



Reg: Cautions against frauds in the name of KYC updation.

केवाईसी अपडेशन (Re-KYC) के नाम पर ग्राहकों के धोखाधड़ी का शिकार होने की लगातार घटनाओं/रिपोर्टों के मद्देनजर, एक बार फिर बैंक, ग्राहकों से, नुकसान को रोकने और ऐसी दुर्भावनापूर्ण प्रथाओं से खुद को सुरक्षित रखने के लिए सावधानी बरतने और उचित देखभाल करने का आग्रह करता है।

In the wake of continuing incidents/ reports of customers falling prey to frauds being perpetrated in the name of KYC updation, RBI once again urges the members of public to exercise caution and due care to prevent loss and safeguard themselves from such malicious practices.

इस तरह की धोखाधड़ी के तौर-तरीकों में आम तौर पर ग्राहकों को फोन कॉल/एसएमएस/ईमेल सहित अनचाहे संपर्क प्राप्त करना शामिल होता है, जिसके माध्यम से उन्हें व्यक्तिगत जानकारी, खाता/लॉगिन विवरण प्रकट करने, या संदेशों में दिए गए लिंक के माध्यम से अनधिकृत या असत्यापित ऐप्स इंस्टॉल करने के लिए प्रेरित किया जाता है। इस तरह के संपर्क अक्सर गलत तात्कालिकता पैदा करने और ग्राहक द्वारा अनुपालन करने में विफल रहने पर खाता फ्रीज/अवरुद्ध/बंद करने की धमकी देने की रणनीति अपनाते हैं। जब ग्राहक आवश्यक व्यक्तिगत या लॉगिन विवरण साझा करते हैं, तो धोखेबाज उनके खातों तक अनधिकृत पहुंच प्राप्त कर लेते हैं और धोखाधड़ी गतिविधियों में संलग्न हो जाते हैं।

The modus operandi for such frauds usually involves customers receiving unsolicited communications, including phone calls/SMS/emails, through which they are manipulated into revealing personal information, account/login details, or installing unauthorized or unverified apps through links provided in the messages. Such communications often employ tactics of creating a false urgency and threatening of account freezing/blocking/closure, if the customer fails to comply. When customers share essential personal or login details, fraudsters gain unauthorized access to their accounts and engage in fraudulent activities.

अपनी सुरक्षा के लिए जनता को निम्नलिखित उपाय अपनाने के लिए प्रोत्साहित किया जाता है:-

In order to safeguard themselves, members of public are encouraged to adopt the following measures:-

क्या करें (Do's):

- केवाईसी अपडेशन के लिए कोई अनुरोध प्राप्त होने की स्थिति में, पुष्टि/सहायता के लिए सीधे बैंक से संपर्क करें।
- बैंक संपर्क नंबर/ग्राहक-सेवा फोन नंबर केवल उसकी आधिकारिक वेबसाइट/स्रोतों के माध्यम से प्राप्त करें। किसी भी साइबर धोखाधड़ी की घटना होने पर तुरंत अपने बैंक/वित्तीय संस्थान को सूचित करें।



- केवाईसी विवरण अपडेट करने के लिए उपलब्ध तरीकों/विकल्पों का पता लगाने के लिए उनकी बैंक शाखा से पूछताछ करें। केवाईसी के अपडेशन/आवधिक अपडेशन के लिए आवश्यकताओं और चैनलों पर अधिक विवरण या अतिरिक्त जानकारी के लिए, Paragraph 38 of the RBI's Master Direction on KYC, को पढ़ें।
- In the event of receiving any request for KYC updation, directly contact their bank/ financial institution for confirmation/ assistance.
- Obtain contact number/ customer care phone number of the bank/ financial institution only through its official website/ sources.
- Inform their bank/ financial institution immediately in case of any cyber fraud incident.
- Enquire with their bank branch to ascertain available modes/ options for updating KYC details.
- For more details or additional information on the requirements and channels for updation/periodic updation of KYC, please read paragraph 38 of the RBI Master Direction on KYC.

क्या नहीं करें (Dont's)

- खाता लॉगिन क्रेडेंशियल, कार्ड की जानकारी, पिन, पासवर्ड, ओटीपी किसी के साथ साझा न करें।
- केवाईसी दस्तावेज़ या केवाईसी दस्तावेज़ों की प्रतियां अज्ञात या अज्ञात व्यक्तियों के साथ साझा न करें।
- असत्यापित/अनधिकृत वेबसाइटों या एप्लिकेशन के माध्यम से कोई भी संवेदनशील डेटा/जानकारी साझा न करें।
- मोबाइल या ईमेल पर प्राप्त संदिग्ध या असत्यापित लिंक पर क्लिक न करें।
- Do not share account login credentials, card information, PINs, passwords, OTPs with anyone.
- Do not share KYC documents or copies of KYC documents with unknown or unidentified individuals or organizations.
- Do not share any sensitive data/ information through unverified/unauthorized websites or applications.
- Do not click on suspicious or unverified links received in mobile or email.

सहायक महाप्रबंधक,