DOs and DON'Ts on Social Media

DOs

1. Use our official handles / pages / profiles / channels to interact with us on social media:

Platform	Name of the handles / pages / profiles / channels of SBI
X (formerly Twitter)	@TheOfficialSBI, @OfficialSBICare
LinkedIn	@state-bank-of-india
Facebook	@StateBankOfIndia
Instagram	@theofficialsbi
You Tube	@TheOfficialSBI
Pinterest	@TheOfficialSBI
Quora	@State-Bank-of-India-4

2.Use Bank's Official Channels, CRCF website (https://crcf.bank.sbi), SBI Toll free Contact Center numbers 18001234, 18002100, or escalation matrix available on Bank's Official Websites/portals to register your complaints/concerns.

3.Always use our Bank's Website URL **https://bank.sbi** directly to keep yourself informed about our products & services. Always check for "https" or padlock icon before using our Bank's website.

4.Keep your password strong by keeping it long, unique, and tough to crack, combining at least one numeric, one special character and mix of Upper- and Lower-case letters. Change your passwords frequently.

5.Immediately notify the bank in case of change in your registered mobile number.

6.Beware of attempts to defraud you through fake profiles using SBI logo, SBI profile names or under the guise of association with SBI on online channels / Social Media platforms promising unrealistic returns on investment. SBI does not endorse any such schemes that promise unrealistic returns, nor do we authorize any person or entity to do so on our behalf.

7.Beware of engaging with and falling prey to deep fake videos of the Bank's Top Officials that claim launch of or support to some investment schemes. The Bank's Top Officials do not offer or support any such investment schemes promising unrealistic or unusually high returns.

8.Beware of Digital Arrest Fraud. Scammers may try to trap you by posing as law enforcement officials by giving threat calls claiming that you will be arrested unless you pay.

9. Be cautious of Google search scams. Visit official websites of organizations for authentic customer care numbers.

10.Always remember that a UPI PIN or scanning of a QR code is required only for sending money, and not for receiving money.

DON'Ts

1.Don't share your personal/financial details such as username, password, OTP, CVV, PIN, account number, debit/credit card details or transaction details on social media.

2.Don't Post images of Debit/Credit cards, account statements, cheques, passbook etc. on social media.

3.Don't share screenshots of your banking app or payment confirmations, that contain your personal / banking information, over social media.

4.Do not discuss confidential information in public places, including social media platforms.

5.Don't click on suspicious links or any .apk file received through SMS/WhatsApp to update KYC, redeem reward point, pay bills, etc. Such SMSs are fake.

6.Don't fall for SMS, Emails, WhatsApp messages offering discounts/gifts, freebies that sound unrealistic or too good to be true. Such attempts may scam you of money or personal details.

7.Do not instantly trust unexpected calls from unknown numbers asking for urgent money or personal details - they could be voice cloning frauds. Always verify before taking any action.

8.Do not perform online banking transactions at public places using public / open Wi-Fi networks.

11. Beware of Income Tax frauds. Do not click on any link. Always visit the official website of Income Tax department to file Income Tax Return. 12.Always report any cybercrime incident immediately without any delay. Dial 1930 or visit https://cybercrime.gov.in/ to report any cybercrime incident. 13.Always report about suspicious messages, profiles or offers pretending to be from the bank on report.phishing@sbi.co.in 14. Always pick up calls from 1600-01-8000 to 8007, 1600-11-7011 to 7015, 1600-00-1351 and 1600-10-0021 and help us protect you from potential frauds.	

Remember: “Bank never asks for your confidential details over Call/SMS/Email”

STAY #SAFEWITHSBI