

Is your SBI YONO account at risk? Govt warns on Aadhaar update scam BS

Clipped from: https://www.business-standard.com/finance/personal-finance/is-your-sbi-yono-account-at-risk-govt-warns-on-aadhaar-update-scam-126032300619_1.html

Scam targets SBI YONO users, govt warns against sharing banking details

The government has flagged a phishing scam targeting users of State Bank of India's (SBI's) YONO app, warning that a viral message asking customers to update Aadhaar or risk account blockage is fake.

Fake alert claims YONO app will be blocked

A message circulating on social media and messaging platforms claims that users must urgently update their Aadhaar details or their YONO app will be blocked. It also asks users to download an APK file to complete the update.

However, the government's fact-checking arm, PIB Fact Check, has dismissed the claim as false.

According to the official clarification, no such instruction has been issued by SBI or its digital banking platform SBI YONO.

What makes this scam dangerous

The fraudulent message attempts to create urgency by warning of account blockage. It then pushes users to:

- Download an APK file from an unknown source
- Share sensitive details such as Aadhaar and banking credentials
- Complete KYC through unofficial channels

Cybersecurity experts have repeatedly warned that APK files shared via WhatsApp or SMS can install malware on devices, allowing fraudsters to access financial data.

What SBI and the government have said

The PIB has clearly stated:

- The claim is fake

- SBI does not ask customers to download APK files for Aadhaar updates
- Customers should never share personal or banking details in response to unsolicited messages

SBI has also reiterated that all official communication happens only through its verified channels.

How to stay safe from such frauds

Users should follow basic precautions to protect their money and personal data:

- Do not click on unknown links or download apps from unofficial sources
- Avoid sharing Aadhaar, OTPs, PINs or banking details over calls or messages
- Verify any urgent request directly with the bank
- Install apps only from trusted platforms such as Google Play Store or Apple App Store

If you receive such messages, report them immediately to SBI at its official phishing email ID.

Why this matters

Such scams are designed to steal banking credentials and gain unauthorised access to accounts. Even a single mistake, such as installing a malicious file, can lead to financial loss.

With digital banking usage rising, fraudsters are increasingly using social engineering tactics that mimic trusted institutions. Staying cautious and verifying information before acting is critical to safeguarding your finances.
