BHIM Baroda Pay

Dos:

- Download BHIM Baroda Pay, UPI application through valid platforms i.e. Google Play store etc.
- Register for mobile banking through your base branch/net banking/BOB ATM/UPI.
- Make sure you login and initiate UPI transaction in complete privacy.
- After completing transaction, make sure you logged out of application successfully.
- For every transaction, you will receive sms alert to your registered mobile number. If you find any unauthorized UPI transaction in your account, please take up with your branch immediately.
- In case of any failed transactions, please take up with escalation matrix provided on website and application.
- Change your UPI application password and UPI PIN / MPIN frequently.
- In case of unauthorized access of your mobile banking/UPI, please de register immediately through ATM / internet banking / base branch (or please contact our Contact Centre).
- In case your mobile phone is lost / stolen, please de register your mobile banking immediately through Base branch / Net banking / ATM / contact center.
- In case your mobile banking / mobile number is de registered / deactivated without your request or you get a call in this regard, somebody may be trying to get a duplicate SIM/ steal your credentials like mPIN / OTP (One time password), etc. In this case, please contact your base branch immediately.

Don’ts:

- Please do not share your passwords / do not store it in your Mobile handset.
- Never let anyone see you entering your application password or UPI PIN / MPIN.
- Never use application/ UPI PIN / MPIN that can be easily guessed Ex: 1111/2222/1234/ Birth year, mobile number/telephone number.
- Don’t install and use UPI application in someone else device.
- Bank of Baroda does not make calls / emails, asking for your UPI / Mobile banking passwords. If any caller pretends to be from our Bank / Contact Centre, please do not entertain such requests as they are fraudulent entities.
- Never carry your registered SIM card and debit card together, as there is a risk of losing both of them, which may enable anybody gaining access to your account.

- PHISHING: Phishing, also called spoofing, is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has.
- Do not share your PIN(s) to anybody, including bank staff. (Bank does not require your user id or PIN at any point of time. So if you receive any communication asking for this information, please do not send your user id or PIN(s)).