राजस्थान ग्रामीण बैंक
RAJASTHAN GRAMIN BANK

केवाईसी अपडेट धोखाधडी

केवाईसी अपडेट के झाँसे में मत फँसो, बैलेंस को सुरक्षित रखो।।

KYC अपडेट धोखाधड़ी एक वित्तीय ठगी है जिसमें अपराधी बैंक अधिकारियों के रूप में ग्राहकों से कॉल, एसएमएस, व्हाट्सएप, ईमेल या सोशल मीडिया के माध्यम से संपर्क करते हैं। वे झूठा दावा करते हैं कि ग्राहक का KYC अधूरा है और खाता ब्लॉक होने से बचाने के लिए तुरंत कार्यवाही करने की आवश्यकता हैं।
इस धोखाधड़ी का मुख्य उद्देश्य ग्राहकों की संवेदनशील जानकारी चुराना होता है — जैसे बैंकिंग लॉगिन विवरण, ओटीपी, ATM कार्ड जानकारी, UPI पिन — या उन्हें रिमोट एक्सेस एप्लिकेशन इंस्टॉल करने के लिए मजबूर करना।

केवाईसी अपडेट फ्रॉड कैसे काम करता है?

स्टेप 1: ग्राहक को इस तरह का SMS प्राप्त होता है
- "आपका खाता ब्लाक हो जाएगा अगर अभी अपडेट नहीं किया।तुरंत लिंक पर क्लिक करें"

स्टेप 2: नकली बैंक प्रतिनिधि का कॉल
- धोखेबाज़ खुद को बैंक अधिकारी बताकर ग्राहक को कॉल करता है।
- वह तुरंत कार्यवाही करने का दबाव और डर पैदा करता

स्टेप 3: संवेदनशील जानकारी की माँग
- OTP, ATM कार्ड विवरण, UPI PIN या बैंकिंग क्रेडेंशियल्स साझा करने को कहा जाता है।
- कभी-कभी रिमोट एक्सेस ऐप इंस्टॉल करने के लिए भी मजबूर किया जाता है।

स्टेप 4: खाता असुरक्षित (Account Compromised)
- धोखेबाज़ बैंकिंग जानकारी ले लेते हैं।
- वे अनाधिकृत लेन-देन करके खाते से धन निकाल लेते हैं।

सुरक्षित रहने के उपाय

- ☑ केवल आधिकारिक बैंक चैनलों के माध्यम से ही KYC अपडेट करें।
- ☑ संदेह होने पर बैंक शाखा से संपर्क करें |

- ☑ कभी भी किसी के कहने पर रिमोट एक्सेस ऐप इंस्टॉल न करें।
- ☑ OTP, पासवर्ड, PIN, CVV या UPI PIN कभी साझा न करें।

- ☑ बैंक कभी भी फ़ोन पर आपके क्रेडेंशियल्स (OTP, पासवर्ड, PIN, CVV, UPI PIN आदि) नहीं माँगता।
- ☑ किसी भी कार्यवाही से पहले हमेशा यह सुनिश्चित करें कि SMS, ईमेल या कॉल आधिकारिक बैंक स्रोत से ही है।

रिपोर्ट

ऑनलाइन धोखाधड़ी की सूचना दें	संदिग्ध ईमेल या कॉल की शिकायत दर्ज करें
cybercrime.gov.in पर सूचित करें । 1930 – साइबर क्राइम हेल्पलाइन नंबर पर कॉल करें।	sancharsathi.gov.in और cybercrime.gov.in पर शिकायत दर्ज करें।