शीर्षक:
मोबाइल बैंकिंग मालवेयर: सोवा एंड्रॉइड ट्रोजन

प्रिय बहुमूल्य ग्राहकों,

यह मालवेयर नकली एंड्रॉइड एप्लिकेशन के भीतर खुद को छुपाता है जो उपयोगकर्ताओं को इंस्टॉल करने में धोखा देने के लिए क्रोम, अमेज़ॅन और एनएफटी (गैर-परिवर्तनीय टोकन) प्लेटफॉर्म जैसे कुछ प्रसिद्ध वैध ऐप के लोगो के साथ दिखाई देते है। जब उपयोगकर्ता अपने नेट बैंकिंग ऐप में लॉग इन करते हैं और अपने बैंक खातों तक पहुंचते हैं तब यह मालवेयर क्रेडेंशियल्स को कैप्चर करता है।

मालवेयर निम्नलिखित कार्य करने में सक्षम है:

- कीस्ट्रोक्स प्राप्त करना
- कुकीज़ चोरी करना
- मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) टोकन को इंटरसेप्ट करना
- वेबकैम से स्क्रीनशॉट लेना और वीडियो रिकॉर्ड करना
- एंड्रॉइड एक्सेसिबिलिटी सेवा का उपयोग करके स्क्रीन क्लिक, स्वाइप आदि जैसे कार्य करना
- कॉपी/पेस्ट
- अनेक ऐप्स में झूठे आवरण जोड़ना
- 200 से अधिक बैंकिंग और भुगतान ऐप्स का अनुकरण करना

सर्वोत्तम कार्यप्रणाली और अनुशंषाएं:
1. आधिकारिक ऐप स्टोर (एंड्रॉइड के लिए प्लेस्टोर और आईओएस के लिए ऐप स्टोर) से ऐप्स डाउनलोड करें।
2. एंड्रॉइड डिवाइस विक्रेताओं से उपलब्ध होने पर एंड्रॉइड अपडेट और पैच इंस्टॉल करें।
3. नवीनतम एंटी-मालवेयर और एंटी-स्पाइवेयर सॉफ़्टवेयर इंस्टॉल करें और उसे रखे रहें।
4. संदिग्ध नंबरों से सावधान रहें जो वास्तविक मोबाइल फोन नंबरों की तरह नहीं दिखते हैं। बैंकों से प्राप्त वास्तविक एसएमएस संदेशों में आमतौर पर प्रेषक सूचना फील्ड में फोन नंबर की बजाय प्रेषक आईडी (बैंक का संक्षिप्त नाम मिलकर) होता है।
5. केवल उन यूआरएल पर क्लिक करें जो वेबसाइट डोमेन को स्पष्ट रूप से इंगित करते हैं।
6. कोई भी संवेदनशील जानकारी प्रदान करने से पहले, ब्राउज़र के एड्रेस बार में ग्रीन लॉक की जांच करके वैध एन्क्रिप्शन प्रमाणपत्रों की जांच करें।

धोखाधड़ी की सूचना तुरंत अपनी शाखा को दें या हमारे टोल फ्री नंबर 1800 103 1906 पर कॉल करें।

अपनी शाखा में कॉल करने के लिए, पासबुक या बैंक की वेबसाइट (https://bankofindia.co.in → हम तक पहुँचें → शाखाएँ) पर उपलब्ध नंबरों का उपयोग करें।

साइबर धोखाधड़ी की रिपोर्ट भारत सरकार के पोर्टल - https://cybercrime.gov.in/ पर अथवा 1930 पर कॉल करें।

आदर एवं आभार सहित /Thanks & Regards,

बैंक ऑफ़ इंडिया Bank of India BOI

सूचना सुरक्षा टीम