घर बैठे ही कैसे लुट जाते हैं आप ऑन लाई धोखाधड़ी से

जैसे-जैसे डिजिटल मनी लेनदेन बढ़ता है, ऑनलाइन बैंकिंग धोखाधड़ी के मामले भी बढ़े हैं। स्कैमर्स आम व्यक्तियों को धोखा देने के लिए विभिन्न तरीकों का उपयोग करते हैं। पेटीएम या गूगल पे के माध्यम से पैसे की मांग करना – यूपीआई-आधारित भुगतान के तरीकों में से प्रमुख एक है जिसके जरिए हैकर्स फ्रॉड को अंजाम देते हैं। सांकेतिक चित्र (फोटो क्रेडिट: razorpay) एक UPI फ्रॉड के मामले में, धोखेबाज एक आम आदमी के मोबाइल डिवाइस तक रिमोट एक्सेस प्राप्त करने का प्रयास करते हैं और वे बैंक का लेनदेन कर सकते हैं।

हम यहाँ बताने जा रहे हैं है कि कैसे इन के तौर-तरीकों को जानकर इस तरह के फ्रॉड का शिकार होने से आप खुद को बचा सकते हैं। फ्रॉडस्टर्स ग्राहकों को Google Play Store या Apple App Store से AnyDesk या TeamViewer जैसे ऐप डाउनलोड करने का लालच देते हैं। ये ऐप अन्य उपयोगकर्ताओं को आपके मोबाइल डिवाइस का रिमोट एक्सेस प्रदान करने में मदद करते हैं। एक बार जब कोई उपयोगकर्ता अपने स्मार्टफ़ोन पर ऐसे ऐप डाउनलोड करता है, तो ग्राहक के मोबाइल / डिवाइस पर एक 9-अंकीय संख्या (ऐप कोड) जनरेट हो जाती है। फ्रॉडस्टर फिर ग्राहक को उसके साथ इस कोड को साझा करने के लिए कहता है।

इस 9-अंकीय संख्या का उपयोग फ्रॉडस्टर द्वारा उसके मोबाइल डिवाइस पर ऐप कोड के रूप में किया जाता है। फिर वह ग्राहक को कुछ अनुमतियाँ प्रदान करने के लिए कहता है जो कि अन्य ऐप्स का उपयोग करते समय आवश्यक होती हैं। जैसे ही उपयोगकर्ता अनुमति देता है, जालसाज़ ग्राहक की डिवाइस का एक्सेस प्राप्त करता है और उसके मोबाइल फोन को आराम से ऑपरेट करना शुरू कर देता है। इस तरह, घोटालेबाज (फ्रॉडस्टर) को ग्राहक से मोबाइल बैंकिंग ऐप क्रेडेंशियल्स मिलते हैं और पहले से इंस्टॉल किए गए मोबाइल ऐप के माध्यम से ग्राहक के मोबाइल डिवाइस पर लेनदेन करना शुरू करते हैं।

साभार- https://yourstory.com/से