



# दि. कराड अर्बन को-ऑप. बँक लि., कराड

(शेड्युल्ड बँक)

## सायबर सुरक्षा जागरूकता - मार्गदर्शिका

सतर्क रहा 2026

आपल्या पैशांचे रक्षण करा, आपली माहिती सुरक्षित तर पैसे सुरक्षित

डिजिटल बँकिंग अत्यंत सोयीस्कर आहे, परंतु सायबर गुन्हेगार लोकांच्या भावनांशी खेळण्यासाठी नवनवीन आणि अत्याधुनिक पद्धती (Social Engineering) वापरतात. एआय (AI) आणि स्वयंचलित तंत्रज्ञानाचा वापर करून होणाऱ्या फसवणुकी पासून स्वतःचा बचाव करण्यासाठी या मार्गदर्शिकेचे पालन करा.

### काय करावे (Do's)

- ✓ **UPI लाभार्थीची पडताळणी करा:**  
तुमचा UPI PIN टाकण्यापूर्वी स्क्रीनवर दिसणारे पैसे मिळवणाऱ्याचे नाव आणि रक्कमेची नेहमी दोनवेळा खात्री करा.
- ✓ **अॅप अधिकृत स्टोअरवरूनच डाउनलोड करा:**  
बँकिंगचे कोणतेही ॲप्लिकेशन नेहमी केवळ गुगल प्ले स्टोअर (Google Play) किंवा ॲपल ॲप स्टोअर (Apple App Store) वरूनच डाउनलोड करा.
- ✓ **डिव्हाइस लॉक आणि MFA लागू करा:**  
बायोमेट्रिक्स (फिंगरप्रिंट/फेस आयडी) किंवा मजबूत पिन वापरून आपला फोन सुरक्षित ठेवा. बँक खात्यांवर मल्टी-फॅक्टर ऑथेंटिकेशन (MFA) सक्रिय करा
- ✓ **यूआरएल (URL) आणि सुरक्षिततेची खात्री करा:**  
नेट-बँकिंग लॉगिन करण्यापूर्वी वेबसाइटचा पत्ता स्पष्टपणे <https://> ने सुरु होतोय की नाही आणि तिथे 'लॉक' (कुलूप) चे चिन्ह आहे की नाही ते तपासा.
- ✓ **संशयास्पद व्यवहारांची त्वरित तक्रार करा:**  
तुमच्या खात्याचे व्यवहार एसएमएस (SMS) आणि स्टेटमेंटद्वारे नियमित तपासा. कोणताही अनोळखी व्यवहार दिसल्यास बँकेला ताबडतोब कळवा.

### काय करू नये (Don'ts)

- ✗ **गोपनीय माहिती कधीही शेअर करू नका:**  
तुमचा OTP, CVV, पासवर्ड किंवा पिन कधीही कोणाशीही शेअर करू नका — अगदी बँकेचे अधिकारी सांगणाऱ्यांसोबतही नाही.
- ✗ **अनोळखी लिंकवर क्लिक करू नये:**  
अनोळखी नंबरवरून एसएमएस, ईमेल किंवा व्हॉट्सअॅपवर आलेल्या कोणत्याही संशयास्पद लिंकवर क्लिक करू नका किंवा अटॅचमेंट उघडू नका.
- ✗ **पब्लिक वाय-फाय वर व्यवहार टाळा:**  
सार्वजनिक ठिकाणी (उदा. रेल्वे स्टेशन, कॅफे) मिळणाऱ्या मोफत किंवा अनएन्क्रिप्टेड पब्लिक वाय-फाय (Public Wi-Fi) वरून बँक व्यवहार किंवा खरेदी करू नका.
- ✗ **“डिजिटल अटक” (Digital Arrest) च्या धमक्यांना बळी पडू नका:**  
पोलीस किंवा सीबीआय (CBI) कधीही व्हॉट्सअॅप किंवा व्हिडिओ कॉलवर कोणालाही “डिजिटल अटक” करत नाहीत. घाबरून कोणालाही पैसे पाठवू नका.
- ✗ **अनोळखी UPI पेमेंट विनंत्या स्वीकारू नका:**  
गुगल पे, फोनपे किंवा पेटीएमवर “बक्षीस मिळवण्यासाठी” आलेली कोणतीही अनोळखी कलेक्ट (Collect) रिक्वेस्ट मंजूर करू नका किंवा पेमेंट लिंक क्लिक करू नका.



# दि. कराड अर्बन को-ऑप. बँक लि., कराड

(शेड्युल्ड बँक)

## सायबर सुरक्षा जागरूकता - मार्गदर्शिका

आपल्या पैशांचे रक्षण करा, आपली माहिती सुरक्षित तर पैसे सुरक्षित

सतर्क रहा 2026

### नवीनतम सायबर धोके आणि फसवणुकीच्या पद्धती

| धोक्याचा प्रकार                                         | फसवणुकीची पद्धत                                                                                                                                                                                                | महत्त्वाची खबरदारी                                                                                                                                           |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AI-आधारित डीपफेक्स</b><br>उच्च जोखीम                 | सायबर भामटे आर्टिफिशियल इंटेलिजन्स (AI) चा वापर करून बँक अधिकारी, कुटुंबातील सदस्य किंवा सहकाऱ्यांचा हुबेहूब आवाज किंवा व्हिडिओ तयार करतात आणि तातडीने पैसे ट्रान्सफर करण्याची मागणी करतात.                    | पैसे पाठवण्यापूर्वी दुसऱ्या खात्रीशीर मार्गाने (उदा. नेहमीच्या नंबरवर फोन करून) पडताळणी करा. व्हिडिओ किंवा ऑडिओ कॉलवर विश्वास ठेवून घाईघाईत व्यवहार करू नका. |
| <b>“डिजिटल अटक” (Digital Arrest)</b><br>अति-गंभीर जोखीम | गुन्हेगार व्हिडिओ कॉलवर पोलीस किंवा सीबीआय अधिकारी असल्याचे भासवतात. उदा, तुमच्या पार्सलमध्ये बेकायदेशीर ड्रग्स सापडले आहेत अशी खोटी भीती दाखवून तुरुंगात टाकण्याची धमकी देतात आणि सेटलमेंटसाठी पैसे उकळतात इ. | खरे पोलीस किंवा सीबीआय अधिकारी कधीही व्हिडिओ कॉलवर चौकशी किंवा अटक करत नाहीत. असा फोन आल्यास त्वरित कट करा आणि घाबरू नका.                                    |
| <b>क्यूआर कोड आणि क्विशिंग</b><br>मध्यम जोखीम           | फसवणूक करणारे ईमेल, व्हॉट्सअप किंवा खोट्या पोस्टर्सवर बनावट क्यूआर (QR) कोड पाठवतात. हे कोड स्पॅम फिल्टर्स बायपास करून थेट वापरकर्त्यापर्यंत पोहोचतात.                                                         | लक्षात ठेवा, क्यूआर कोड नेहमी केवळ पैसे पाठवण्यासाठी स्कॅन केला जातो, पैसे मिळवण्यासाठी किंवा केवायसी (KYC) अपडेट करण्यासाठी कधीही नाही.                     |
| <b>खोट्या सर्च इंजिन जाहिराती</b><br>मध्यम जोखीम        | गुन्हेगार गुगल किंवा बिंगवर बँकेच्या मूळ वेबसाइटसारखीच दिसणारी हुबेहूब बनावट जाहिरात लिंक (Sponsored Link) तयार करतात. त्यावर क्लिक केल्यास युजर्सचा पासवर्ड चोरीला जातो.                                      | सर्च रिझल्टमध्ये "Sponsored" किंवा "Ad" लिहिलेल्या लिंकवर क्लिक करणे टाळा. नेहमी बँकेचा अधिकृत वेब पता ब्राउझरमध्ये स्वतः टाईप करा.                          |

### स्मार्ट बँकिंगसाठी महत्त्वाच्या सूक्ष्म टिप्स

#### १. व्यवहारांची मर्यादा सेट करा:

तुमच्या मोबाईल बँकिंग ॲपचा वापर करत असताना रोजच्या व्यवहारांची कमाल मर्यादा (Daily Limit) निश्चित करा आणि गरज नसेल तेव्हा आंतरराष्ट्रीय कार्ड वापर बंद ठेवा.

#### २. दहा मिनिटांचा नियम लागू करा:

जर एखाद्या फोन किंवा मेसेजमुळे मनात भीती, घाई किंवा घबराट निर्माण होत असेल, तर स्वतःला १० मिनिटे थांबवा, शांत व्हा आणि विश्वासू मित्राचा किंवा बँकेचा सल्ला घ्या.

#### ३. सेव्ह केलेली माहिती हटवा:

ब्राउझर किंवा ऑनलाईन शॉपिंग ॲप्समध्ये सेव्ह केलेले नेट-बँकिंगचे पासवर्ड आणि क्रेडिट/डेबिट कार्डचे तपशील नियमितपणे डिलीट करा.

फसवणूक झाली आहे? त्वरित 'सुवर्ण तासात' (Golden Hour : 1 Hour) पाऊल उचला! 📞 डायल करा: १९३० किंवा त्वरित [cybercrime.gov.in](https://cybercrime.gov.in) वर तक्रार करा. सायबर फ्रॉड संबंधित रिफंड रिक्वेस्ट [mrm-ncrp.mha.gov.in](https://mrm-ncrp.mha.gov.in) या पोर्टलवर रजिस्टर करा.