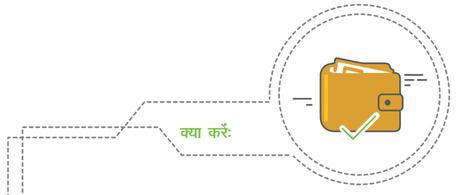
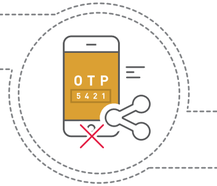
मोबाइल वॉलेट



क्या करें:

- प्रामाणिक वॉलेट ऐप्स को ही इन्स्टॉल करें और उसका सत्यापन भी करें
- फोन की सुरक्षा के लिए उसमें पिन डालकर रखें
- किसी भी लेन–देन से पहले यह पक्का कर लें कि आप जिसके साथ लेन–देन कर रहे हैं, आपने उस व्यक्ति का मोबाइल नंबर सही डाला है



क्या न करें:

- हर वॉलेट के लिए एक जैसा पासवर्ड न रखें
- ओपन वाई–फाई या किसी ऐसे डिवाइस का प्रयोग करके लेन–देन न करें जिसकी सुरक्षा को लेकर आप आश्वस्त नहीं हैं
- संदेहास्पद QR Code को अपने मोबाइल से स्कैन 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

छोटी सी पुस्तिका की सहायता से जानें, डिजिटल लेन–देन के दौरान क्या करें और क्या न करें

www.dsci.in/digital-payment-suraksha

इसे स्कैन करें

ऑनलाइन एवं मोबाइल बैंकिंग

क्या करें:

- किसी भी तरह के भुगतान के लिए हमेशा केवल सत्यापित और भरोसेमंद ब्राउजर एवं HTTPS द्वारा सुरक्षित वेबसाइट का ही प्रयोग करें
- समय–समय पर अपना पासवर्ड बदलते रहें। इस बात का यदि जरा सा भी शक हो कि आपका पासवर्ड गलत हाथों में पड़ गया है तो पासवर्ड को तत्काल बदल दें
- भुगतान या लेन–देन के लिए जिस भी ऐप्लीकेशन या ऐप (बैंक/पेमेंट बैंक/वॉलेट) का प्रयोग करते हैं उसे हमेशा अपडेट करते रहें

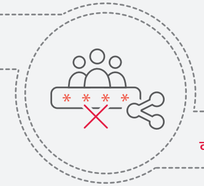
क्या न करें:

- लॉगिन से जुड़ी जानकारियां कभी भी अपने फोन में सेव न करें। ऐसे किसी किओस्क पर लॉगिन न करें जिसकी विश्वसनीयता को लेकर आप आश्वस्त न हों
- सार्वजनिक उपकरणों (उदाहरण के लिए किसी साइबर कैफे या ऑफिस का कंप्यूटर) या असुरक्षित और खुले नेटवर्क (ओपन वाईफाई) का प्रयोग करके कोई डिजिटल लेन–देन न करें
- अपना मोबाइल बैंकिंग पिन किसी के साथ भी साझा न करें

USSD भुगतान

क्या करें:

- किसी भी लेन–देन से पहले मोबाइल मनी आइडेंटिफायर और मोबाइल नंबर दोनों की पुष्टि कर लें
- थोड़े–थोड़े अंतराल पर अपना M-PIN नंबर बदलते रहें
- USSD से जुड़ी अनुरोध आने पर उसे ध्यान से देखें



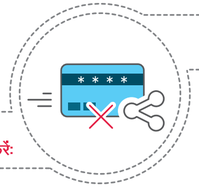
क्या न करें:

- अपना M-PIN किसी के साथ साझा न करें
- अपना M-PIN कहीं लिखकर न रखें
- अपना OTP किसी के साथ साझा न करें

क्रेडिट और डेबिट कार्ड

क्या करें:

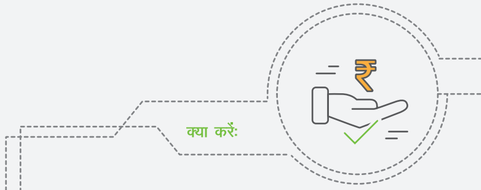
- जब कार्ड का प्रयोग हो रहा हो उस समय आप कार्ड पर अपनी नजर बनाए रखें। काम होते ही तुरंत उसे वापस लेकर रख लें
- कार्ड से लेन–देन करने पर एक SMS आता है। कार्ड से लेन–देन के बाद जांच लें कि SMS में बताई गई लेन–देन की रकम और वास्तविक लेनदेन की रकम में कोई अंतर न हों
- रसीदों और विवरणों का सुरक्षित निपटान करें



क्या न करें:

- मर्चेंट को अपने कार्ड से जुड़ी जानकारियां सुरक्षित कभी भी रखने न दें
- CVV और PIN नंबर किसी के साथ साझा न करें
- अपना डेबिट या क्रेडिट कार्ड किसी को न दें

UPI और BHIM



क्या करें:

- मर्चेंट की तरफ से दिए जाने वाले भुगतान विवरण अनुरोध को जांचने के बाद ही भुगतान करें
- अपने UPI से आधारित ऐप्स को हमेशा अपडेटेड रखें
- किसी परिचित व्यक्ति को ही पैसे ट्रांसफर करें

क्या न करें:

- UPI का M-PIN न तो किसी को बताएं न ही इसे कहीं लिखकर रखें
- UPI/BHIM के माध्यम से लेन–देन कभी भी jailbroken फोन से न करें
- पैसे प्राप्त करने वाले का सत्यापन किए बिना उसे पैसे भेजने से बचें

आधार सक्षम भुगतान प्रणाली

क्या करें:

- पैसे भेजने से पहले आधार नंबर की जांच कर लें
- केवल POS मशीनों या बायोमेट्रिक डेटा कैप्चर मशीनों पर ही लेन–देन के लिए आधार कार्ड का प्रयोग करें
- यह जांच लें कि POS मशीन या बायोमेट्रिक डेटा कैप्चर मशीन के साथ कोई छेड़छाड़ नहीं हुई हो। जहां प्रामाणिक मशीनें इस्तेमाल होती हों वहीं से लेन–देन करें

क्या न करें:

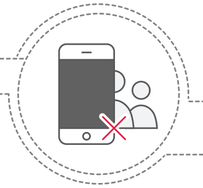
- मर्चेंट को अपना बायोमेट्रिक या कार्ड की डिटेल सुरक्षित रखने की इजाजत न दें
- अपना AEPS कार्ड कहीं भूलें नहीं। उसे अपनी नजरों से ओझल न होने दें
- बिना वजह किसी को अपना आधार नंबर या निजी जानकारी न बताएं

बुनियादी जरूरतें

क्या करें:

- अपने डिवाइस को हमेशा अपडेट रखें। एक मजबूत पासवर्ड डालकर लॉक करके उसे सुरक्षित रखें
- लेनदेन से जुड़ी जानकारियों और अलर्ट पर नजर रखें। किसी भी प्रकार के संदेहास्पद या धोखाधड़ी के प्रयासों की सूचना तत्काल संबंधित सर्विस प्रोवाइडर और पुलिस को दें
- यदि आपका मोबाइल खो जाता है या चोरी हो जाता है तो अपना सिम तत्काल ब्लॉक कराएं। अपने बैंक या जो वॉलेट प्रयोग करते हैं उस संस्था के साथ–साथ पुलिस को भी इस बारे में सूचित करें
- गोपनीय वित्तीय जानकारियां मांगने वाले अवांछित फोन कॉल, SMS या इमेल को लेकर सतर्क रहें
- अपने मोबाइल में ऐसे ऐप्स डाउनलोड करके रखें जो वायरस मालवेयर और फोन में होने वाले अवांछित घुसपैठ को रोककर फोन की सुरक्षा करते हैं। ऐसे ऐप्स को हमेशा सक्रिय रखें
- प्रमाणित ऐप स्टोर या प्लेस्टोर से ही मोबाइल में कोई ऐप्स डाउनलोड करें। उन्हीं ऐप्स को डाउनलोड करें जिनके बारे में अच्छी समीक्षा की गई हो
- ऐप्स की प्रामाणिकता जांचने के लिए उसके लिंक का मिलान बैंक की वेबसाइट पर दिए गए लिंक से कर लें

बुनियादी जरूरतें



क्या न करें:

- एडिमिनिस्ट्रेटिव प्रिविलेज (असामान्य अधिकार जो इंटरनेट सुरक्षा की दृष्टि से जोखिम वाले हैं) के साथ कभी भी इंटरनेट का प्रयोग न करें
- SMS या ईमेल पर आए किसी भी संदेहजनक लिंक को बिलकुल क्लिक न करें
- अप्रमाणिक और असत्यापित स्रोत से कभी भी ऐप्स इन्स्टॉल न करें
- किसी भी jailbroken फोन से मोबाइल बैंकिंग न करें
- असुरक्षित वाई–फाई प्वाइंट का प्रयोग करके कभी भी ऑनलाइन भुगतान न करें
- अज्ञात स्रोतों से प्राप्त ईमेल को कभी भी न तो खोलें न ही उसके साथ भेजे गए अटैचमेंट को कभी डाउनलोड करें
- अपना फोन किसी अपरिचित को कभी न सौंपे
- आपके डेबिट कार्ड या क्रेडिट कार्ड के एटीएम पिन, CVV, पासवर्ड की एक्सपायरी डेट पूछने वाले किसी भी ईमेल, फोन या SMS का उत्तर न दें