

কি কি করণীয়

1. আমাদের ব্যাঙ্কিং ওয়েবসাইটগুলির URL মনে রাখবেন [(https://bank.sbi), (https://onlinesbi.com)] সবসময় "https" বা padlock দেখে নিশ্চিত হয়ে তারপর আমাদের ব্যাঙ্কিং অ্যাপ্লিকেশনগুলি ব্যবহার করুন।
2. আপনার পাসওয়ার্ড নিরাপদ ও সুরক্ষিত রাখতে অন্তত একটি সংখ্যা, একটি special character এবং Upper আর Lower কেস অক্ষর মিলিয়ে, অন্ততপক্ষে ৮ টি character এর পাসওয়ার্ড ব্যবহার করুন। মাঝে মাঝে পাসওয়ার্ড বদলাতে থাকুন।
3. আমাদের app গুলি (YONO SBI, YONO Lite SBI, BHIM SBI, SBI Quick) শুধুমাত্র Google Play Store/ iOS App Store থেকে ইন্সটল করুন।
4. সবসময় মনে রাখবেন UPI PIN বা QR কোড স্ক্যান শুধুমাত্র টাকা পাঠানোর সময় প্রয়োজন, টাকা পাওয়ার সময় নয়।
5. SBI ব্যাঙ্কের পরিষেবা সংক্রান্ত/প্রচারমূলক বার্তা/মেসেজগুলিতে সবসময় "SBI, SB" এই শর্ট কোডগুলিই থাকবে, যেমন - SBIBNK, SBIINB, SBYONO, ATMSBI
6. SMS notification চালু/বজায় রাখার জন্য আপনার সঠিক মোবাইল নাম্বার ব্যাঙ্কের সাথে যুক্ত রাখুন।

কি কি করবেন না

1. নিজের ব্যক্তিগত/আর্থিক তথ্য যেমন ইউজার নেম, পাসওয়ার্ড, OTP, কার্ডের নাম্বার, CVV, PIN ইত্যাদি কারো সাথে, এমনকি ব্যাঙ্কের প্রতিনিধির সাথেও, শেয়ার করবেন না।
2. সব একাউন্ট এর জন্য একইরকম পাসওয়ার্ড রাখবেন না।
3. ওপেন/পাবলিক Wi-Fi ব্যবহার করে কোনোরকম ব্যাঙ্কের লেনদেন করবেন না।
4. অপরিচিত ব্যক্তির পরামর্শে কোনো অ্যাপ ইন্সটল করবেন না।
5. পাসওয়ার্ড, MPIN, একাউন্ট নাম্বার এই ধরনের গুরুত্বপূর্ণ তথ্য মোবাইল ফোনে রাখবেন না।
6. কোনো SMS/ই মেইল/সামাজিক যোগাযোগ মাধ্যমে ব্যাঙ্ক থেকে পাঠানো বা ব্যাঙ্কের তরফে কোনো লিঙ্ক দেওয়া থাকলে সেটি খুলবেন না।



মনে রাখবেন: "ব্যাঙ্ক কখনই কল/এসএমএস/ইমেলের মাধ্যমে আপনার গোপনীয় বিষয় গুলি চায় না।"

যেকোনো সহায়তার জন্য আমাদের হেল্পলাইন নম্বরে কল করুন:

**1800-11-22-11/ 1800-425-3800/ 1800 1234/1800111109**

To report any suspicious activity, kindly email on [report.phishing@sbi.co.in](mailto:report.phishing@sbi.co.in) or call the cybercrime helpline number **1930**

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

**STAY #SAFEWITHSBI**