MOBILE WALLET

DOs:

- Always verify and install authentic wallet apps
- Ensure your phone is protected with a PIN
- Make sure the beneficiary's mobile number is correct before transactions

DON'Ts:

- Avoid using a common password for all wallets
- Refrain from using open Wi-Fi or unverified devices for making payments
- Do not scan untrusted QR Codes

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

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

Introduce yourself to the world of dos and don'ts of digital payments with this handy booklet.

www.dsci.in/digital-payment-suraksha

SCAN THIS

ONLINE AND MOBILE BANKING

DOs:

- Use only verified and trusted browsers & HTTPS secured websites for payments
- Ensure you change passwords frequently and promptly if compromised
- Always keep your payment transaction applications (banks/payment banks/ wallets) updated with the latest version

DON'Ts:

- Never store login credentials on phone; also don't enter credentials on untrusted kiosks
- Avoid transacting through public devices and on unsecure/open networks
- Refrain from sharing your mobile banking PIN with anyone

USSD PAYMENT

DOs:

- Always validate Mobile Money Identifier and mobile number before any transaction is done
- Ensure that you change your M-PIN at regular intervals
- Be observant of incoming USSD requests

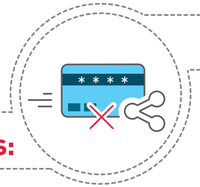
DON'Ts:

- Never share your M-PIN with anyone
- Refrain from writing down your M-PIN
- Avoid sharing your OTP with anyone

CREDIT AND DEBIT CARD

DOs:

- Always keep an eye on your card during usage and promptly take it back
- Always check if there's any discrepancy between the transaction SMS details and actual transaction
- Ensure that you securely dispose of receipts and statements



DON'Ts:

- Never allow merchants to store your card information
- Avoid sharing CVV and PIN with anyone
- Do not leave your credit or debit card with anyone

UPI AND BHIM

DOs:

- Check the payment collect request details with the merchant before making the payment
- Be sure to keep UPI-based apps updated
- Make sure you transfer money only to known beneficiaries

DON'Ts:

- Never share or write down your UPI M-PIN
- Avoid using jailbroken devices for UPI/BHIM transactions
- Refrain from transferring money without verifying the recipient first

AEPS

DOs:

- Always verify Aadhaar number before transferring money
- Use Aadhaar ID to carry out transactions only at POS and biometric data capture device
- Ensure that the devices (POS and biometric capture machine) are not tampered with and only certified devices are being used

DON'Ts:

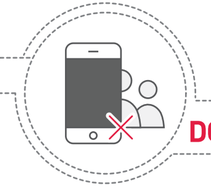
- Never allow merchants to store your biometrics and card details
- Refrain from leaving your AEPS card unattended or letting it go out of sight
- Avoid giving away your Aadhaar & personal details without valid reason

BASIC ESSENTIALS

DOs:

- Always keep your device updated, locked & protected with a strong password
- Keep a watch on transaction logs and alerts; and report suspicious or fraudulent attempts to relevant service providers & police officials
- Immediately block your SIM if your device gets lost or stolen and inform respective bank/wallet organisation & police officials
- Beware of unsolicited calls, texts or emails asking for sensitive financial information
- Applications for detecting and removing threats, including firewalls, virus malware and intrusion-detection systems, mobile security solutions should be installed and activated
- Download applications on your devices from authentic App stores with good reviews only
- Ensure authenticity of applications by validating from links on Bank's websites

BASIC ESSENTIALS



DON'Ts:

- Never access the Internet with administrative privileges
- Refrain from clicking suspicious links received in SMS or email
- Never install apps from untrusted & unverified sourses
- Steer clear of using jailbroken or rooted devices for mobile banking
- Avoid connecting to unsecure Wi-Fi points for online digital payments
- Avoid opening or downloading emails or attachments from unknown sources
- Never handover your device to strangers
- Avoid responding to emails, phone calls or text messages asking for Debit card / Credit card / ATM pin / CVV / Expiry date or Passwords