UPI AND BHIM

DOs:

- Always keep records of UPI transactions
- Ensure that employees are fully educated about frauds
- Activities that lead to fraud, e.g. sharing of pin, account number and personal information, should be discouraged

DON'Ts:

- Biometrics & M-Pin details should never be stored in any form - physical or electronic
- Never neglect the security of customers' information
- Avoid issuing collect request without verifying customer details

AWARENESS CAMPAIGN PARTNERS

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

सत्यमेव जयते
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

DIGITAL PAYMENTS

#SaralBhiSecureBhi

This booklet will introduce you to the dos and don'ts to keep in mind, when you accept payment from your customers digitally.

www.dsci.in/digital-payment-suraksha

SCAN THIS

AEPS

DOs:

- Ensure that the devices (POS and biometric capture machine) are not tampered with and only certified devices are being used
- Always keep your POS upgraded and maintain its security
- Ensure that you promptly report suspicious behaviour of POS

DON'Ts:

- Avoid placing POS in open or unsecure areas
- Never print full card or Aadhaar details on slips and reports
- Aadhaar details - number, personal information, biometrics should not be stored

BASIC ESSENTIALS

DOs:

- Always educate your employees who handle payments regarding threats
- Always use secure and trusted payment gateways which are thoroughly tested
- Ensure authenticity of applications by validating from links on Bank's websites
- Ensure that devices used (POS & biometric capture machine) are updated, not tampered with and only certified devices are being used
- Keep a watch on transaction logs and alerts; and report suspicious or fraudulent attempts to relevant service providers & police officials

DON'Ts:

- Never install apps from untrusted and unverified sources/app stores
- Never use unsecure/open Wi-Fi points for accepting digital payments
- Never leave payment devices unattended or hand it over to strangers
- Never store customers' sensitive information such as Biometric, M-Pin, Password, etc. in any form (physical/electronic)

ONLINE AND MOBILE BANKING

DOs:

- Always use secure and trusted payment gateways
- Make sure payment gateway integration is thoroughly tested
- Regularly check that customers are able to transact using online and mobile banking

DON'Ts:

- Avoid asking customers their online banking information
- Never disregard security of payment module
- Never ignore fraud attempts, promptly report to bank/payment gateway

MOBILE WALLET

DOs:

- Always tally payment received from wallets & keep track of transaction reference numbers
- Regularly check that customers are able to transact using secure & static QR code
- Always verify the agent's official ID before sharing sensitive information

DON'Ts:

- Refrain from storing customers' sensitive information in any form (physical/electronic)
- Never ignore attempts of fraud and promptly report to the concerned wallet company
- Avoid collecting customer information that's more than required

CREDIT AND DEBIT CARD

DOs:

- Execute card transactions only under the supervision of the customer
- Always keep your POS upgraded and maintain its security
- Ensure that the POS Devices are not tampered with and only certified devices are being used

DON'Ts:

- Avoid POS devices getting out of sight/supervision & should not be accessed by unauthorized people
- Never store card CVV and PIN
- Refrain from storing customers' card details unless absolutely required