

स्मिशिंग म्हणजे काय?

हा फिशिंगचा एक प्रकार आहे जेव्हा फसवणूक करणारी व्यक्ती कुणालाही फसवणूकीचे एसएमएस अलर्ट द्वारे त्यांची खाजगी माहिती देण्यासाठी फसवण्याचा प्रयत्न करते.

जसे की यामध्ये ईमेल ऐवजी टेक्स्ट मेसेज / एसएमएस / फोन नंबरचा समावेश असतो, जो एक विश्वासार्ह स्रोताकडून आल्याचे समजले जाते. तुमची केवायसी अपडेट करणे, तुमचे डेबिट / क्रेडिट कार्ड रिवॉर्ड पॉइंट्स रीडीम करणे इत्यादी साठी तुम्हाला फसवले जाते. ऑनलाईन पासवर्ड, ओटीपी इत्यादी सारखी तुमची वैयक्तिक माहिती शेयर करण्यास तुम्हाला प्रवृत्त करण्यासाठी सोशल इंजीनियरिंगचे घटक वापरतात.

सावध रहा!!!

- कोणत्याही अनोळखी व्यक्तीसोबत तुमचा पिन, पासवर्ड, कार्ड क्रमांक, सीव्हीव्ही क्रमांक, ओटीपी इत्यादी शेयर करू नका, मग भलेही तो/ती बँक कर्मचारी असल्याचा दावा करत असेल. बँक कधीही कोणतीही महत्त्वाची माहिती विचारणार नाही.
- तुमच्या बँक खात्यात पैसे जमा करण्याचे आश्वासन देत असले तरीही वैयक्तिक किंवा आर्थिक तपशीलांची मागणी करणाऱ्या अपरिचित स्रोतांकडून आलेल्या मेसेजेसना उत्तर देऊ नका.
- मेसेज पाठवणाऱ्या व्यक्तीला तुम्ही ओळखत नाही तोपर्यंत तुमच्या फोनवर आलेल्या लिंक्सवर क्लिक करू नका. मेसेजचा खरेपणा तपासा, जरी तो परिचित व्यक्तीकडून आलेला असेल.
- टेक्स्ट मेसेजने पाठवलेल्या लिंक द्वारे कधीही ॲप्स इंस्टॉल करू नका. तुमच्या द्वारे तुमच्या डिवाइसमध्ये इंस्टॉल केलेले कोणतेही ॲप्स थेट अधिकृत ॲप स्टोरमधून आलेले पाहिजे.

एसएमएसिंगद्वारे ओळख चोरी होण्याचे तुम्ही बळी पडत नाही याची खात्री करण्यासाठी सावधगिरी बाळगा.

सायबर फसवणूक झाल्यास तात्काळ तक्रार करा:

सायबर फसवणूकीचा बळी पडल्यास त्वरित कारवाई करा. राष्ट्रीय सायबर गुन्हे हेल्पलाइन 1930 वर संपर्कसाधा आणि

<https://cybercrime.gov.in/> या संकेतस्थळावर तक्रार नोंदवा. तसेच, तुम्ही Sancharsaathi Portal वरूनही तक्रार दाखल करू शकता.

वेळेवर तक्रार केल्यास पुढील फसवणूक टाळता येते आणि इतरांनाही सतर्ककरता येते.