September 2022

SBI

The banker to every Indian

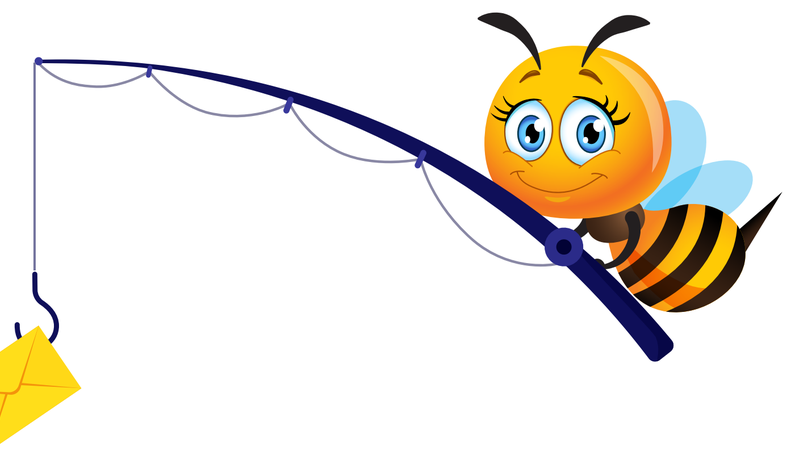
Hive

BE DIGITALLY SAFE AND SECURE WITH SBI EASY TIPS

Bee Smart.
Bee Secure.

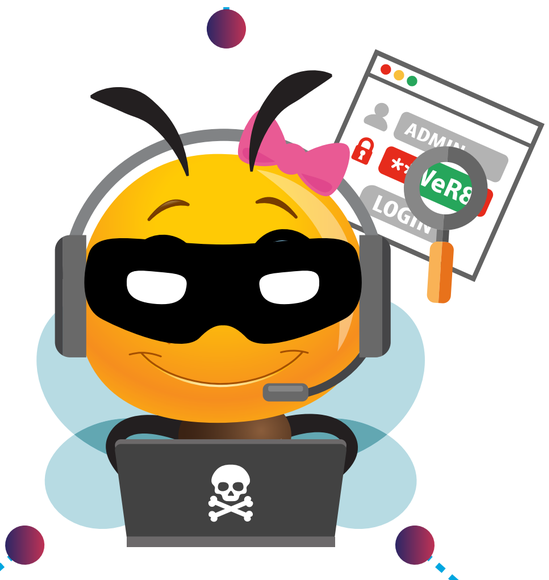
Honeycombs are built in such a way that there's no space wasted. Their hexagon panels fit side by side which keeps their habitat safe from mites, shrikes, and badgers. Similarly, in the third edition of SBI Hive, we provide some safety tips that will keep your account strong and safe from cybercrimes and luring fraudsters.

Don’t be trapped or duped in hands of fraudsters

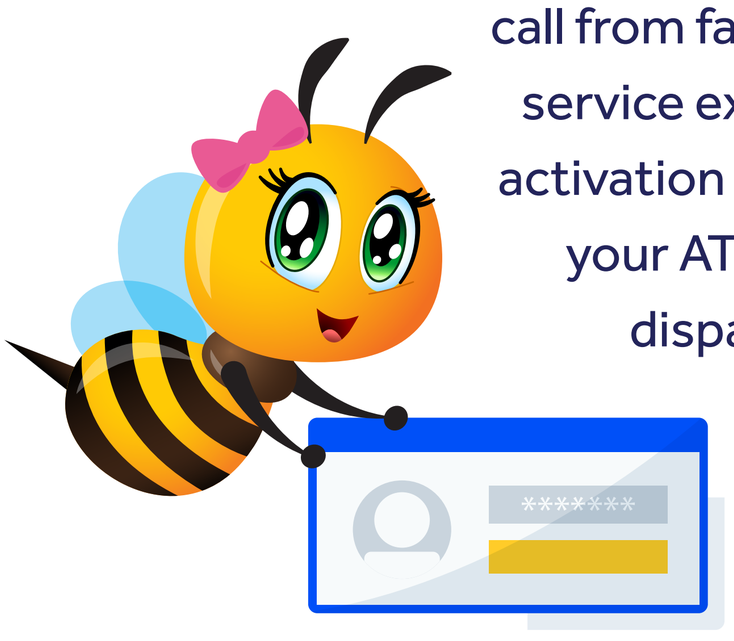


For KYC updation, PAN Card updation, Unblocking Account notices via SMS/Email which contain an embedded phishing web link to steal your credentials

Calling as SBI bank employees and misleading you in divulging confidential information



Using malware or social engineering skills that take control of your device and gain access of OTPs



You May get a support call from fake customer service executive for activation of card once your ATM Card is dispatched

Luring you by sending an e-mail/SMS/phone call promising reward and asking to provide personal information or for updating your account details in the bank site

SBI never sends email /SMS or makes phone calls for getting customer information.

Explore Superior Digital Experience

INB

A web Portal – URL is
https://www.onlinesbi.sbi/

Debit Cards

Variety of Cards available for making Banking convenient for you

YONO Lite

Available as an App -
install from Play/App Store

SBI BHIM PAY APP / UPI

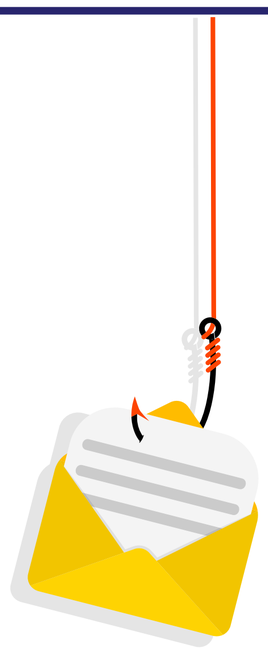
install from Play/App Store or enable through INB/YONO/YONO Lite

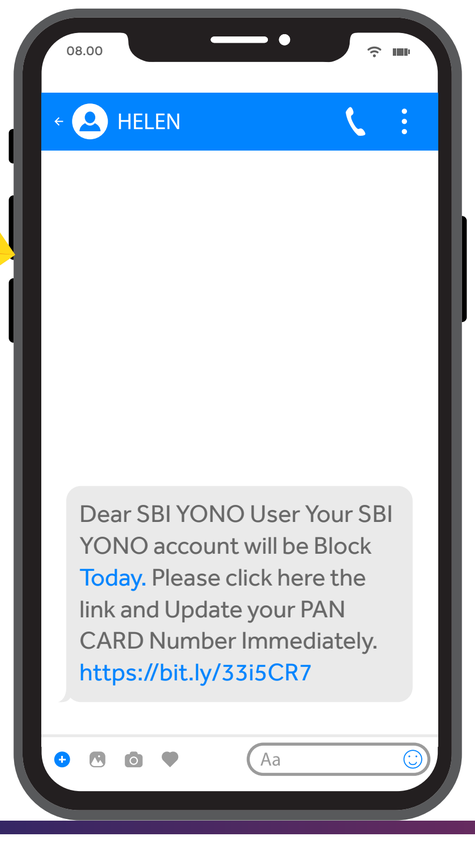
YONO

Available as an App -
install from Play/App Store

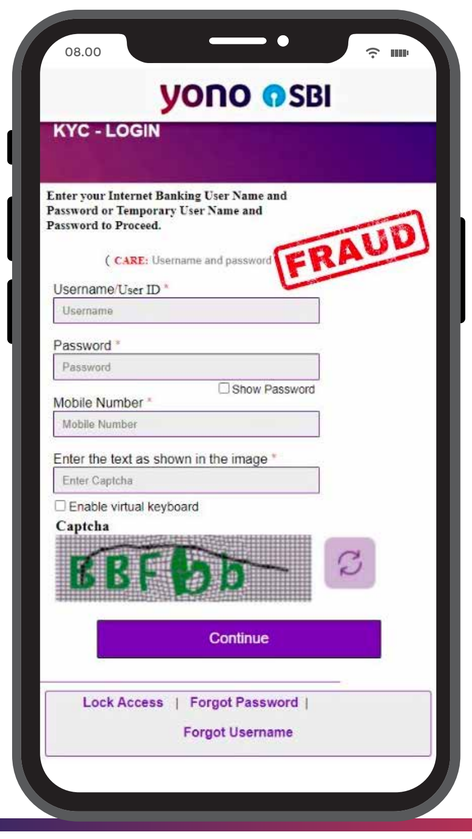
Never respond to any popup, email, SMS or phone call, seeking your personal information such as username, password(s), mobile number, ATM Card details, etc.

Live examples of fraudulent SMS/Links in YONO:





After clicking the link, a fake YONO Web Portal screen is displayed prompting users to input credentials –



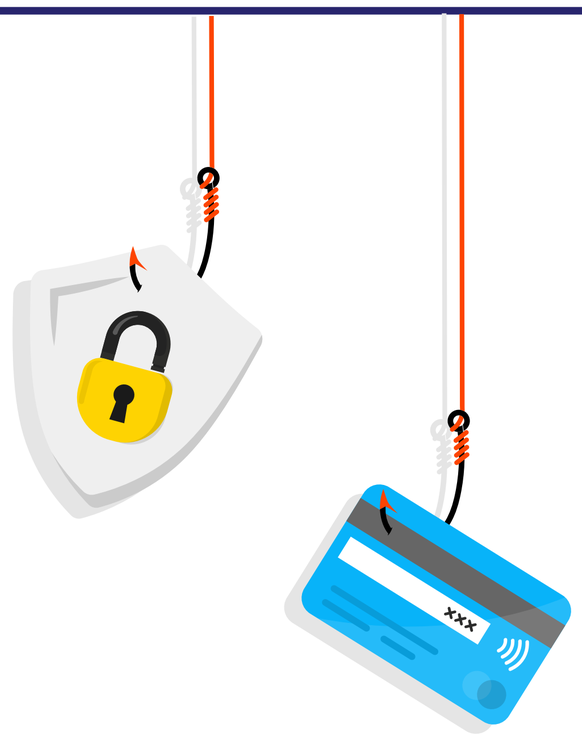
“ Never provide username/Password/ Mobile No./OTP, etc. on such links or to anyone”

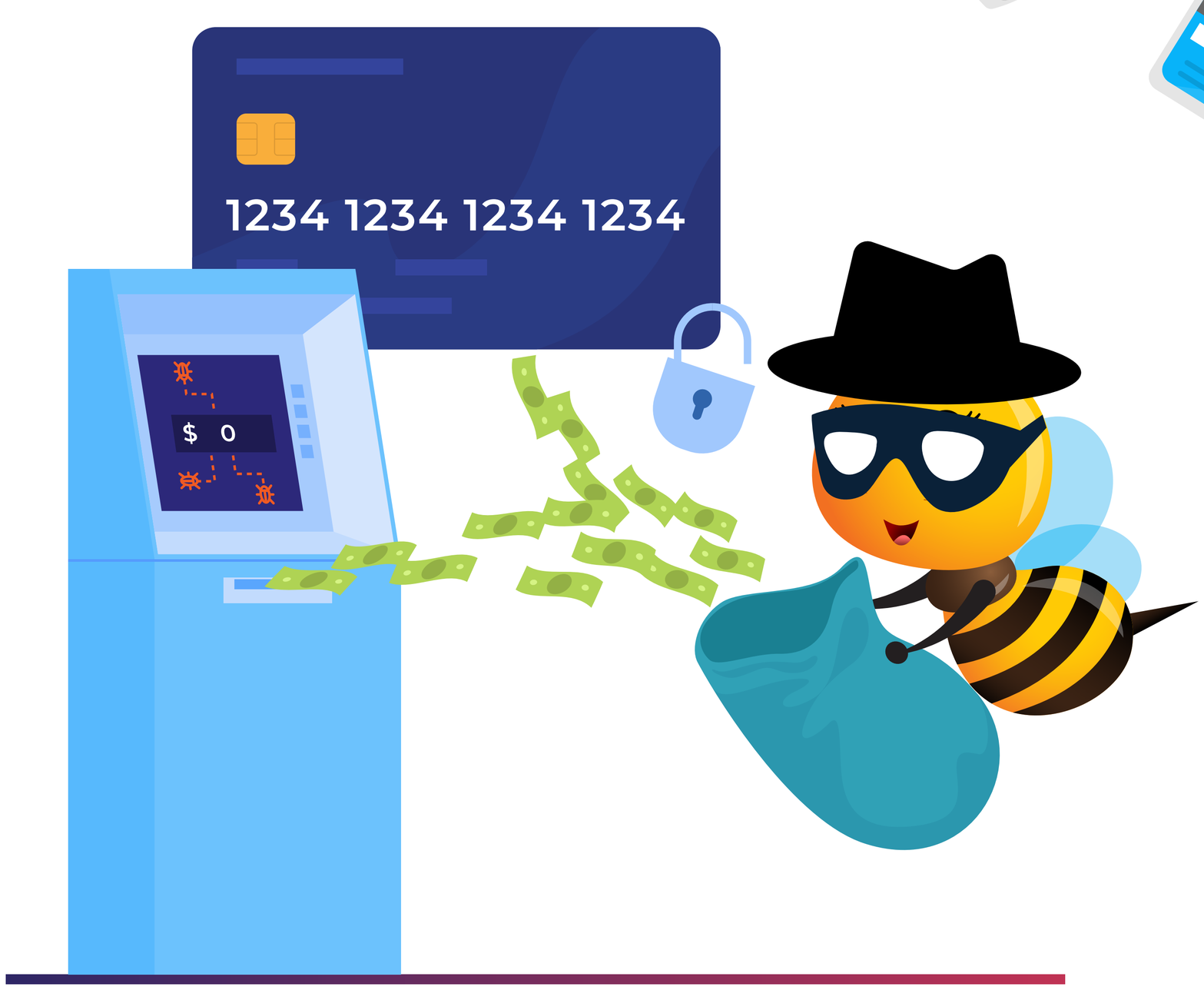
Web portal of YONO is discontinued and YONO SBI can be accessed only through App available on Play/App Store. Create MPIN to avoid typing INB credentials frequently.

Current methods of frauds in Yono Lite/ RINB

- By creating duplicate websites with contact numbers, Cyber Criminal tried to trap you to download / click malware app/link and debit any small amount to capture with INB login credentials and mobile remote access and ultimately the money from your account.
- Active users on social media get lured to share account details

Do not access Internet banking site from cyber cafes or shared PCs





Some examples of frauds in Debit Cards

- **Card Swapping**

  Fraudsters swapping ATM Cards by distracting customers when encountering difficulties while transacting and offering assistance

- **Skimming / Cloning**

  By installing hidden device in an ATM, fraudsters steal information during ATM transaction and create duplicate ATM Card

Manage your debit card transactions through online Banking by setting a limit for card transactions at e-commerce platforms, POS and ATM - both for domestic and international transactions.

Examples of frauds in UPI

Fraudsters could make you download screen sharing apps on various pretexts and misuse the permit to access your personal data

You may get a request to share your UPI PIN to authorise a transfer which could be fraudulent

Using Sale Purchase apps, fraudsters pretend as prospective buyers/sellers prompting you to pay through UPI mode

Always remember that a PIN is needed only for transferring amounts, not for receiving mony

Genuineness of the VPA be ensured before making donations in the accounts of PM Care/ CM Relief funds etc.

Alertness can keep us safe. Please reach out to us in case of any doubt / fraud incidence

1 For every financial transaction, a precautionary email is being sent to you:

"If not done by you, forward this email from email ID registered with SBI to unauthorisedtransaction@sbi.co.in to deactivate your user id. You may also call 1-800-111109"

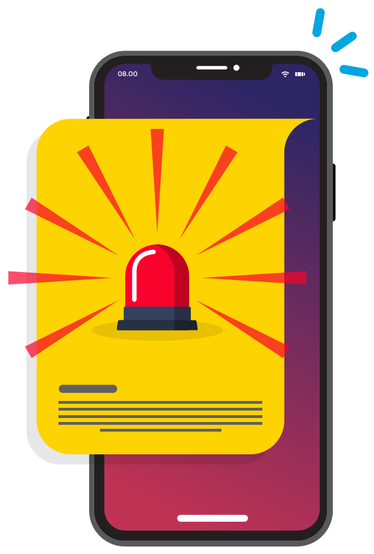
2 SMS is also being sent with the transaction details with the following suffix:

"If not done by you, forward this SMS from mobile number registered with SBI to 9223008333."

3 Other ways to reach us –

(i) visit to the link: https://crcf.sbi.co.in (available 24x7) and lodge your complaint

(ii) Contact any SBI Branch (Home or Non – home) to lodge your complaint



- Once you trigger the alarm via any of the above mode, your Debit card / USER-ID of YONO / RINB / YONO Lite / VPA will be deactivated instantly and automatically
- Post de-activation, complaint is auto lodged in Complaint Resolution Management system
- You will receive Ticket Reference Number along with information about successful/unsuccessful blocking of debit card / deactivation of user ID of the Online Platform (YONO/ RINB/ YONO Lite / UPI ID)

Please report Unauthorized Electronic Debit transaction to us immediately

24/7 Raise your issues...

Raise your issues 24x7 and get quick redressal

Toll Free Number

1800 111109

SMS Number

9223008333

Email ID

unauthorisedtransaction@sbi.co.in

24x7 Complaint Management web portal

https://crcf.sbi.co.in

- **If defrauded amount is amounts less than or equal to Rs.1,00,000/- - File a simple Police Complaint**

  OR

  Register online either on National Cyber Crime Reporting Portal (https://cybercrime.gov.in) or in the website of State / Regional Police.

- **If defrauded amount is more than Rs.1,00,000/- - File FIR with the Police Station.**

Do not click on any unverified URLs. SBI never collects information using any third-party websites

National Cyber Crime Reporting Helpline Number – 1930

For any support, you may dial our Contact Centre Numbers 1800 1234 and 1800 2100