Do’s & Dont’s of Mobile Banking

Do's :

- ✓ **Password protect** the mobile phone. It is recommended to set the maximum number of incorrect password submissions no more than three.
- ✓ Choose a **strong password** to keep your account and data safe.
- ✓ **Change your password regularly.**
- ✓ **Review** your account **frequently** to check for any unauthorized transactions.
- ✓ **Report a lost or stolen phone** immediately to your service provider and law enforcement authorities.

Don'ts :

- × **Never give your password** or confidential information over the phone or internet. Never share these details with anyone.
- × Don’t click on links **embedded in emails/social networking sites claiming** to be from the bank or representing the bank.
- × Don’t transfer **funds without due validation** of the recipient, as funds once transferred cannot be reversed**.**
- × **Don’t store sensitive information** such as card details, mobile banking password and user ID in a separate folder on your phone.
- × Don’t forget to **inform the bank of changes in your mobile** number to ensure that SMS notifications are not sent to someone else.
- × Never reveal or write down password or retain any email or paper communication from the bank with **regard to the password.**
- × Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources.
- × Be cautious while using **Bluetooth in public places** as someone may access your confidential data/information.
- × Be careful about the websites you are browsing, if it does not look authentic, **do not download anything** from it.