बैंकिंग साइबर धोखाधड़ी से कैसे बचें?

1. क्या एटीएम से पैसा निकालने के लिए किसी अंजान व्यक्ति की सहायता लेनी चाहिए?

नहीं। यदि आपने एटीएम कार्ड अंजान व्यक्ति को दिया तो वह आपका एटीएम कार्ड धोखे से अपने पास रख लेगा। उसके बाद आपके एटीएम कार्ड और एटीएम पिन का प्रयोग करके आपके बैंक खाते से पैसा निकाल लेगा।

2. क्या .APK (.एपीके) फ़ाइल को डाउनलोड एवं इंस्टॉल करना चाहिए?

नहीं। मैसेज/ईमेल/व्हाट्सएप/टेलीग्राम/लिंक इत्यादि से प्राप्त .APK (.एपीके) फाइल को डाउनलोड एवं इंस्टॉल न करें अन्यथा आपका मोबाइल फोन हैक हो सकता है। हमेशा अधिकृत प्ले स्टोर/ऐप स्टोर से ही ऐप्स इंस्टॉल करें।

3. क्या एटीएम पिन, यूपीआई पिन, पासवर्ड, ओटीपी, कार्ड नंबर, एक्सपायरी तिथि, सीवीवी को फोन पर साझा करना चाहिए?

नहीं। यदि आपने साझा किया तो साइबर धोखाधड़ी का शिकार हो सकते हैं।

4. क्या अंजान लिंक पर क्लिक करना चाहिए?

नहीं। अंजान लिंक पर क्लिक न करें।

5. क्या अपने बैंक खाते में पैसा मंगाने के लिए यूपीआई पिन की आवश्यकता होती है?

नहीं। यूपीआई ट्रांजैक्शन पिन का उपयोग खाते से पैसा निकालने के लिए किया जाता है। खाते में पैसा प्राप्त करने के लिए यूपीआई पिन की आवश्यकता नहीं होती है।

6. क्या फोन/मैसेज/ईमेल/सोशल मीडिया/लिंक इत्यादि के माध्यम से अपने गोपनीय व्यक्तिगत और वित्तीय विवरण जैसे आधार नंबर, पैन नंबर, ओटीपी, डेबिट/क्रेडिट कार्ड नंबर, एक्सपायरी तिथि, सीवीवी, ऑनलाइन बैंकिंग पासवर्ड, पिन इत्यादि को साझा करना चाहिए?

नहीं। यदि आपने उपरोक्त विवरण साझा किया तो आपके साथ साइबर धोखाधड़ी हो सकती है।

7. क्या अपने मोबाइल फोन में एनीडेस्क अथवा टीम व्यूअर क्विक सपोर्ट ऐप इंस्टॉल करना चाहिए?

नहीं। यदि आप इस ऐप को इन्स्टाल करते हैं और ऐप में दिया गया 9 नंबर का कोड किसी को बताते हैं तो वह आपका मोबाइल फोन हैक कर लेगा और बैंक खाते की जानकारी लेकर आपके खाते से पैसा निकाल लेगा।

8. यदि आपको सीबीआई, ईडी, पुलिस, आरबीआई, इनकम टैक्स इत्यादि के नाम पर कोई वीडियो कॉल आती है तो क्या करना चाहिए?

डरिए मत! इसकी शिकायत नजदीकी पुलिस स्टेशन पर अथवा https://cybercrime.gov.in पर कीजिए।

9. अंजान नंबर से आने वाली विडियो कॉल रिसीव करनी चाहिए कि नहीं?

नहीं। क्योंकि अंजान नंबर से विडियो कॉल रिसीव करने पर आप ब्लैकमेल और साइबर धोखाधड़ी का शिकार हो सकते हैं।

10. क्या किसी अंजान व्हाट्सएप अथवा टेलीग्राम ग्रुप से जुड़ना चाहिए?

नहीं। अगर आप ऐसे ग्रुप में जुड़ेंगे तो आपके साथ साइबर धोखाधड़ी हो सकती है।

11. बैंक केवाईसी कैसे/ कहाँ जाकर अपडेट करें?

बैंक की शाखा में, बैंक मित्र/ बीसी लोकेशन पर, इंटरनेट बैंकिंग/ मोबाइल बैंकिंग से अथवा बैंक की आधिकारिक वेबसाइट पर जाकर वीडियो केवाईसी के माध्यम से अपना केवाईसी अपडेट करा सकते हैं।

12. क्या अपने बैंक खाते का प्रयोग दूसरे व्यक्ति का पैसा मंगाने के लिए किया जाना चाहिए?

नहीं। यदि कोई आपसे आपका बैंक खाता नंबर अपने पैसे मंगाने के लिए माँगता है तो उसे साफ मना कर दें।

13. साइबर धोखाधड़ी की शिकायत कहाँ करें?

राष्ट्रीय साइबर अपराध रिपोर्टिंग हेल्पलाइन नंबर 1930 पर तुरंत कॉल करें अथवा **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल** https://cybercrime.gov.in पर रिपोर्ट करें।

14. क्या साइबर धोखाधड़ी की शिकायत अपने बैंक में भी करनी चाहिए?

हाँ। इसके बारे में अपने बैंक को जरूर सूचित करें ताकि ऑनलाइन बैंकिंग सुविधाओं को ब्लॉक किया जा सके।

15. अपने बैंक का टोल फ्री नंबर कैसे पता करें?

टोल फ्री नंबर बैंक के पासबुक, डेबिट कार्ड/क्रेडिट कार्ड, और बैंक की आधिकारिक वेबसाइट/ऐप पर उपलब्ध होता है।

16. साइबर सुरक्षा से संबंधित नवीनतम जानकारी कहाँ से प्राप्त करें?

भारतीय साइबर अपराध समन्वय केन्द्र, गृह मंत्रालय के आधिकारिक सोशल मीडिया अकाउंट **CyberDost** को फॉलो करें।

जागरूक रहें, साइबर सुरक्षित रहें!

सत्येन्द्र शर्मा, (मुख्य प्रबंधक- आई.टी.), पी.एन.बी. अध्ययन एवं नवोत्थान केंद्र: प्रधान कार्यालय

पंजाब नैशनल बैंक टोल फ्री नंबर: 1800 1800, 1800 2021 1800 180 2345 (क्रेडिट कार्ड के लिए)