



## Do's

1. Do remember the URL of our banking websites [(https://bank.sbi), (https://onlinesbi.com)]. Always check for "https" or padlock before using our banking applications.
2. Keep your password strong and complex with minimum length of 8 characters combining at least one numeric, one special character and mix of Upper and Lower case letters. Change your passwords frequently.
3. Install our apps (YONO SBI, YONO Lite SBI, BHIM SBI, SBI Quick) from Google Play Store/iOS App Store only.
4. Always remember that a UPI PIN or scanning of a QR code is required only for transferring amounts, not for receiving.
5. Transactional/Promotional messages sent by SBI will always bear Short Codes "SBI, SB" only, for e.g., SBIBNK, SBIINB, SBYONO, ATMSBI.
6. Notify the bank about change in your mobile number to ensure that SMS notifications continue to be sent to you.



## Don'ts

1. Do not share your personal/financial details like username, password, OTP, Card Number, CVV, PIN etc. with anyone including the Bank's representatives.
2. Do not use common passwords for all accounts.
3. Do not connect to open/public Wi-Fi for conducting Banking transactions.
4. Do not install any app on the advice of strangers.
5. Do not store sensitive information such as passwords, MPIN, account numbers, etc. on your phone.
6. Do not click on links embedded in SMS/emails/social networking sites claiming to be from the bank or representing the bank.



**Remember: "Bank never asks for your confidential details over Call/SMS/Email"**

Call our helpline numbers for assistance: **1800112211/ 18004253800/ 18001234/ 1800111109**

To report any suspicious activity, kindly email on **report.phishing@sbi.co.in** or call the cybercrime helpline number **1930**

For more information visit: **<https://www.cybercrime.gov.in>**

**STAY #SAFEWITHSBI**