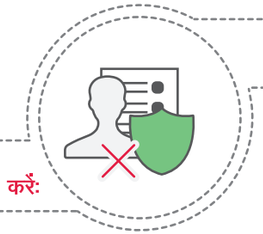
UPI और BHIM

क्या करें:

- UPI लेनदेन का रिकॉर्ड जरूर रखें
- यह सुनिश्चित करें कि कर्मचारियों को धोखाधड़ी से जुड़ी बातों की जानकारी हो
- किसी को पिन बताने, अकाउंट नंबर और दूसरी व्यक्तिगत जानकारियां बताने से धोखाधड़ी की भरपूर आशंका रहती है, ये जानकारियां साझा करने से बचें



क्या न करें:

- बायोमेट्रिक और M-Pin का विवरण (लिखकर या इलेक्ट्रॉनिक माध्यम में) कभी भी कहीं न रखें
- ग्राहकों की जानकारी की सुरक्षा में कभी ढिलाई न करें
- ग्राहक के विवरण की पुष्टि किए बिना फंड कलेक्ट करने का अनुरोध न करें

जागरूकता अभियान के साझेदार

Government of Telangana

नाबार्ड

NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

airtel Payments Bank

AXIS BANK

mastercard

Paytm Payments Bank

PayPal

VISA

Follow us

dsci_connect dsci.connect

dsci-security-council-of-India

Digital India
Power To Empower

Ministry of Electronics and Information Technology
Government of India

DIGITAL PAYMENT suraksha

A Joint Initiative of

DSCI PROMOTING DATA PROTECTION | Google

"Digital money will empower the poor"

- Narendra Modi
Prime Minister

डिजिटल भुगतान

#SaralBhiSecureBhi

इस पुस्तिका के माध्यम से आप जानेंगे कि किसी ग्राहक से डिजिटल भुगतान स्वीकार करते समय क्या करें और क्या न करें

www.dsci.in/digital-payment-suraksha

इसे स्कैन करें

आधार सक्षम भुगतान प्रणाली

क्या करें:

- यह सुनिश्चित करें कि POS या बायोमेट्रिक कैप्चर मशीन के साथ कोई छेड़छाड़ न हुई हो और केवल प्रमाणित मशीनें ही प्रयोग की जा रही हैं
- अपने POS को हमेशा अपग्रेड करके रखें और इसकी सुरक्षा का पूरा ध्यान रखें
- POS में जैसे ही कोई संदेहास्पद बात नजर आती है आप उसकी तत्काल रिपोर्ट करने की आदत डालें

क्या न करें:

- POS को खुले में या किसी असुरक्षित स्थान पर न लगाएं
- स्लिप या रिपोर्ट में कभी भी आधार की जानकारियां प्रिंट न करें
- आधार के ब्योरे – जैसे आधार नंबर, निजी जानकारियां, बायोमेट्रिक विवरण आदि इकट्ठा न करें

बुनियादी जरूरतें

क्या करें:

- जो भी कर्मचारी भुगतान सम्भालतें हों, उन्हें इससे जुड़े खतरों के बारे में अच्छे से प्रशिक्षित करें
- हमेशा ऐसे पेमेंट गेटवे का प्रयोग करें जो सुरक्षित हों, विश्वसनीय हों और जिनकी भली–भांति जांच की गई हो
- ऐप्स की प्रमाणिकता जांचने के लिए उसके लिंक का मिलान बैंक की वेबसाइट पर दिए गए ऐप्स के लिंक से करें
- यह सुनिश्चित करें कि जो POS या बायोमेट्रिक कैप्चर मशीनें प्रयोग की गई है वे प्रामाणिक हों, अपडेटेड हों और मशीनो से कोई छेड़छाड़ नहीं की गई हो
- लेनदेन से जुड़े लॉग्स और अलर्ट पर नजर रखें। यदि आपको इसमें कुछ भी संदिग्ध लगता है तो तत्काल इसकी सूचना संबंधित सर्विस प्रोवाइडर और पुलिस को दें

क्या न करें:

- अप्रमाणिक और असत्यापित स्रोतों से न तो ऐप्स इन्स्टॉल करें न कभी ऐसे ऐप्स का प्रयोग करें
- डिजिटल पेमेंट स्वीकारने के लिए कभी भी असुरक्षित ओपन वाई–फाई पॉइंट्स का प्रयोग न करें
- जिन उपकरणों का प्रयोग पेमेंट लेने के लिए करते हों उन्हें हमेशा अपनी निगरानी में रखें। उसे कहीं भी छोड़कर न जाएं न ही किसी अपरिचित के हवाले करें
- ग्राहकों की संवेदनशील जानकारियां जैसे बायोमेट्रिक, M-Pin, पासवर्ड आदि को किसी भी रूप में (लिखकर या इलेक्ट्रॉनिक माध्यम में) अपने पास न रखें

ऑनलाइन एवं मोबाइल बैंकिंग

क्या करें:

- हमेशा सुरक्षित और विश्वसनीय पेमेंट गेटवे का ही प्रयोग करें
- यह सुनिश्चित कर लें कि गेटवे के इंटीग्रेशन की भली–भांति जांच की गई हो
- ग्राहक ऑनलाइन या मोबाइल बैंकिंग का प्रयोग करके लेन–देन सुगमता से कर पा रहे हैं या नहीं, इस बात की नियमित तौर पर जांच करते रहें

क्या न करें:

- ग्राहकों से कभी भी उनके ऑनलाइन बैंकिंग से जुड़ी जानकारियां न मांगें
- भुगतान मॉड्यूल की सुरक्षा को कभी भी अनदेखा न करें
- धोखाधड़ी का कोई प्रयास हुआ हो तो उसको अनदेखा न करें। बैंक या संबंधित पेमेंट गेटवे को तत्काल रिपोर्ट करें

मोबाइल वॉलेट

क्या करें:

- वॉलेट से प्राप्त रकम का मिलान जरूर कर लें और लेन–देन के रेफरेंस नंबर को ट्रैक करते रहें
- नियमित तौर पर यह जांच करते रहें कि ग्राहक सुरक्षित और स्थिर QR कोड का प्रयोग करके लेन–देन कर पा रहे हैं
- संवेदनशील सूचनाएं भेजने से पहले एजेंट की आधिकारिक आईडी को सत्यापित कर लें

क्या न करें:

- ग्राहकों की संवेदनशील जानकारियां किसी भी स्वरूप में (चाहे लिखकर या इलेक्ट्रॉनिक माध्यम में) रखने से परहेज करें
- धोखाधड़ी के प्रयासों को अनदेखा न करें। संबंधित वॉलेट कंपनी को तत्काल सूचित करें
- ग्राहकों से आवश्यकता से अधिक जानकारी न मांगे

क्रेडिट और डेबिट कार्ड

क्या करें:

- कार्ड से किया जाने वाला लेन–देन हमेशा ग्राहक की नजरों के सामने करें
- POS को हमेशा अपग्रेड करके रखें और इसकी सुरक्षा का ध्यान रखें
- यह सुनिश्चित करें कि POS उपकरण के साथ कोई छेड़छाड़ न हुई हो। केवल प्रमाणित उपकरणों का ही प्रयोग करें

क्या न करें:

- POS उपकरण हमेशा अपनी निगरानी में रखें। इसे अपनी नजरों से ओझल न होने दें। अनधिकृत व्यक्तियों को POS उपकरण न छूने दें
- कार्ड का CVV या पिन कभी भी इकठ्ठा न करें
- ग्राहक के कार्ड का विवरण तब तक अपने पास न रखें जब तक कि इसकी आवश्यकता पूर्ण रूप से न हो