

भीम बड़ौदा पे

क्या करें :-

- भीम बड़ौदा पे यूपीआई एप्लीकेशन को वैध प्लेटफार्म अर्थात गूगल प्ले स्टोर आदि के माध्यम से डाउनलोड करें.
- अपनी मूल शाखा / नेट बैंकिंग/ बॉब एटीएम/ यूपीआई के माध्यम से मोबाइल बैंकिंग के लिए पंजीकरण करें.
- यह सुनिश्चित करें कि आप लॉग इन और यूपीआई लेनदेन की शुरुआत गोपनीय तरीके से कर रहे हैं.
- लेन देन पूरा करने के पश्चात यह सुनिश्चित करें कि आपने सफलतापूर्वक एप्लीकेशन से लॉग आउट किया है.
- प्रत्येक लेनदेन के लिए, आपको आपके पंजीकृत मोबाइल नंबर पर एसएमएस अलर्ट प्राप्त होगा. यदि आप खाते में अनधिकृत यूपीआई लेनदेन पाते हैं, तो कृपया तत्काल इसकी सूचना अपनी शाखा को दें.
- किसी भी असफल लेनदेन के मामले में, कृपया हमारी वेबसाइट और एप्लीकेशन में प्रदान किए गए विभिन्न पदाधिकारियों को सूचना दें.
- अपने यूपीआई एप्लीकेशन पासवर्ड और यूपीआई पिन/ एम पिन को निरंतर बदलें.
- आपके मोबाइल बैंकिंग/ यूपीआई तक अनधिकृत इस्तेमाल की कोशिश के मामले में, अपने एटीएम/ इंटरनेट बैंकिंग/ आधार शाखा (या हमारे कॉल सेंटर से संपर्क करें) के माध्यम से तत्काल शिकायत दर्ज करें.
- आपका मोबाइल फोन खो जाने/ चोरी होने के मामले में, तत्काल मूल शाखा/ नेट बैंकिंग/ एटीएम/ संपर्क केंद्रों के माध्यम से अपना मोबाइल बैंकिंग पंजीकरण बंद करवाएं.
- आपके अनुरोध के बिना आपके मोबाइल बैंकिंग/ मोबाइल नंबर का पंजीकरण हटाने / निष्क्रिय करने के संबंध में या इस संबंध में आपको कॉल आता है, तो इसका आशय यह है कि कोई आपका डुप्लीकेट सिम प्राप्त करना चाह रहा है / आपके एम पिन / ओटीपी (वन टाइम पासवर्ड) आदि जैसे विवरण चुराना चाह रहा है, ऐसे मामलों में तत्काल अपनी मूल शाखा से संपर्क करें.

क्या ना करें:-

- कृपया अपना पासवर्ड किसी से भी साझा ना करें / अपने मोबाइल के हैंडसेट में स्टोर ना करें.
- अपना एप्लीकेशन पासवर्ड या यूपीआई पिन/ एम पिन दूसरों से छुपा कर दर्ज करें.
- अपने एप्लीकेशन/ यूपीआई पिन/ एम पिन को आसानी से अनुमान लगाये जाने योग्य न रखें. जैसे: 1111/2222/1234/ जन्म वर्ष, मोबाइल नंबर, टेलीफोन नंबर आदि.

- किसी दूसरे व्यक्ति के डिवाइस में यूपीआई एप्लीकेशन इंस्टॉल और प्रयोग ना करें.
- बैंक ऑफ बड़ौदा आपके यूपीआई / मोबाइल बैंकिंग पासवर्ड पूछने के लिए आपको कॉल या ईमेल नहीं भेजता. कोई कॉलर हमारे बैंक से / संपर्क केंद्र से कॉल करने का बहाना करे, तो ऐसे कॉलर से कृपया बातचीत ना करें क्योंकि वह धोखाधड़ी में शामिल है.
- अपने पंजीकृत सिम कार्ड और डेबिट कार्ड को एक-साथ ना रखें दोनों को एक साथ खोने का खतरा है और इससे किसी को भी आपके खाते तक पहुंचना आसान हो जायेगा.
- फिशिंग: - फिशिंग जिसे स्पूफिंग भी कहा जाता है, धोखाधड़ी के प्रयोजन से आधिकारिक प्रतीत होने वाली इलेक्ट्रॉनिक अधिसूचना या मैसेज द्वारा विश्वसनीय व्यक्ति या कारोबार का अहसास दिलाते हुए वास्तविक आवश्यकता दर्शाते हुए ठोंगी व्यक्ति द्वारा पासवर्ड और क्रेडिट कार्ड विवरण जैसी संवेदनशील जानकारी की धोखाधड़ी से प्राप्त किया जाता है. ईमेल यूजर को ऐसी वेबसाइट पर डायरेक्ट करता है, जहां उनसे उनकी व्यक्तिगत जानकारी, जैसे कि पासवर्ड और क्रेडिट कार्ड, सामाजिक सुरक्षा तथा बैंक खाता संख्या अपडेट करने को कहा जाता है, जो मूल संस्थान के पास पहले से ही मौजूद है.
- बैंक कर्मचारियों सहित किसी से भी अपना पिन साझा ना करें (बैंक को किसी भी समय आपका यूजर आईडी या पिन जानने की आवश्यकता नहीं है). अतः ऐसी सूचना मांगने के लिए आपके पास कोई पत्र/ ईमेल/ कॉल आता है, तो कृपया उन्हें अपना यूजर आईडी या पिन ना बताएं)