UPI AND BHIM

AWARENESS CAMPAIGN PARTNERS





AEPS



- 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



DOM 12:

- 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













mastercard.







Follow us





in dsci-security-council-of-India

suraksha

A Joint Initiative of





"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





- 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



- 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

ONLINE AND MOBILE BANKING

MOBILE WALLET

CREDIT AND DEBIT CARD

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)



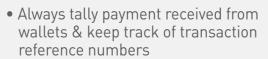
- Always use secure and trusted payment gateways
- Make sure payment gateway integration is thoroughly tested
- Regularly check that customers are able to transact using online and mobile banking



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





- 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



- 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