस लिंक के माध्यम से जन्म दिनांक, मोबाइल नंबर, ई-मेल आईडी मांगते हैं। हम आपसे निवेदन करते हैं कि ऐसी कोई भी जानकारी न दें। बैंक कभी भी इस तरह की कोई जानकारी नहीं मांगता।

कृते मुख्य सूचना सुरक्षा अधिकारी

बैंक ऑफ महाराष्ट्र

****