

ਕਰੋ

1. ਸਾਡੀਆਂ ਬੈਂਕਿੰਗ ਵੈੱਬਸਾਈਟਾਂ [(<https://bank.sbi>), (<https://onlinesbi.com>)] ਦਾ URL ਯਾਦ ਰੱਖੋ। ਸਾਡੀਆਂ ਬੈਂਕਿੰਗ ਐਪਲੀਕੇਸ਼ਨਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾਂ "https" ਜਾਂ ਤਾਲੇ ਦੀ ਜਾਂਚ ਕਰੋ।
2. ਘੱਟੋ-ਘੱਟ 8 ਅੱਖਰਾਂ ਦੀ ਲੰਬਾਈ ਦੇ ਨਾਲ ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਮਜ਼ਬੂਤ ਅਤੇ ਗੁੰਝਲਦਾਰ ਰੱਖੋ ਜਿਸ ਵਿੱਚ ਘੱਟੋ-ਘੱਟ ਇੱਕ ਸੰਖਿਆਤਮਕ, ਇੱਕ ਵਿਸ਼ੇਸ਼ ਅੱਖਰ ਅਤੇ ਵੱਡੇ ਅਤੇ ਹੇਠਲੇ ਕੇਸਾਂ ਦੇ ਮਿਸ਼ਰਣ ਸ਼ਾਮਲ ਹੋਣ। ਆਪਣੇ ਪਾਸਵਰਡ ਵਾਰ-ਵਾਰ ਬਦਲੋ।
3. ਸਿਰਫ਼ Google Play Store/iOS ਐਪ ਸਟੋਰ ਤੋਂ ਸਾਡੀਆਂ ਐਪਸ (YONO SBI, YONO Lite SBI, BHIM SBI, SBI Quick) ਨੂੰ ਇੰਸਟਾਲ ਕਰੋ।  
ਹਮੇਸ਼ਾ ਯਾਦ ਰੱਖੋ ਕਿ ਇੱਕ UPI ਪਿੰਨ ਜਾਂ QR ਕੋਡ ਦੀ ਸਕੈਨਿੰਗ ਸਿਰਫ਼
4. ਰਕਮਾਂ ਨੂੰ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਲਈ ਜ਼ਰੂਰੀ ਹੈ, ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਨਹੀਂ।  
SBI ਦੁਆਰਾ ਭੇਜੇ ਜਾਣ ਵਾਲੇ ਲੈਣ-ਦੇਣ/ਪ੍ਰਚਾਰ ਸੰਬੰਧੀ ਸੁਨੇਹਿਆਂ ਵਿੱਚ
5. ਹਮੇਸ਼ਾ ਛੋਟੇ ਕੋਡ "SBI, SB" ਹੋਣਗੇ, ਜਿਵੇਂ ਕਿ, SBIBNK, SBIINB, SBYONO, ATMSBI
- ਬੈਂਕ ਨੂੰ ਆਪਣੇ ਮੋਬਾਈਲ ਨੰਬਰ ਵਿੱਚ ਤਬਦੀਲੀ ਬਾਰੇ ਸੂਚਿਤ ਕਰੋ ਤਾਂ ਜੋ ਇਹ
6. ਯਕੀਨੀ ਬਣਾਇਆ ਜਾ ਸਕੇ ਕਿ SMS ਸੂਚਨਾਵਾਂ ਤੁਹਾਨੂੰ ਭੇਜੀਆਂ ਜਾਂਦੀਆਂ ਰਹਿਣ।

ਨਾ ਕਰੋ

1. ਆਪਣੇ ਨਿੱਜੀ/ਵਿੱਤੀ ਵੇਰਵਿਆਂ ਜਿਵੇਂ ਕਿ ਉਪਭੋਗਤਾ ਨਾਮ, ਪਾਸਵਰਡ, OTP, ਕਾਰਡ ਨੰਬਰ, CVV, PIN ਆਦਿ ਨੂੰ ਬੈਂਕ ਦੇ ਪ੍ਰਤੀਨਿਧੀਆਂ ਸਮੇਤ ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝਾ ਨਾ ਕਰੋ।
2. ਸਾਰੇ ਖਾਤਿਆਂ ਲਈ ਆਮ ਪਾਸਵਰਡ ਨਾ ਵਰਤੋ।
3. ਬੈਂਕਿੰਗ ਲੈਣ-ਦੇਣ ਕਰਨ ਲਈ ਓਪਨ/ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਨਾਲ ਕਨੈਕਟ ਨਾ ਕਰੋ।
4. ਅਜਨਬੀਆਂ ਦੀ ਸਲਾਹ ਤੇ ਕੋਈ ਵੀ ਐਪ ਇੰਸਟਾਲ ਨਾ ਕਰੋ।
5. ਆਪਣੇ ਫ਼ੋਨ ਤੇ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਕਿ ਪਾਸਵਰਡ, MPIN, ਖਾਤਾ ਨੰਬਰ ਆਦਿ ਸਟੋਰ ਨਾ ਕਰੋ।
6. ਬੈਂਕ ਤੋਂ ਹੋਣ ਜਾਂ ਬੈਂਕ ਦੀ ਨੁਮਾਇੰਦਗੀ ਕਰਨ ਦਾ ਦਾਅਵਾ ਕਰਨ ਵਾਲੇ SMS/ਈਮੇਲਾਂ/ਸੋਸ਼ਲ ਨੈੱਟਵਰਕਿੰਗ ਸਾਈਟਾਂ ਵਿੱਚ ਏਮਬੇਡ ਕੀਤੇ ਲਿੰਕਾਂ ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ।



ਯਾਦ ਰੱਖੋ: "ਬੈਂਕ ਕਦੇ ਵੀ ਕਾਲ/SMS/ਈਮੇਲ 'ਤੇ ਤੁਹਾਡੇ ਗੁਪਤ ਵੇਰਵਿਆਂ ਦੀ ਮੰਗ ਨਹੀਂ ਕਰਦਾ।"

ਕਿਸੇ ਵੀ ਸਹਾਇਤਾ ਲਈ ਸਾਡੇ ਹੈਲਪਲਾਈਨ ਨੰਬਰ 'ਤੇ ਕਾਲ ਕਰੋ:

**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**