SBI

The banker to every indian

Customer Awareness Guide

Safegaurd yourself from online frauds
Stay alert and #SafeWithSBI

Dear Customers,

Awareness is the key to prevent cyber frauds

As the world continues to digitize and become more linked, cyber security has become a serious issue for everyone.

A cyber-attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber-attacks aim to disable, disrupt, destroy, or control computer systems or to alter, block, delete, manipulate, or steal the data held within these systems.

Cyber criminals launch most cyber-attacks, especially those against the individuals/commercial entities, for financial gain. These attacks often aim to steal sensitive data, such as customer credit card numbers or employee personal information, which the cybercriminals then use to access money or goods using the victims' identities.

The most popular type of cyber-attacks, known as social engineering attacks, take advantage of social interactions to get access to important data. Deception is at the heart of all social engineering attacks. Cyber thieves deceive and influence their victims into performing specific acts, such as circumventing security measures or exposing sensitive information. Similarly, accepting attachments from unknown senders, clicking on links in phishing emails, and using weak passwords are just a few examples of how an individual's actions can cause vulnerabilities that even the strongest cyber security systems cannot prevent, because the victim himself/herself allows the attacker to enter the system.

There is no guaranteed way for any organization to prevent a cyber-attack, but there are numerous cybersecurity best practices that organizations can follow to reduce the risk. Reducing the risk of a cyber-attack relies on using a combination of skilled security professionals, processes, and technology. With cyber-threats increasing significantly, cybersecurity awareness is vital to keeping your workforce and business safe online.

The effective cybersecurity measures necessitate that every individual and every user of digital applications/platforms be aware of cyber security dangers and best practices to follow for safe use of IT and digital platforms. This booklet is designed to teach you the fundamentals of cyber security, the cyber frauds that take place, as well as the recommended practices for conducting secure digital transactions. I am confident that the booklet will assist you in better understanding cyber threats and guide you on a safe and secure digital journey with State Bank of India.

Be a cyber aware customer.
With Best Wishes,

S. Srinivasa Rao
Dy. Managing Director & Chief Risk Officer

17 May 2023

Table of Contents:

Introduction to Cybersecurity

Cybersecurity refers to the safeguarding of electronic infrastructure, including servers, data, computers, mobile devices, and networks, from malicious attacks. The key to cybersecurity is implementing adequate measures to ensure online and digital safety, protecting against fraud and unauthorised access by hackers.

19 out of 20 cyber frauds will not take place at all, if human error is eliminated entirely.

In the context of cyber security, human error refers to unintended action(s) or lack of action(s) by users that may result in a cyber incident. Studies suggest that as much as 95% of such incidents are attributable to human error. If it were possible to completely eliminate human error, approximately 19 out of every 20 cyber breaches could be prevented.

Let us strive to reduce human error & create a holistic defence against cyber crime. Stay alert and #SafeWithSBI

Some common human errors committed by users are:

- Downloading mobile apps on the advice of unknown person(s).
- Clicking on unknown links sent by SMS or Email.
- Sharing of financial details such as Card No./PIN/CVV/OTP with others on emails/calls/SMS/social media.
- Granting permission to mobile applications like access to gallery, messages, contacts, maps etc. which may not be required for the functioning of the app.
- Connecting devices to unauthorised public Wi-Fi networks for performing digital transactions.
- Using weak or easily guessable passwords and not changing them frequently.

Income Tax Refund Fraud

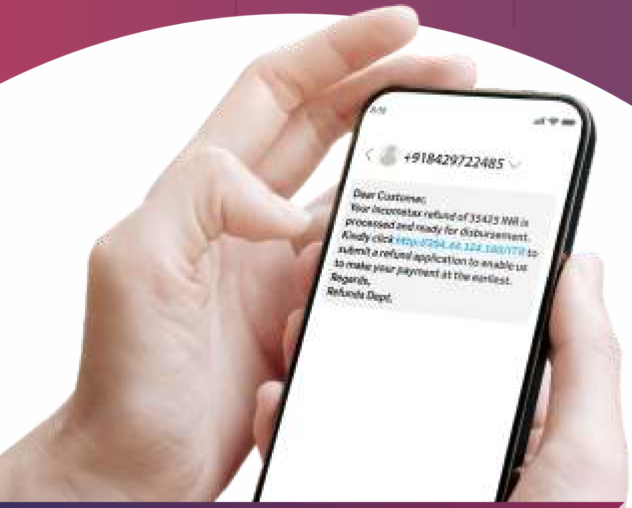
IT RETURN FRAUD

IT return fraud is prevalent and cybercriminals send bulk SMSs asking users to submit an application for initiation of an income tax refund.

These messages contain a link that redirects users to a webpage that looks very similar to the official income tax e-filing website.

Personal information

- Full Name
- PAN
- Aadhaar Number
- PIN Code
- Address
- Mobile Number
- Email Address
- Gender



+918429722485

Dear Customer,
Your Incometax refund of 35425 INR is processed and ready for disbursement. Kindly click [illegible] to submit a refund application to enable us to make your payment at the earliest.
Regards,
Refunds Dept.

Banking information

- Account Number
- IFSC Code
- Credit Card Number
- Expiry Date
- CVV
- PIN Number

After submitting crucial data, users are asked to install an app to receive money. The malicious app asks for device admin rights & other permissions like reading email messages, call logs, etc., taking complete control of the user's device. With these details & control over mobile, they execute fraudulent transactions through your account.

Always validate such SMSs before responding to them. Visit the official IT return website by typing the URL.

Illegal Loan Apps Scam

Illegal Loan Apps Scam

In recent years, a surge has been observed in financial fraud involving illegal and unregulated digital loan applications offering loans at a higher rate of interest. From 928 in 2021 to 3,471 in 2022, cases of fraud and extortion through apps offering small loans have been received by the Mumbai Cyber Crime Branch.

Fraudsters target people from low or medium-income groups who:

Are in need of money,

Are not tech-savvy

Have lower credit scores, poor credit, heavy debt, less knowledge of finance and technology.

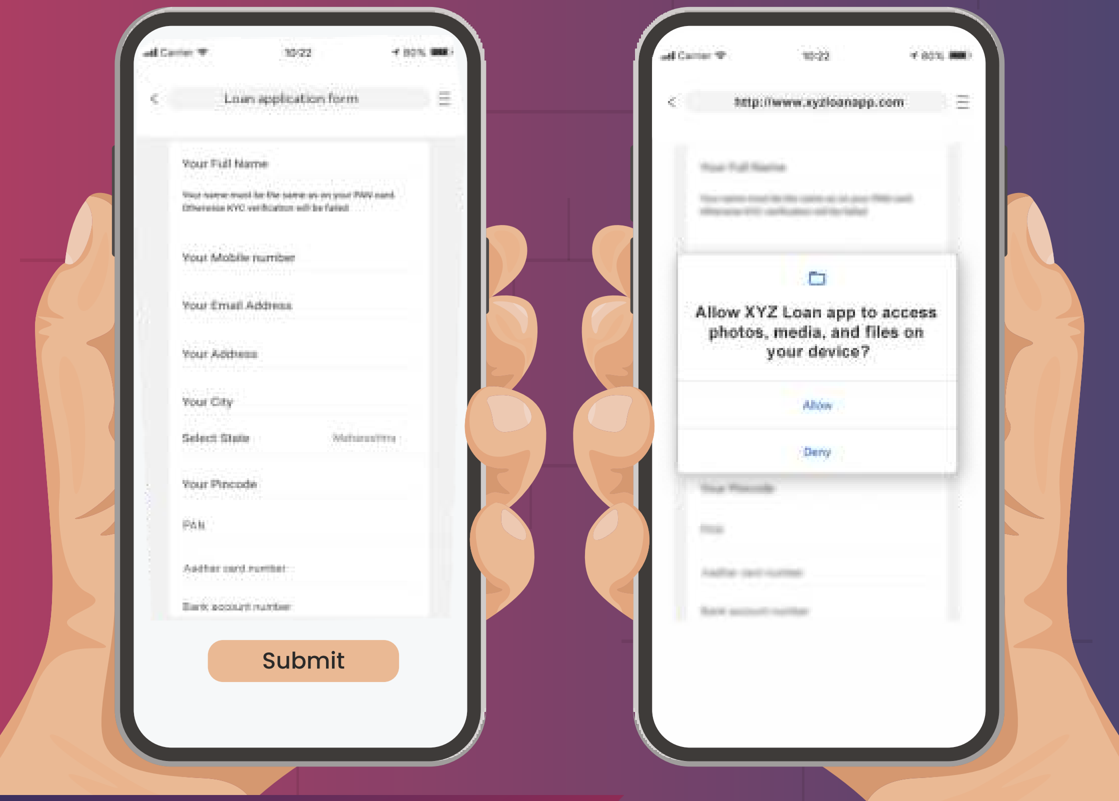
They are offered small amounts (₹ 10,000 – ₹ 30,000) as loan

- After downloading the app, users are prompted to fill out an application form seeking confidential details like PAN, Aadhaar number, bank account details, etc.

- These apps also ask for access to the microphone, photo gallery, mail, and contacts.

- Once the victim's information is collected and the loan is disbursed without clear-cut terms & conditions and listed fees, the app operator threatens to make the victim's confidential data public if repayment of the loan is delayed or missed.

Always check whether these loan apps are affiliated with any bank or NBFC before providing any confidential information.



Loan application form

Your Full Name

Your name must be the same as on your PAN card. Otherwise KYC verification will be failed.

Your Mobile number

Your Email Address

Your Address

Your City

Select State Maharashtra

Your Pincode

PAN

Aadhar card number

Bank account number

Submit

http://www.xyzloanapp.com

Allow XYZ Loan app to access photos, media, and files on your device?

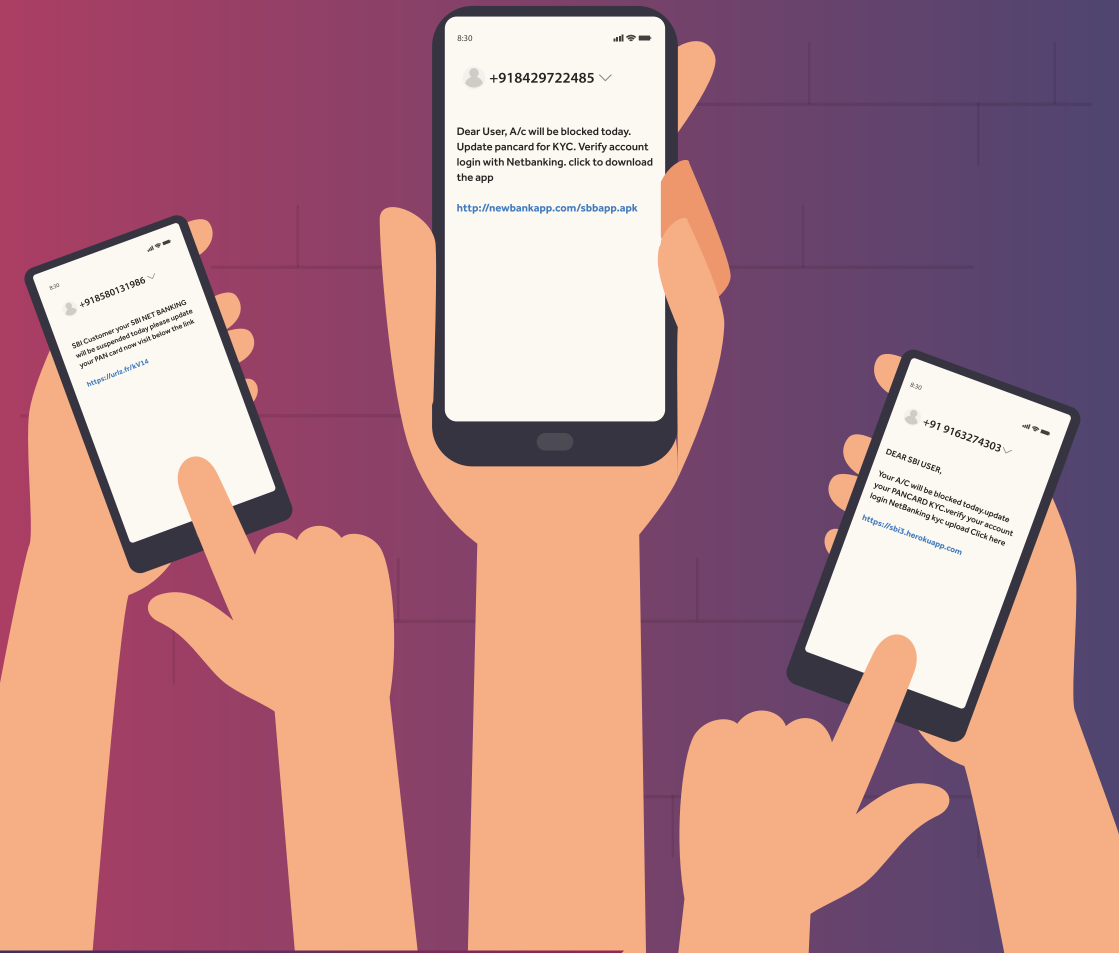
Allow

Deny

KYC Scam through Fake App Download

KYC Scam through Fake App Download

Scammers send bulk SMSs to people in the name of KYC updation and create a sense of urgency by stating that “Your account will be blocked”.



+918580131986

SBI Customer your SBI NET BANKING will be suspended today please update your PAN card now visit below the link

https://urlz.fr/kV14

+918429722485

Dear User, A/c will be blocked today. Update pancard for KYC. Verify account login with Netbanking. click to download the app

http://newbankapp.com/sbbapp.apk

+91 9163274303

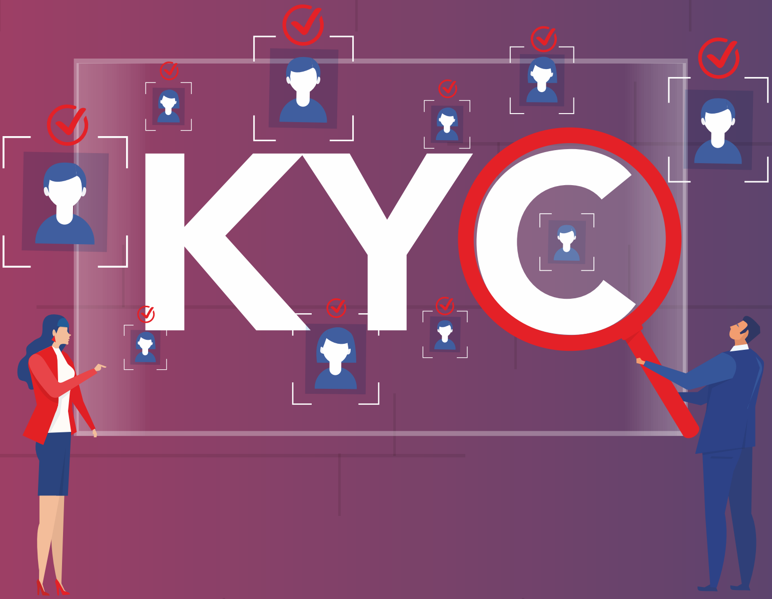
DEAR SBI USER,

Your A/C will be blocked today.update your PANCARD KYC.verify your account login NetBanking kyc upload Click here

https://sbi3.herokuapp.com

- Due to fear of the account getting blocked, the victim navigates to http://newbankapp.com/sbbapp.apk to download the APK file.

- Once the APK file is downloaded on the victim's phone, the app requests permission to access
  - **Messages & Emails**
  - **Contact directory**
  - **Call logs**
  - **Other personal information**



- The fake app asks for your personal details like
  - **Aadhaar**
  - **Login ID & Password**
  - **PAN**
  - **OTP, etc.**

As the malicious app looks like the genuine one, the victim submits all the information and falls prey to such frauds.

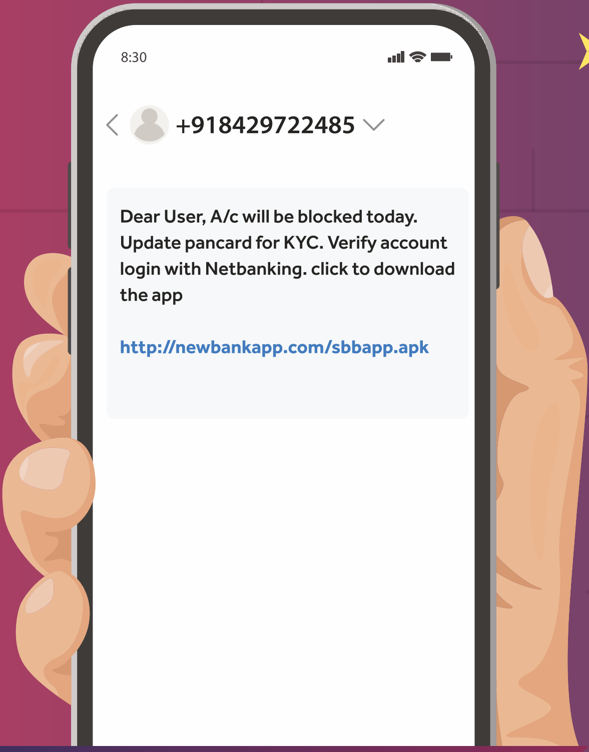
Always download the banking apps from trusted official stores such as App Store, Play Store after understanding the functionality of these

KYC SCAM THROUGH FAKE WEBSITE

KYC SCAM THROUGH FAKE WEBSITE

Cybercriminals send fake messages to multiple users asking them to update their KYC details immediately in order to avoid their bank account getting blocked.

- The victim reacts to this SMS immediately and clicks on the malicious link to update KYC details.
- The victim gets redirected to a fake website that looks very similar to a genuine bank's website.
- The victim enters the correct login credentials which are used by fraudsters to get access to the victim's net banking account and hence, the OTP is generated.



8:30

+918429722485

Dear User, A/c will be blocked today. Update pancard for KYC. Verify account login with Netbanking. click to download the app

http://newbankapp.com/sbbapp.apk

- Victim enters the OTP and fraudsters get access to the victim's account which they misuse to siphon off the money.

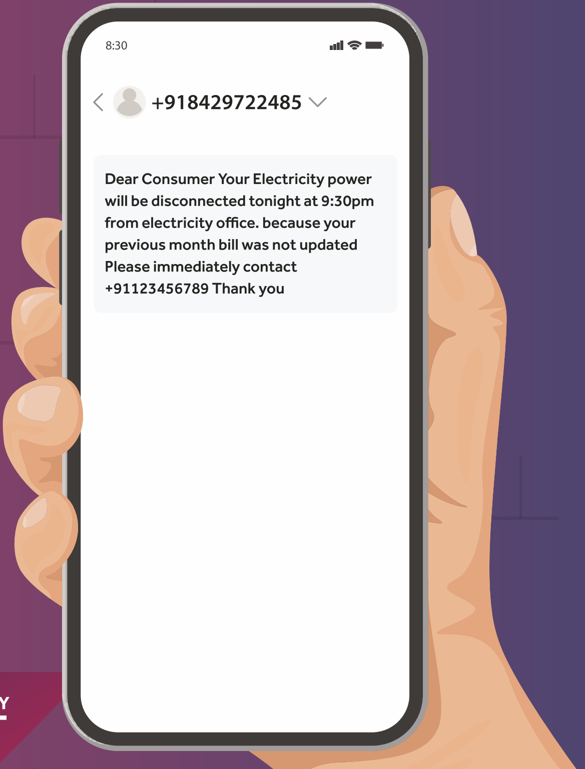
Verify the sender details of the SMS and validate the URL before responding to such SMSs.

Electricity Bill Fraud

Electricity Bill Fraud

Many users receive an SMS from a random number regarding the disconnection of power supply.

- Due to genuine fear and a sense of urgency, people call the mentioned number. The receiver impersonates an electricity department official who tricks the victim to trust the person.
- The fraudster typically asks the potential victim to download an app for making the due payment.
- Once the app is downloaded, the victim is asked to share the passcode to verify the app and tells the victim to proceed with the payment of dues immediately.
- The victim, unaware of the scam, makes the payment without realizing that their mobile screen is being recorded by the fraudster using the screen-sharing app which the victim must have downloaded.
- The fraudster misuses the sensitive information to access the victim's account and siphons off all the money.



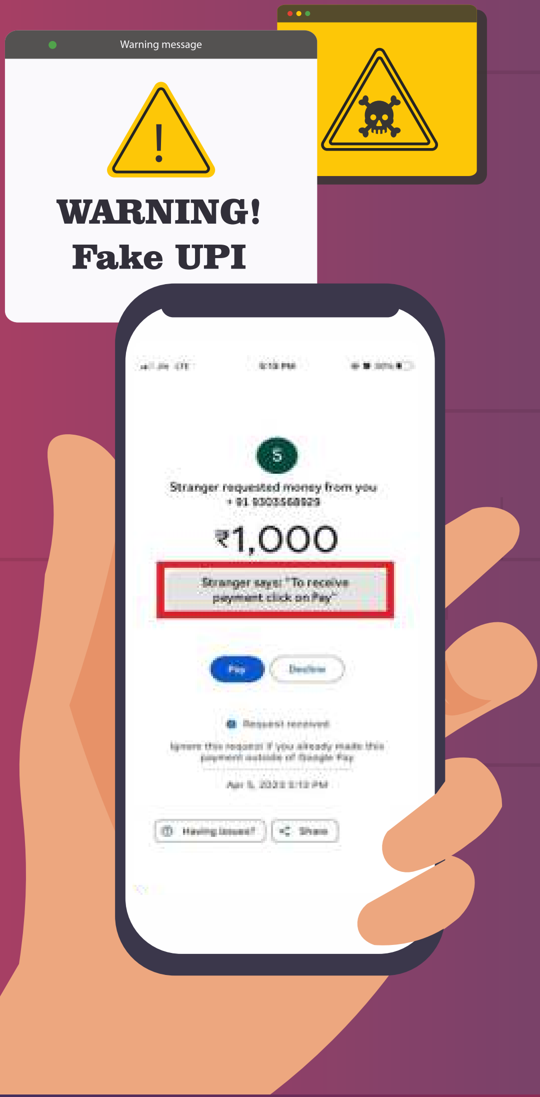
Dear Consumer Your Electricity power will be disconnected tonight at 9:30pm from electricity office. because your previous month bill was not updated Please immediately contact +91123456789 Thank you

Do not download any app on the advice of any stranger. Think before you act.

UPI Collect Request Scam

UPI Collect Request Scam

Cybercriminals create fake “collect requests” and send it to many users asking them to accept the “collect request” to receive money from them.



Stranger requested money from you
+91 9303568929

₹1,000

Stranger says: "To receive payment click on Pay"

Request received

Ignore this request if you already made this payment outside of Google Pay

Apr 5, 2023 3:13 PM

- When the victim accepts the fraudster’s collect request and submits the UPI PIN, money is debited from the victim’s account.
- UPI collect request is sent to the victim for payment of a specified amount. The victim does not receive any money by accepting the “collect request”.

Always remember UPI PIN is not required to receive money. Do not accept UPI collect requests from unknown sources.

UPI QR CODE Scam

UPI QR CODE SCAM

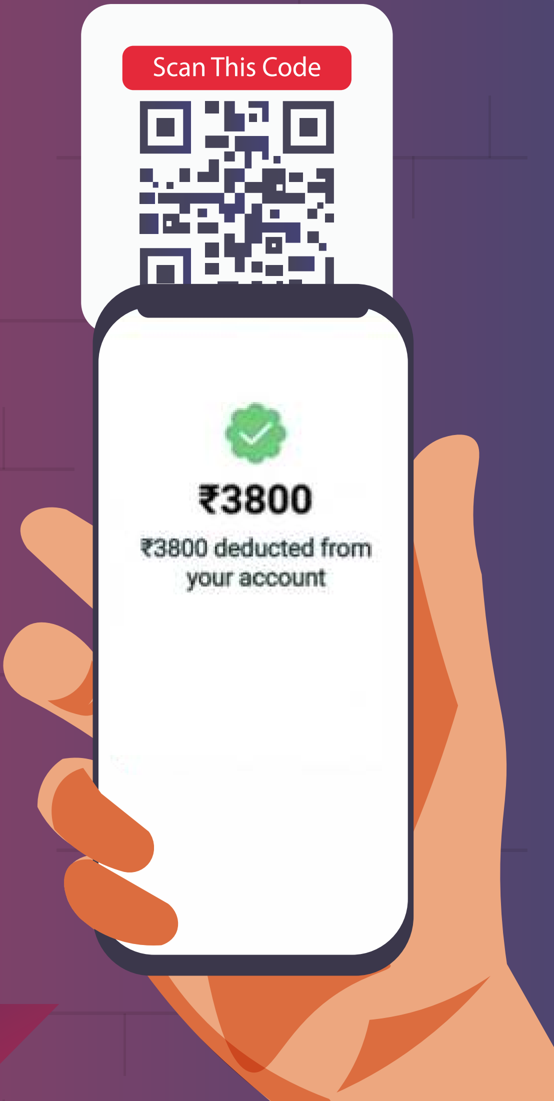
Fraudsters target people who list their products for sale on **online websites like OLX, eBay, etc.** Fraudsters call the sellers and agree to buy the product as per the listed price.

- To gain the victim's trust, the fraudster sends a minimum token amount and then sends the QR code to receive the remaining money.

- The victim, unaware of the scam, scans the QR code and submits the UPI PIN thinking they will receive the money, but instead, money is debited from their account.

- Once the victim scans the QR code and submits the UPI PIN, the account gets debited.

Always remember QR code is scanned to make a payment and not to receive any payment.



Fake Customer Care/ Contact Center Scam

Fake Customer Care/ Contact Center Scam

Cybercriminals create fake pages for customer care / contact center details pretending to be a genuine organization. The fake page displays the mobile number of fraudsters as contact center details.

When any person searches the customer care details on Google, the fraudster's details are displayed. When the number is dialed, the fraudster tricks the victim to trust them and do as they instruct.

The fraudster asks the victim to

- Share personal details
- Share banking details
- To download a remote access app

The victim downloads the app, unaware that the fraudster has access to the screen. The fraudster misuses these details, executes the fraud and steals the victim's money.

Always visit the official website for customer care or contact details.

Remote access app scam

```
( function  (ko, datacontext)  } }
 <div style="background-image:url('/pix/samples/bg1.gif');
    background . text- todoitem ;
    height . text - :200px;">
<p>The image can be tiled across the background, while the text runs across the top.</p>
</div>

/ /  persisted properties

<html> <p style="font-weight:bold;">HTML font code is done using CSS.</p>
<html> <body style="background-color:yellowgreen;color:white;">
<html> <.todolistid = data.todoidb;

  / / Non - persisted properties
   <html> <errorMessage = ko . observable() ;

 <p style="color:orange;">HTML font code is done using CSS.</p>

   function  todoitem(data) {;
     var  self = this ;
     data = dta  ll { } ;
<p>You can make <span style="font-style:italic">some</span> the HTML 'span' tag.
<p>You can bold <span style="">parts</span> of your text using the HTML tag.</p>

<html> <p style="font-weight:bold;"
>HTML font code is done using CSS.</p>
<html> <body style="background-
color:yellowgreen;
color:white;">
<html> <.todolistid = data.todoidb;

         todoitem(data) { ;
         var  self = this ;
         data = dta  ll { } ;

         todoitem(data) { ;
         var  self = this ;
         data = dta  ll -----2{ } ;
```

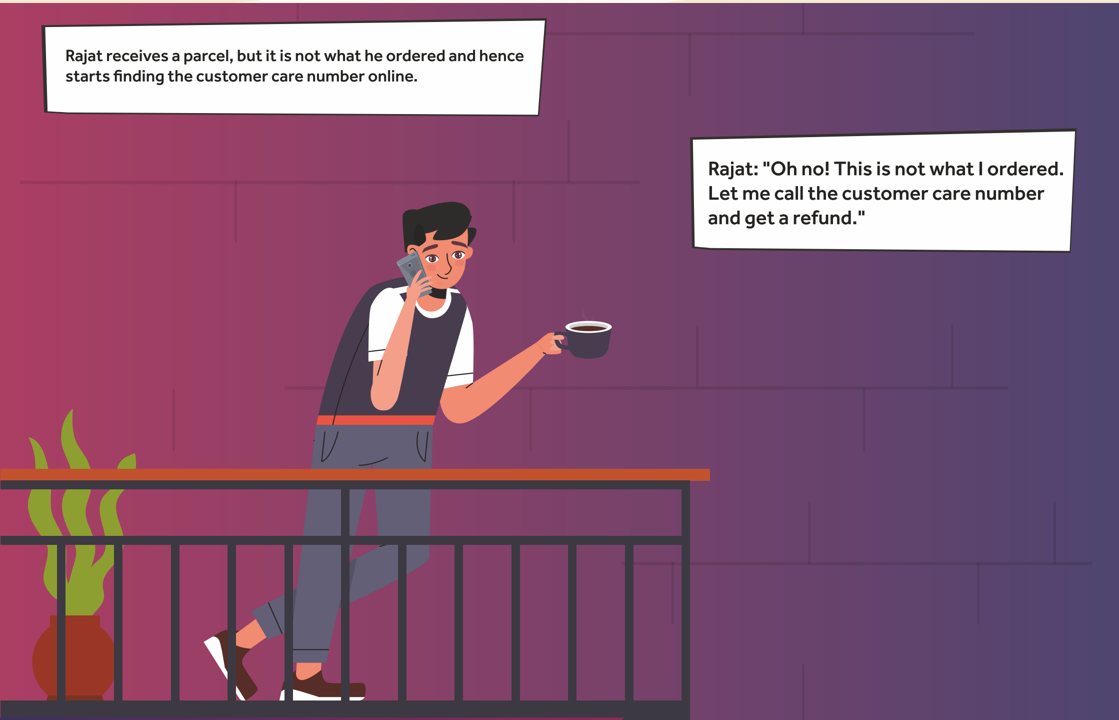
```
  / / Non - persisted properties
   <html> <errorMessage = ko . observable() ;

 <p style="color:orange;">HTML font code is done using CSS.</p>

   function  todoitem(data) { ;
     var  self = this ;
     data = dta  ▮ { } ;
<p>You can make <span style="font-style:italic">some</span> the HTML 'span' tag.
<p>You can bold <span style="">parts</span> of your text using the HTML tag.</p>
       <p>You can make----------- <span style="font- alic">
       <p>You can make----------- <span style="font- alic">
       <p>You can make----------- <span style="font- alic">
       <p>You can make----------- <span style="font- alic">
       <p>You can make----------- <span style="font- alic">
       todoitem(data) { ;
       var  self = this ;
       data = dta  ll -----2{ } ;
```

The fraudster is working on developing a website and ensuring that the customer care number created by her is ranked on top of search results.

Fraudster: "This is perfect, no one will be able to suspect this is a fake number."

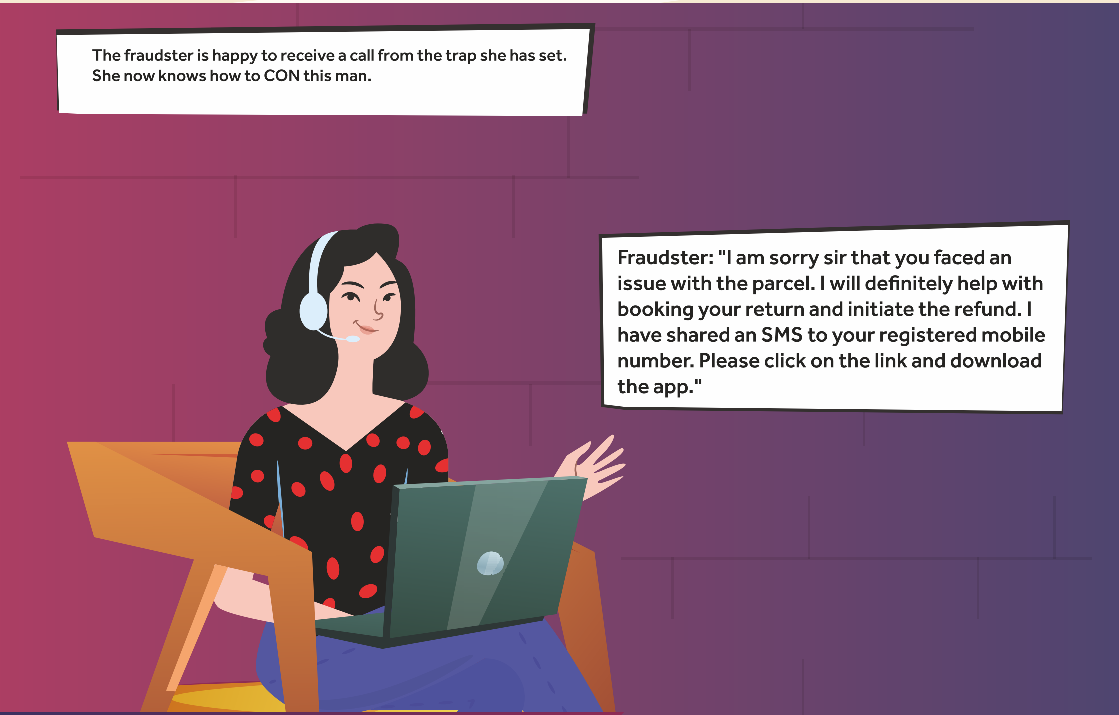


Rajat receives a parcel, but it is not what he ordered and hence starts finding the customer care number online.

Rajat: "Oh no! This is not what I ordered. Let me call the customer care number and get a refund."

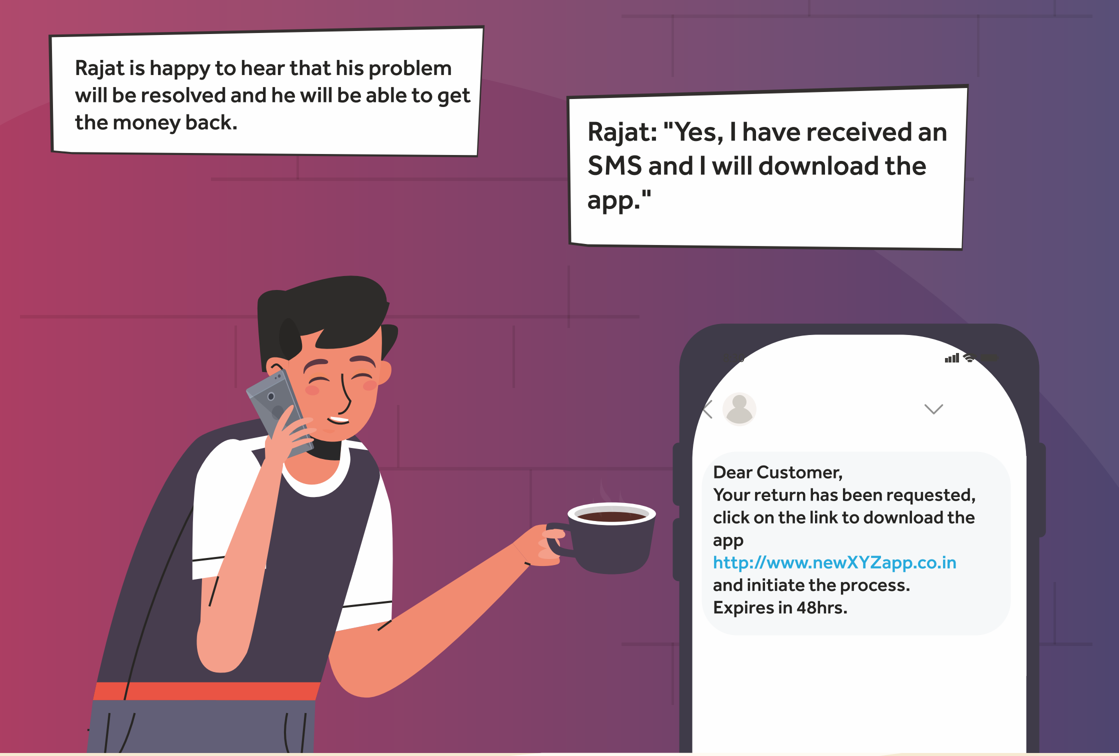
Rajat starts searching for the customer care number and finds it. He clicks on the first number that shows up and asks for the return & refund to be initiated.

Rajat: "Hello! I received a parcel and it is not what I ordered. Please initiate the process for return and refund."



The fraudster is happy to receive a call from the trap she has set. She now knows how to CON this man.

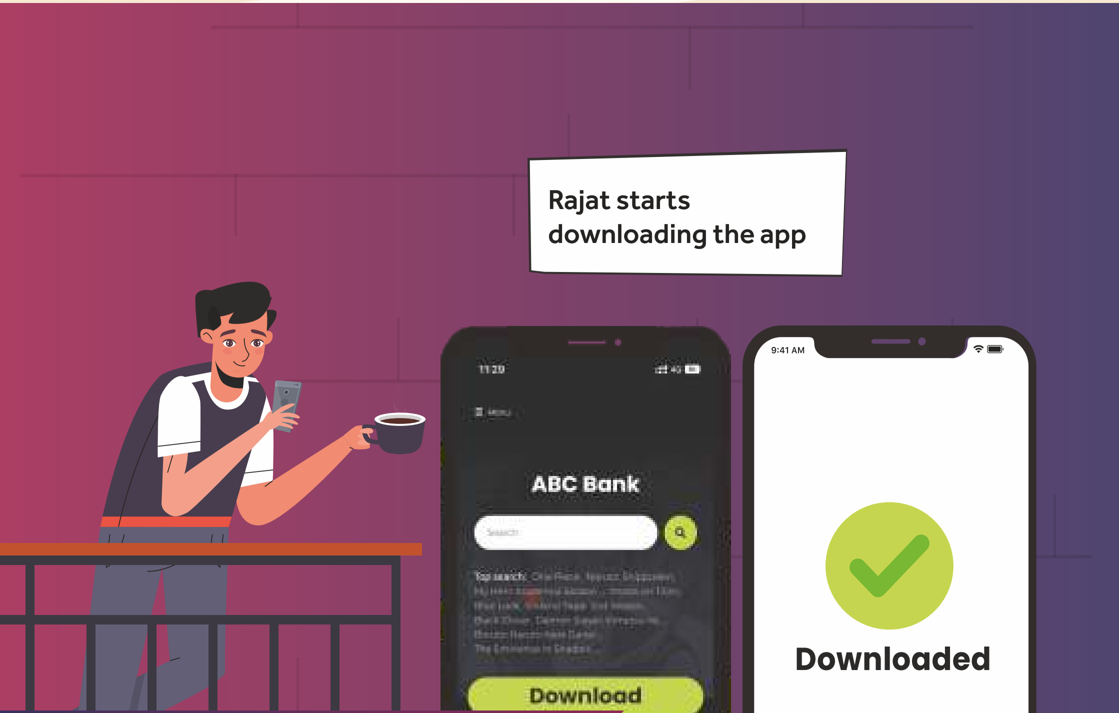
Fraudster: "I am sorry sir that you faced an issue with the parcel. I will definitely help with booking your return and initiate the refund. I have shared an SMS to your registered mobile number. Please click on the link and download the app."



Rajat is happy to hear that his problem will be resolved and he will be able to get the money back.

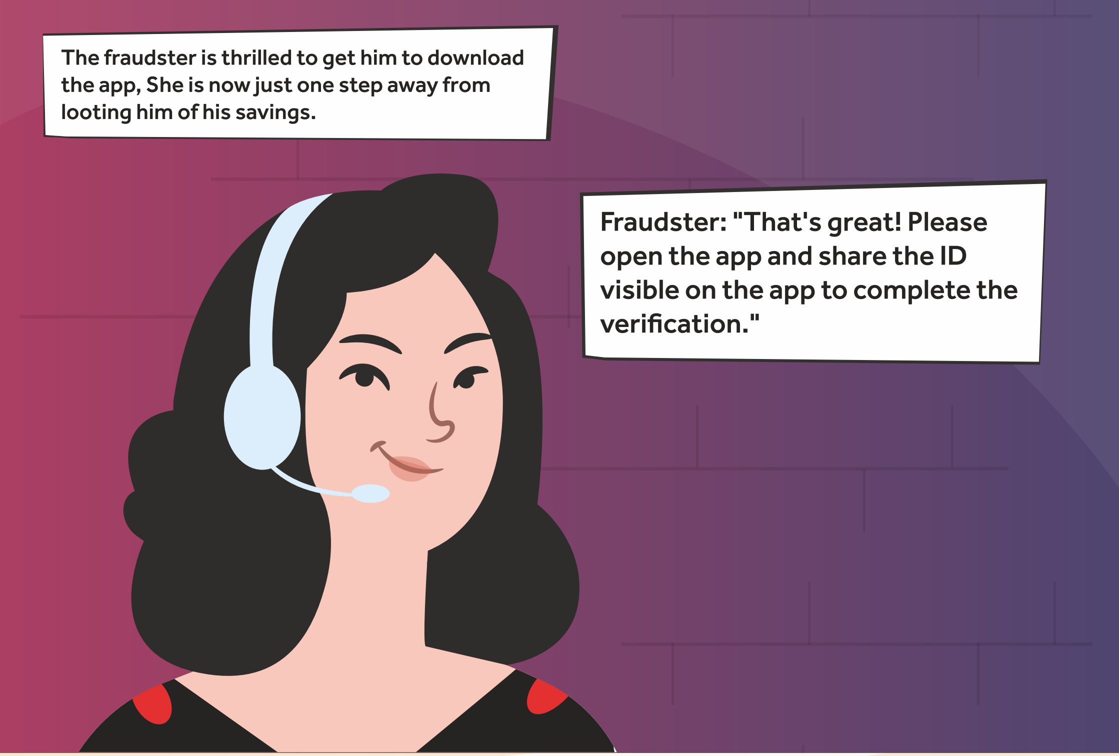
Rajat: "Yes, I have received an SMS and I will download the app."

Dear Customer,
Your return has been requested, click on the link to download the app
http://www.newXYZapp.co.in
and initiate the process.
Expires in 48hrs.

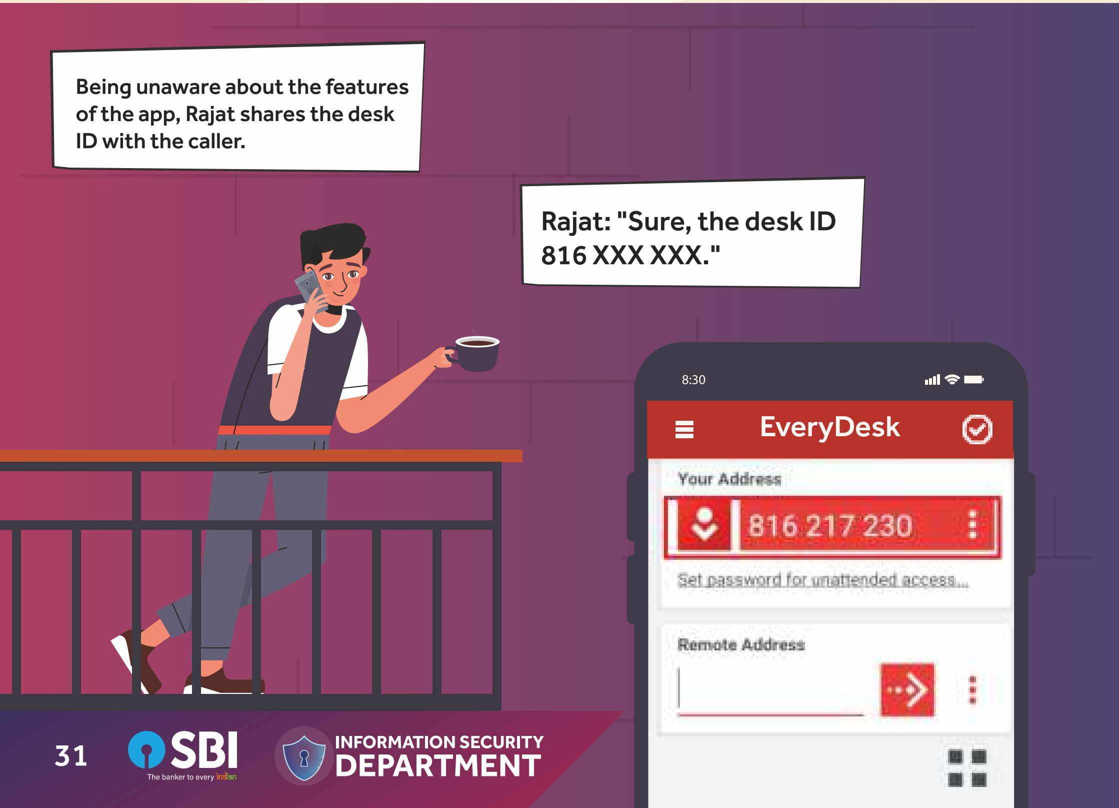


Rajat starts downloading the app

The fraudster is thrilled to get him to download the app, She is now just one step away from looting him of his savings.


Fraudster: "That's great! Please open the app and share the ID visible on the app to complete the verification."

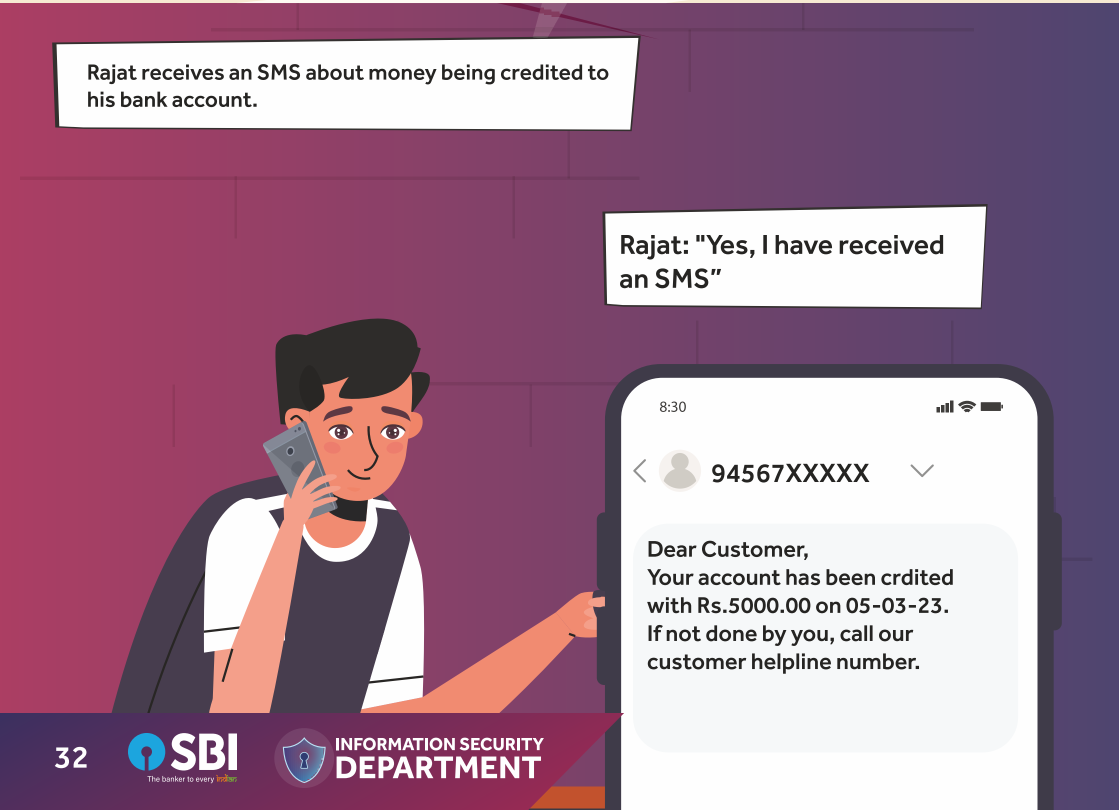
Being unaware about the features of the app, Rajat shares the desk ID with the caller.


Rajat: "Sure, the desk ID 816 XXX XXX."
8:30
EveryDesk
Your Address
816 217 230
Set password for unattended access...
Remote Address

The fraudster now sends another SMS that shows that the refund amount has been credited to Rajat.

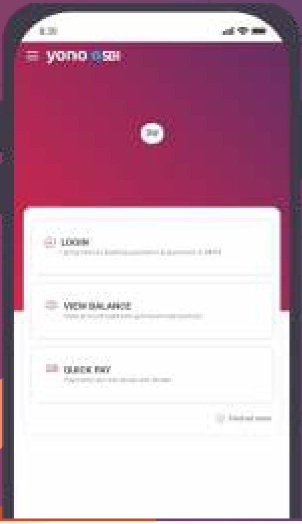
Fraudster: “Thank you for sharing the ID sir, we have initiated the refund, kindly check your bank account to confirm that you have received the refund."

Rajat receives an SMS about money being credited to his bank account.



Dear Customer,
Your account has been crdited with Rs.5000.00 on 05-03-23.
If not done by you, call our customer helpline number.

After receiving the message, Rajat now opens his bank app to check if the payment has been credited.



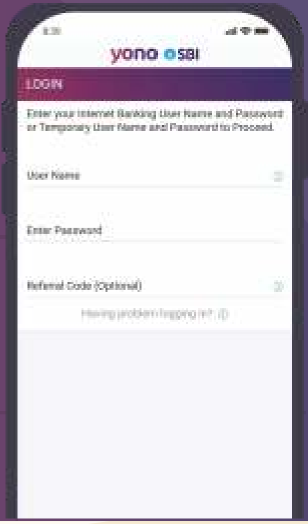
8:30

yono SBI

LOGIN

VIEW BALANCE

QUICK PAY



8:30

yono SBI

LOGIN

Enter your Internet Banking User Name and Password or Temporary User Name and Password to Proceed.

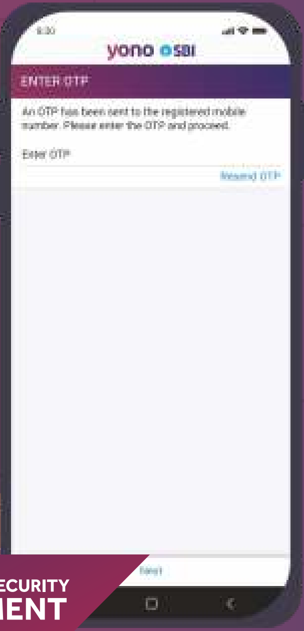
User Name

Enter Password

Referral Code (Optional)

Having problem logging in?

Rajat logs into his account without realising the screensharing app is still running on his device.



8:30

yono SBI

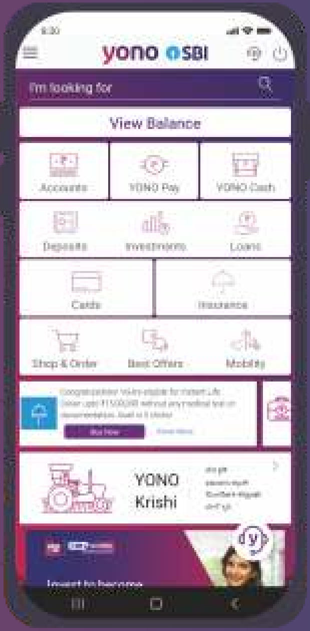
ENTER OTP

An OTP has been sent to the registered mobile number. Please enter the OTP and proceed.

Enter OTP

Resend OTP

Next



8:30

yono SBI

I'm looking for

View Balance

Accounts | YONO Pay | YONO Cash

Deposits | Investments | Loans

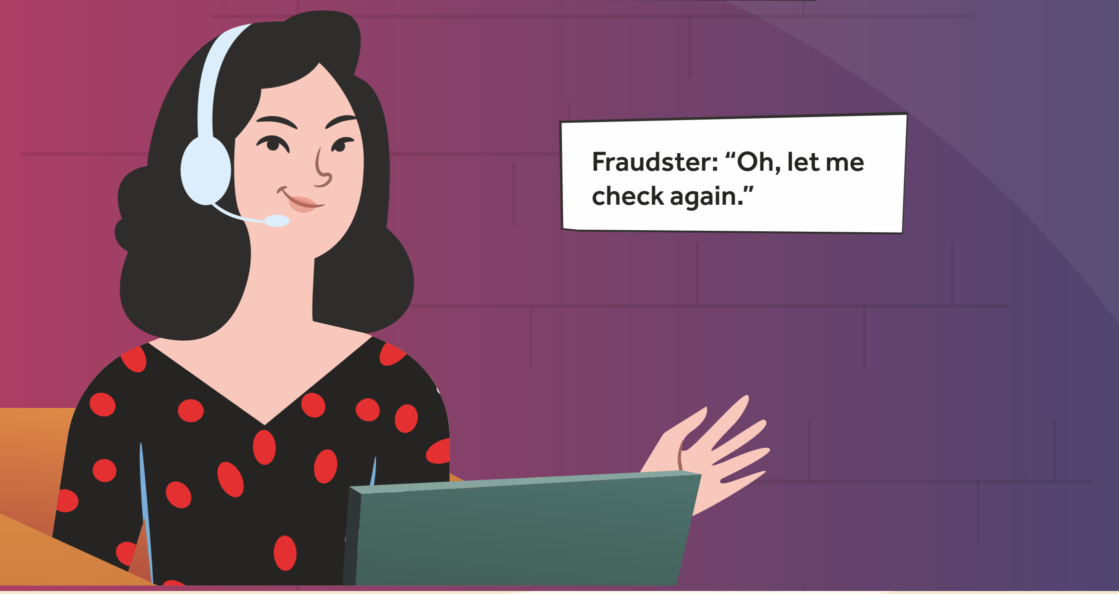
Cards | Insurance

Shop & Order | Best Offers | Mobility

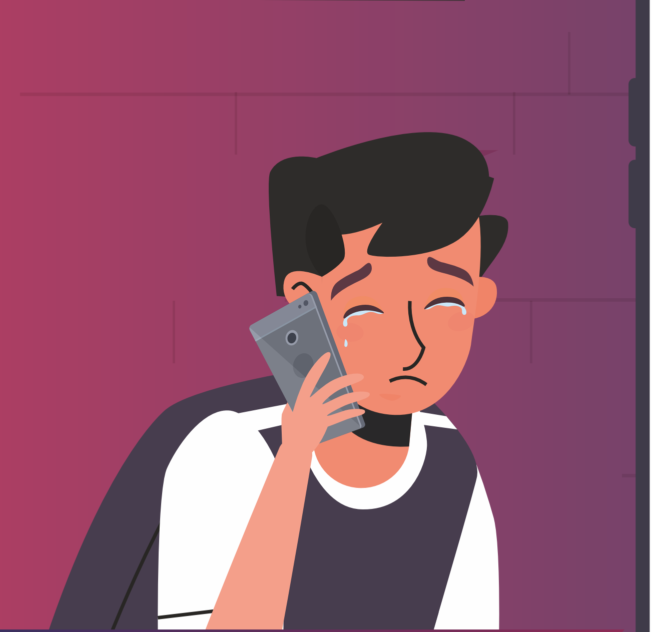
YONO Krishi

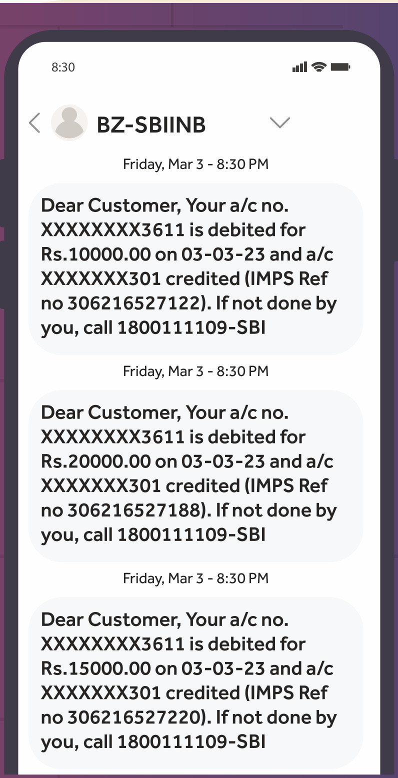
Invest to become

With the remote access app working in the background, the fraudster gets access to Rajat's bank account and initiates withdrawing money.



Rajat starts receiving debit messages on his phone.





BZ-SBIINB

Friday, Mar 3 - 8:30 PM

Dear Customer, Your a/c no. XXXXXXXX3611 is debited for Rs.10000.00 on 03-03-23 and a/c XXXXXXX301 credited (IMPS Ref no 306216527122). If not done by you, call 1800111109-SBI

Friday, Mar 3 - 8:30 PM

Dear Customer, Your a/c no. XXXXXXXX3611 is debited for Rs.20000.00 on 03-03-23 and a/c XXXXXXX301 credited (IMPS Ref no 306216527188). If not done by you, call 1800111109-SBI

Friday, Mar 3 - 8:30 PM

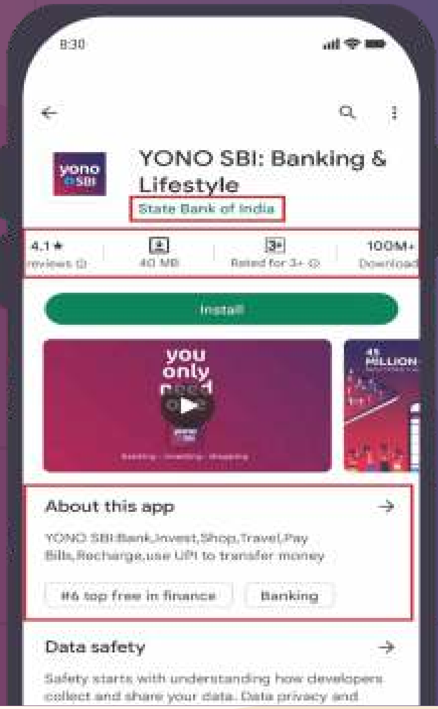
Dear Customer, Your a/c no. XXXXXXXX3611 is debited for Rs.15000.00 on 03-03-23 and a/c XXXXXXX301 credited (IMPS Ref no 306216527220). If not done by you, call 1800111109-SBI

How remote access scam can be avoided:

1. Never search Customer Care Number online. Always visit the official website and look for the Customer Care Number. For SBI Customer Care Number you can visit https://sbi.co.in

2. To receive a refund, we never have to download any kind of app or share information like login details, OTP or PIN with anyone. Always remember that an authentic provider will directly transfer the refund amount to the account through which the transaction was done previously.

3. Before downloading any app always check if the app is from a genuine provider by going through its reviews, number of downloads and always read the "About this app" page to understand the functionality of the app.



8:30

YONO SBI: Banking & Lifestyle

State Bank of India

4.1 ★	40 MB	3+	100M+
reviews ⓘ		Rated for 3+ ⓘ	Download

About this app →

YONO SBI:Bank,Invest,Shop,Travel,Pay Bills,Recharge,use UPI to transfer money

#6 top free in finance

Banking

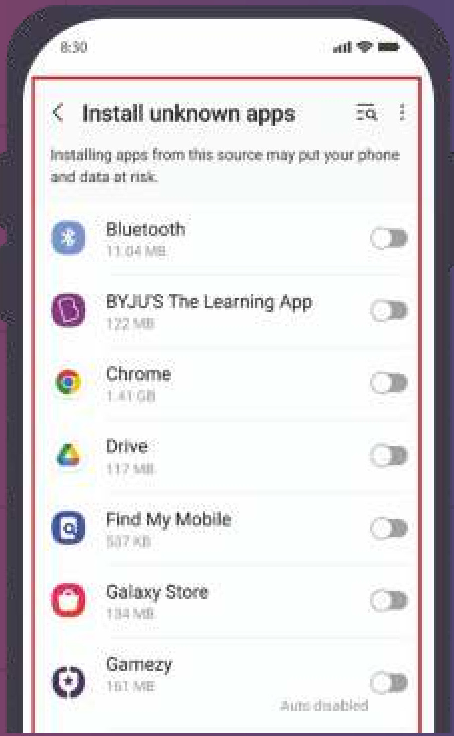
Data safety →

Safety starts with understanding how developers collect and share your data. Data privacy and

4. Turn off or Disable "Allow Installation of apps from sources other than the "Play Store or App Store" option under Settings - Security.

5. Beware of persons asking you to download any apps, as such apps may help them access your device.

6. If you suspect that your device is behaving abnormally, immediately disconnect your device from the internet and restart the device.



8:30

Install unknown apps

Installing apps from this source may put your phone and data at risk.

App	Size
Bluetooth	11.04 MB
BYJU'S The Learning App	122 MB
Chrome	1.41 GB
Drive	117 MB
Find My Mobile	507 KB
Galaxy Store	134 MB
Gamezy	161 MB

Auto disabled

Stay Alert & #SafeWithSBI

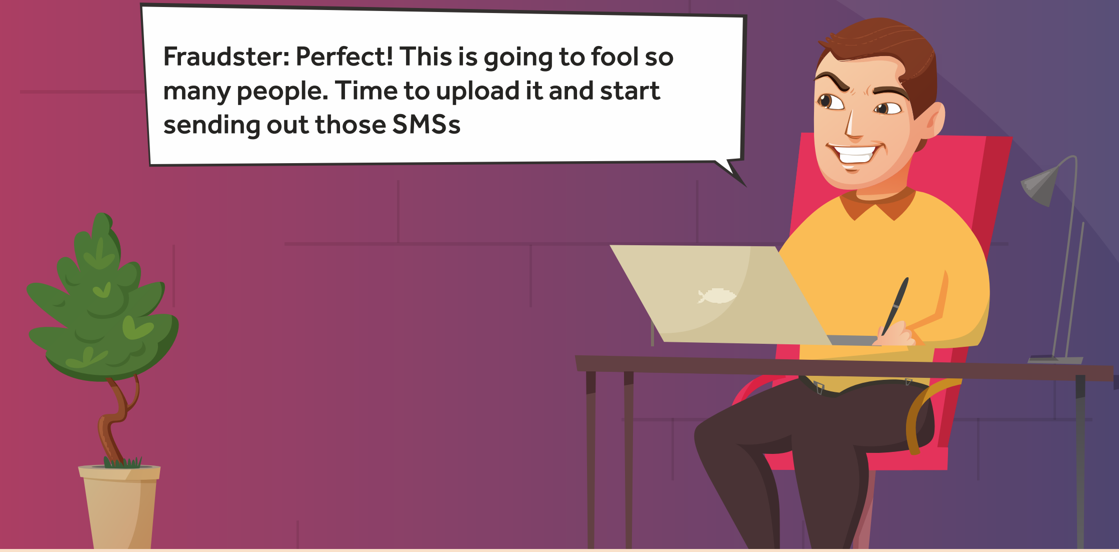
FAKE BANK APP SCAM

The fraudster is working diligently and creating a fake version of the lending app. They know that this is just the first step in their plan to scam unsuspecting victims.

With the fake app ready, the fraudster knows that many people will be unaware of the difference between a fake and a real bank app. They will be tempted to download the fake bank app, thinking that it is legitimate.

Fraudster: "Ha! This will be the perfect way to steal people's money!"
Please Wait (45%)

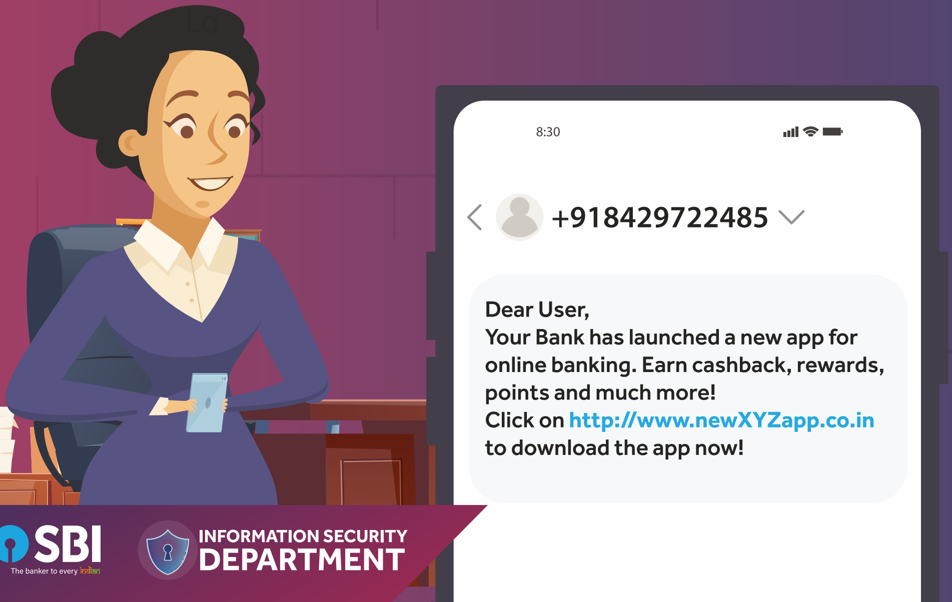
The fraudster sends out fake SMSs, pretending to be the bank and urging people to download the app. They know that many people will fall for the trick.


Fraudster: Perfect! This is going to fool so many people. Time to upload it and start sending out those SMSs

Many unsuspecting victims receive the SMS message with a fake link and believe that it is a legitimate message from their bank. They click on the link to download the app, thinking it will improve their banking experience.

Isha is seen sitting at her desk, working on her computer when her phone buzzes with an incoming message.

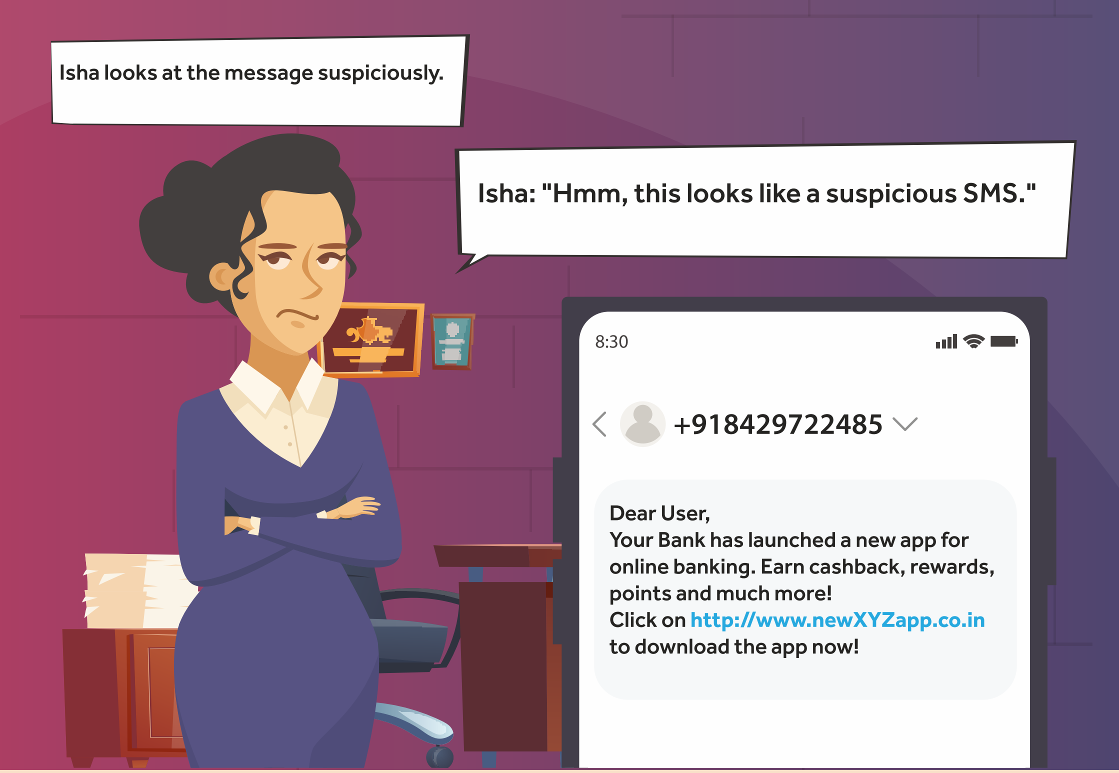
Isha receives an SMS from her bank regarding a new online banking app. However, she starts to doubt its authenticity.



8:30

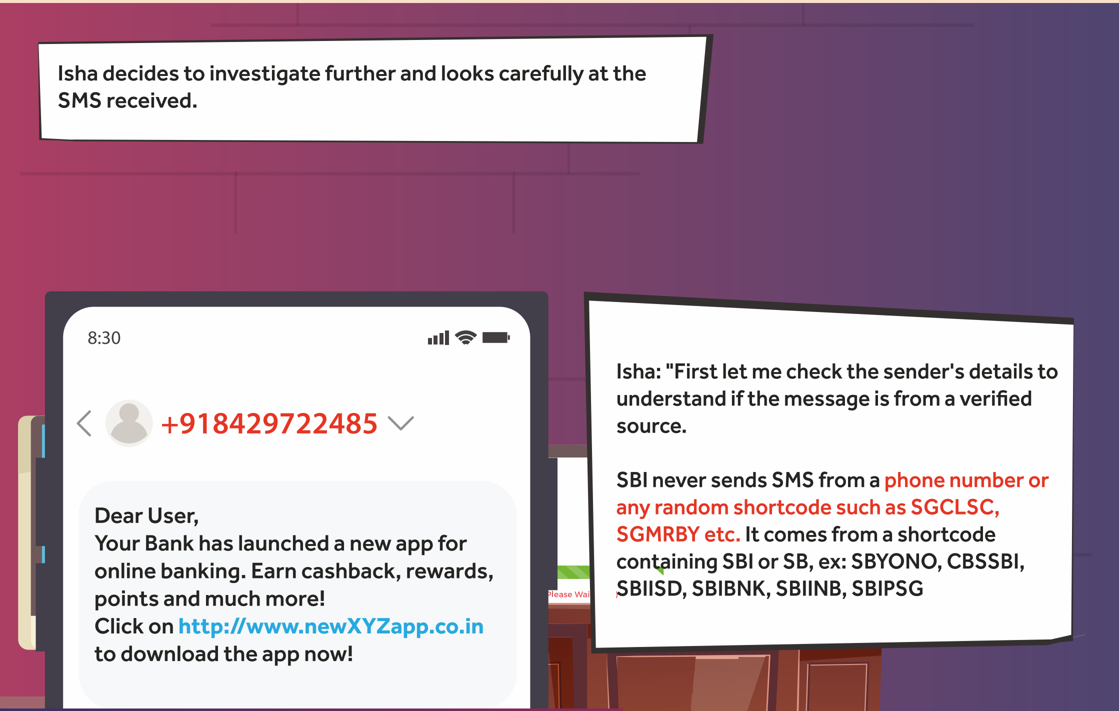
+918429722485

Dear User,
Your Bank has launched a new app for online banking. Earn cashback, rewards, points and much more!
Click on http://www.newXYZapp.co.in to download the app now!



Isha looks at the message suspiciously.

Dear User,
Your Bank has launched a new app for online banking. Earn cashback, rewards, points and much more!
Click on http://www.newXYZapp.co.in to download the app now!



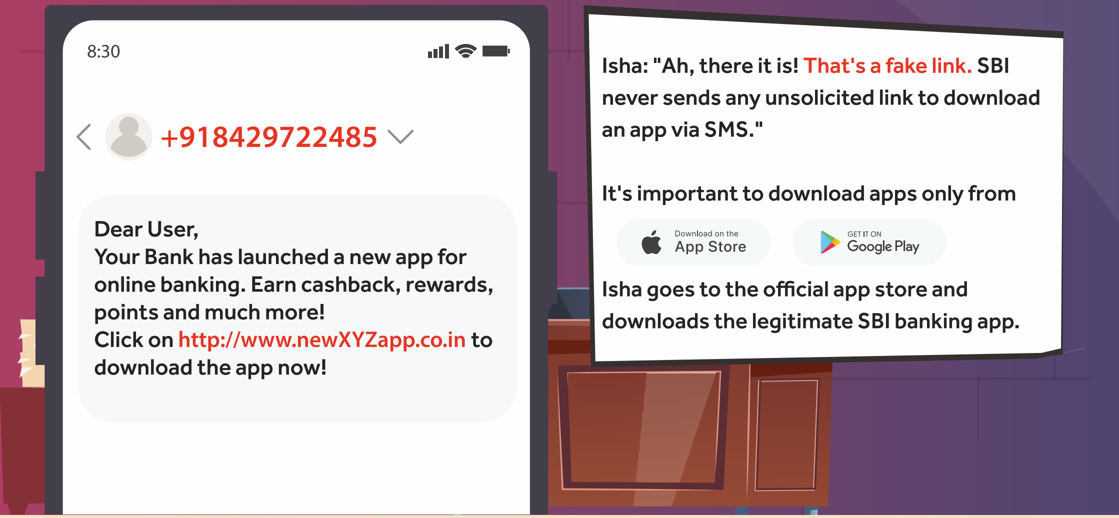
Isha decides to investigate further and looks carefully at the SMS received.

Dear User,
Your Bank has launched a new app for online banking. Earn cashback, rewards, points and much more!
Click on http://www.newXYZapp.co.in to download the app now!

Isha: "First let me check the sender's details to understand if the message is from a verified source.

SBI never sends SMS from a phone number or any random shortcode such as SGCLSC, SGMRBY etc. It comes from a shortcode containing SBI or SB, ex: SBYONO, CBSSBI, SBIISD, SBIBNK, SBIINB, SBIPSG

Isha decides to investigate further and looks carefully at the SMS received.



8:30

+918429722485

Dear User,
Your Bank has launched a new app for online banking. Earn cashback, rewards, points and much more!
Click on http://www.newXYZapp.co.in to download the app now!

Isha: "Ah, there it is! That's a fake link. SBI never sends any unsolicited link to download an app via SMS."

It's important to download apps only from

Download on the App Store   GET IT ON Google Play

Isha goes to the official app store and downloads the legitimate SBI banking app.

- **Always download bank apps from verified sources such as Google Play Store / Apple App Store. Do not download apps from third-party websites or app stores.**
- **Be cautious of unsolicited SMS or emails that claim to be from your bank and ask you to download a new app or click on a link.**
- **Verify the authenticity of the message by checking the shortcode and contacting your bank.**
- **Do not share your login credentials or personal information with anyone, even if they claim to be from your bank.**
- **Regularly monitor your bank accounts and transactions to detect any unauthorized activity.**
- **Report any suspicious activity or transactions to your bank immediately.**
- **Remember, it is always better to be safe than sorry. Be cautious of any messages or emails that ask you to download an app or share personal information.**

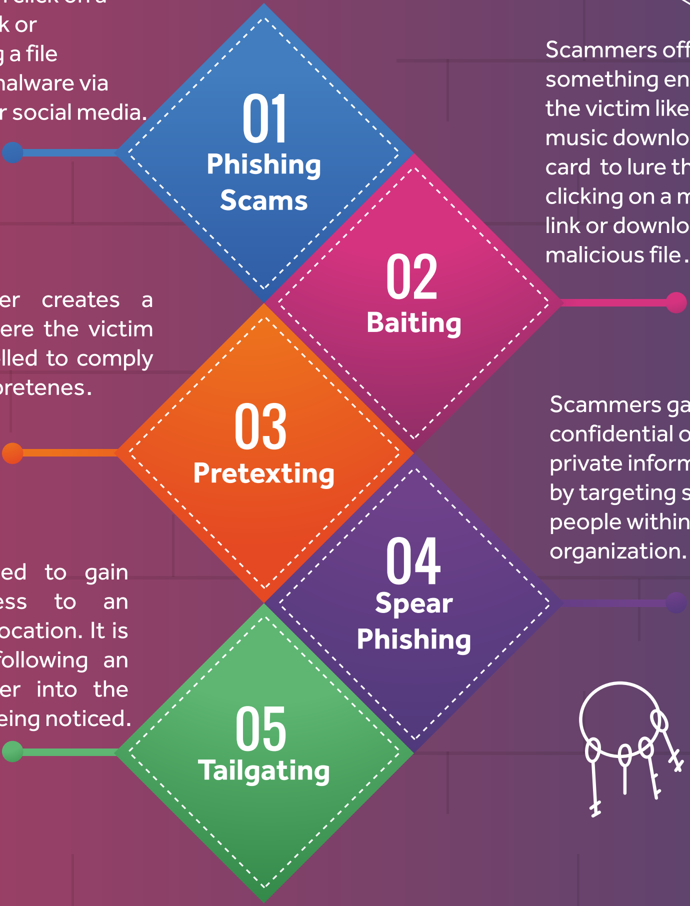
Stay Alert & #SafeWithSBI

Social Engineering Attacks

What is Social Engineering?

Social engineering is the use of psychological manipulation to influence individuals or groups into divulging sensitive, private or financial information.

Types of Social Engineering Attacks:



01 Phishing Scams

Attackers trick victims by making them click on a malicious link or downloading a file containing malware via text, email or social media.

02 Baiting

Scammers offer something enticing to the victim like free music download or gift card to lure them into clicking on a malicious link or download a malicious file.

03 Pretexting

The attacker creates a scenario where the victim feels compelled to comply under false pretenes.

04 Spear Phishing

Scammers gain confidential or private information by targeting specific people within an organization.

05 Tailgating

An attack used to gain physical access to an unauthorized location. It is achieved by following an authorized user into the area without being noticed.

How Scammers use emotions to trick/manipulate you:

Curiosity
Creating a sense of curiosity by enticing the victim

Fear
Creating a sense of fear by pressuring the victim into taking immediate action

Empathy
Using empathy to establish a connection with the victim and gain their trust

Urgency
Creating a sense of urgency

Familiarity
Pretending to be someone you know

Authority
Pretending to be someone in a position of authority

How to Prevent Social Engineering Attacks

- Refrain from clicking on any suspicious links or downloading any unknown files.
- Use two-factor authentication to protect your account from scammers trying to gain access.
- Keep all software, including operating systems, browsers and plugins up to date with the latest patches and security updates.
- Limit access to sensitive information to only those who require it to perform their job duties.
- Establish clear and concise security policies and guidelines for employees to follow.
- Educate yourself and stay up to date with all the recent types of attacks taking place.

Safe Internet Banking Practices

Things to Remember when using Internet Banking

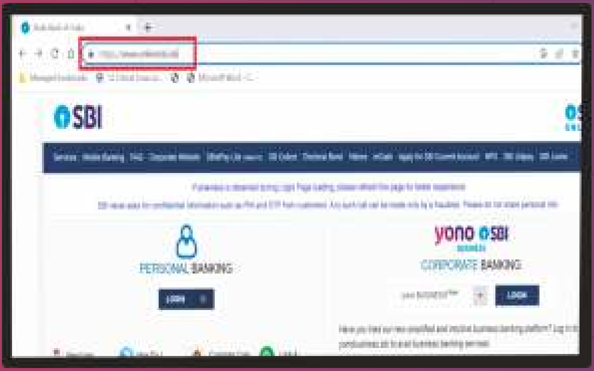
Keep your login credentials safe: Your internet banking login credentials (i.e. usernameand password) are sensitive information that should not be shared with anyone.

Use secure internet connections: Always use a secure internet connection when accessing your internet banking account and check for HTTPS Secure Connection.

Don’t save login credentials: Avoid saving your login credentials on a public computer or in your browser, as this can be a security risk.

Logout properly: Always logout of your internet banking account properly, and don't simply close the browser window.

How to Access the Internet Banking Portal Securely

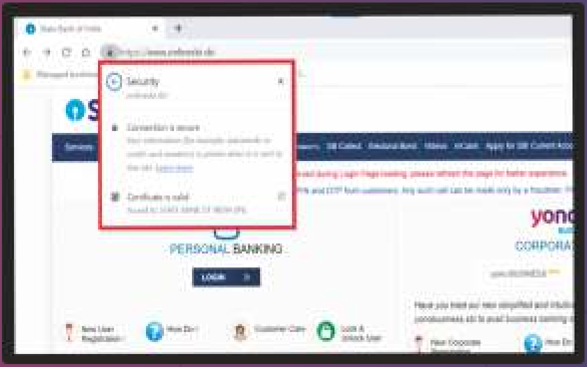


STEP 1:

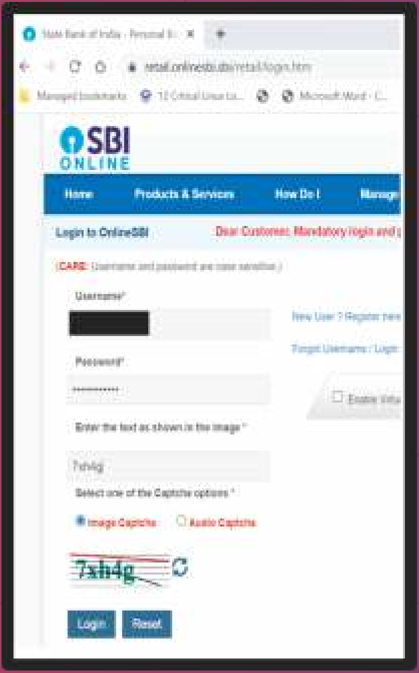
Go to the Online SBI official page

STEP 2:

Check if the website is secure by clicking on the padlock and verifying that the certificate belongs to "STATE BANK OF INDIA [IN]" and is valid



How to Access the Internet Banking Portal Securely



Login to OnlineSBI

Dear Customer, Mandatory login and

(CARE: Username and password are case sensitive.)

Username*

[redacted]

Password*

•••••••••••

Enter the text as shown in the image *

7xh4g

Select one of the Captcha options *

● Image Captcha ○ Audio Captcha

7xh4g

Points to remember:

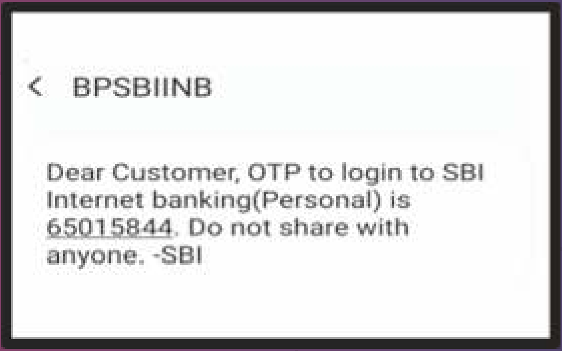
- Keep a strong and unique login password having combination of alphabets, numbers & special characters.
- Never share your login credentials with anyone.
- Never share the OTP to login with anyone as it would grant them access your internet banking.
- If you receive SMS for OTP to login without you initiating the access to your INB, instantly change the INB password and inform your bank.

STEP 3:

Login to your SBI bank account by entering your user ID, password and captcha

STEP 4:

Using 2 factor authentication and enter the OTP received on registered mobile number to login



< BPSBIINB

Dear Customer, OTP to login to SBI Internet banking(Personal) is 65015844. Do not share with anyone. -SBI

Security Features That Can Be Enabled to Experience Secure Digital Banking

- Bank provides you various online banking platforms such as ATM Cards, UPI, internet banking channels, etc. to perform digital transactions
- There are security features provided by bank that should be enabled to experience secure digital banking

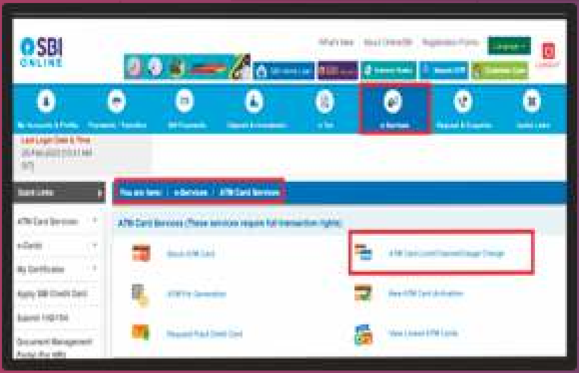
ATM Card Security:

- ATM cards can be used to withdraw money from ATM machines, to carry out transactions at POS machines and to perform e-commerce transactions
- There are various functionality provided by Bank to secure the ATM cards from fraudulent transactions or reduce the exposure of loss.

Let us understand how can we enable these features:

Set ATM Card Limit

By setting a daily limit on your ATM card, you can limit the amount of money that can be withdrawn from your account in case your card is lost or stolen. This can prevent unauthorized access to your funds and minimize the risk of financial losses.

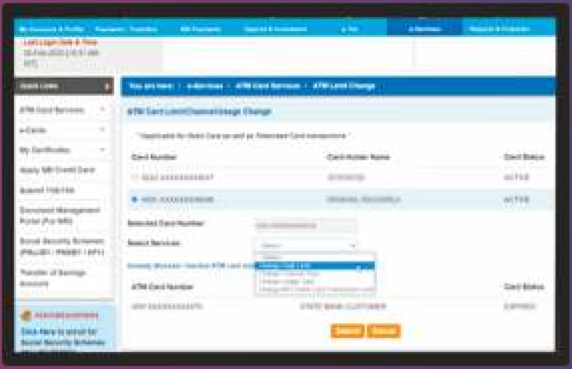

SBI ONLINE
Quick Links
ATM Card Services
e-Cards
My Certificates
Apply SBI Credit Card
Submit 15G/15H
Document Management Portal (For NRI)
You are here: e-Services / ATM Card Services
ATM Card Services (These services require full transaction rights)
Block ATM Card
ATM Card Limit/Channel/Usage Change
ATM Pin Generation
New ATM Card Activation
View Linked ATM Cards

STEP 1:

Under E Services go to ATM Card Limit / Channel / Usage Change

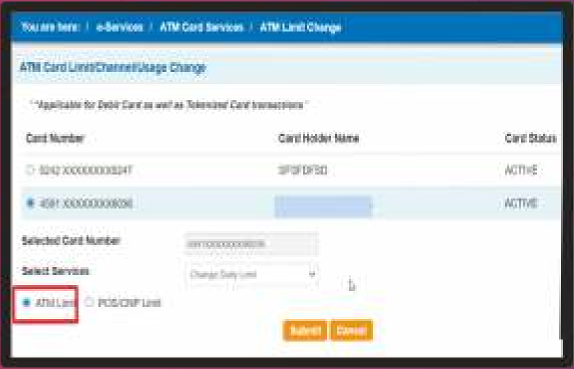
STEP 2:

Select account number and then select Change Limit from the Dropdown menu



Set ATM Card Limit

We can set the limit of ATM cards at ATM machines, POS & CNP (Card not present i.e., e-commerce) transaction to reduce the amount of loss in case the ATM card & PIN is lost or stolen.



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

"*Applicable for Debit Card as well as Tokenized Card transactions"

Card Number	Card Holder Name	Card Status
○ 6242 XXXXXXXXX8247	SFDFDFSD	ACTIVE
● 4591 XXXXXXXXX9036	[redacted]	ACTIVE

Selected Card Number: 4591XXXXXXXXX9036

Select Services: Change Daily Limit

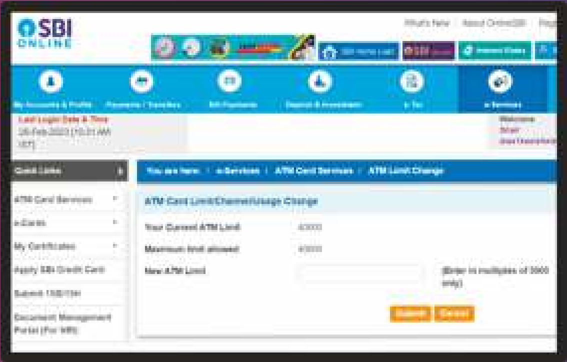
● ATM Limit ○ POS/CNP Limit

STEP 3:

Select the option ATM Limit and then click on Submit

STEP 4:

Set new ATM Limit and then click on Submit



Last Login Date & Time
26-Feb-2023 [10:31 AM IST]

You are here: / e-Services / ATM Card Services / ATM Limit Change

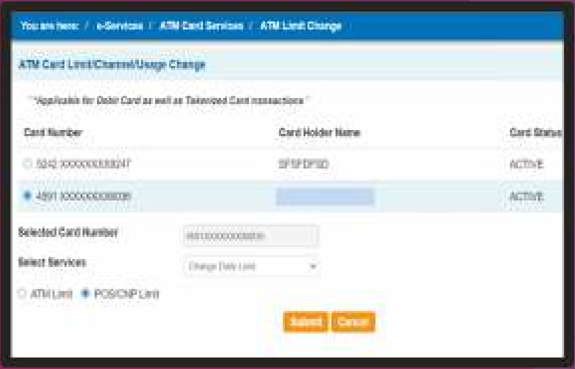
ATM Card Limit/Channel/Usage Change

Your Current ATM Limit: 40000

Maximum limit allowed: 40000

New ATM Limit: (Enter in multiples of 5000 only)

Set POS/CNP Limit



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

"Applicable for Debit Card as well as Tokenized Card transactions"

Card Number	Card Holder Name	Card Status
○ 5242 XXXXXXXX8247	SFSFDFSD	ACTIVE
● 4591 XXXXXXXX8036		ACTIVE

Selected Card Number: 4591XXXXXXXX8036

Select Services: Change Daily Limit

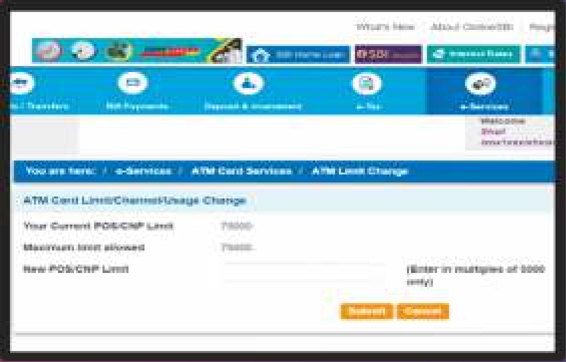
○ ATM Limit ● POS/CNP Limit

STEP 5:

Select the option POS/CNP Limit and then click on Submit

STEP 6:

Set new POS/CNP Limit and then click on Submit



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

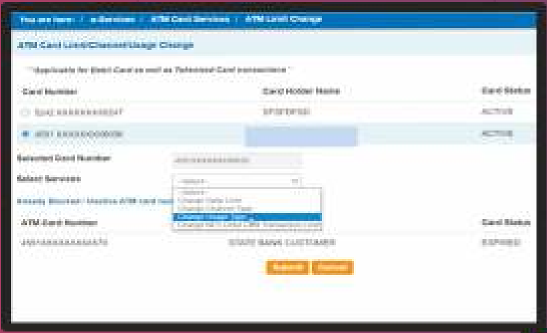
Your Current POS/CNP Limit: 75000

Maximum limit allowed: 75000

New POS/CNP Limit: (Enter in multiples of 5000 only)

Enable / Disable International Usage of ATM Card

International transactions can also be performed through ATM card without any second factor authentication such PIN or OTP. Hence, it is recommended to keep international transaction on your ATM card disabled to prevent any fraudulent transactions in case the card is lost or stolen.



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

Card Number	Card Holder Name	Card Status
○		ACTIVE
●		ACTIVE

Selected Card Number

Select Services: -Select-

ATM Card Number		Card Status
	STATE BANK CUSTOMER	EXPIRED

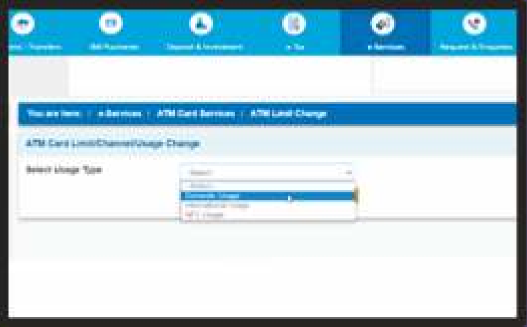
Submit Cancel

STEP 1:

Go back to the dropdown menu and select Change Usage Type

STEP 2:

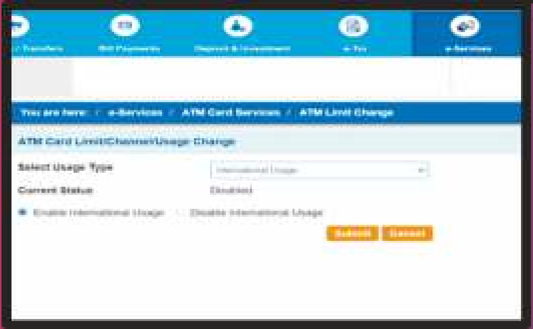
Select International Usage and click Submit



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

Select Usage Type: -Select-



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

Select Usage Type: International Usage

Current Status: Disabled

● Enable International Usage ○ Disable International Usage

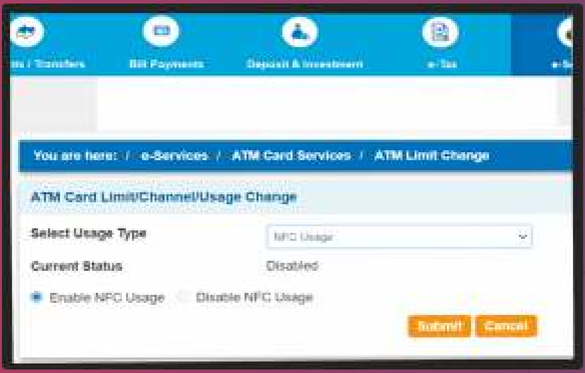
Submit Cancel

STEP 3:

Select whether you want to disable or enable International Transactions

Enable / Disable NFC Usage of ATM Card

NFC is a facility provided to make transaction of up to Rs. 5000/- daily without entering the ATM PIN. If NFC transactions are not performed by you, it is recommended to disable the NFC usage on your card. If your card is lost and NFC is enabled, anyone can perform NFC transaction of Rs. 5000/- daily.



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

Select Usage Type: NFC Usage

Current Status: Disabled

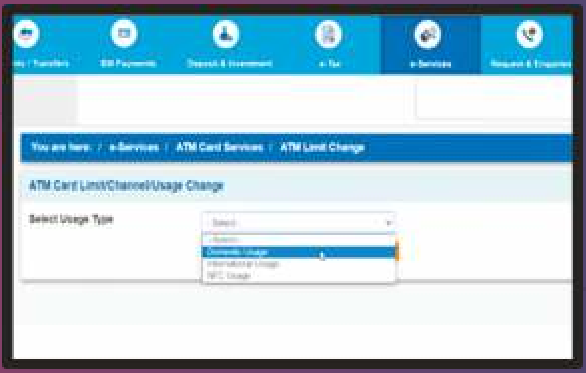
● Enable NFC Usage ○ Disable NFC Usage

STEP 1:

Go back to Usage Type and Select NFC Usage

STEP 2:

Select whether you want to disable or enable NFC Transactions



You are here: / e-Services / ATM Card Services / ATM Limit Change

ATM Card Limit/Channel/Usage Change

Select Usage Type: Select

Block ATM Card

If you suspect any fraudulent transaction through ATM card or if your ATM card is lost, you should immediately block your ATM Card through following ways:

01

Go to the Internet Banking Portal and block your ATM Card throughthe portal. Process shown on next page

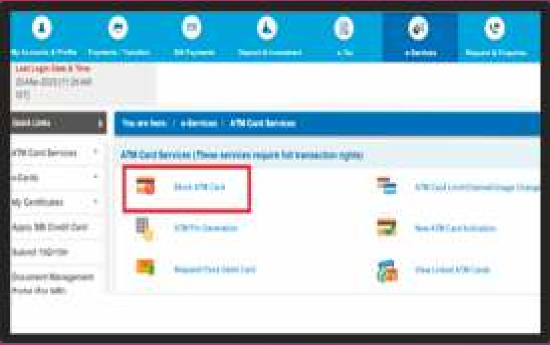
02

You can also block ATM card through the nearest SBI branch

03

You can also block your ATM card by calling on these helpline number: 1800111109, 1800 2100, 1800 1234

Block ATM Card



Last Login Date & Time [illegible]

You are here / e-Services / ATM Card Services

ATM Card Services (These services require full transaction rights)

- ATM Card Services
- e-Cards
- My Certificates
- Apply SBI Credit Card
- Submit 15G/15H
- Document Management Portal (For NRI)

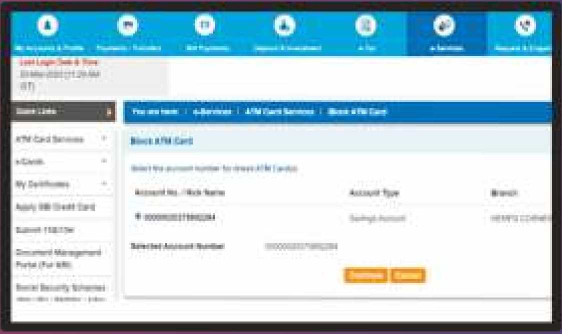
Block ATM Card | ATM Card Limit/Channel/Usage Change
ATM Pin Generation | New ATM Card Activation
Request Paid Debit Card | View Linked ATM Cards

STEP 1:

Go to the e-Services and under ATM Card Services click on Block ATM Card

STEP 2:

Select Account Number and click on Continue



Last Login Date & Time [illegible]

You are here / e-Services / ATM Card Services / Block ATM Card

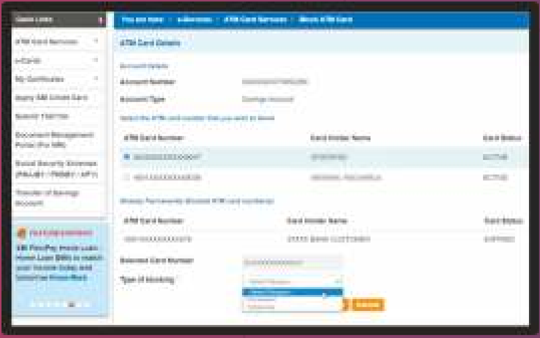
Block ATM Card

Select the account number for block ATM Card(s)

Account No. / Nick Name	Account Type	Branch
● [illegible]	Savings Account	[illegible]

Selected Account Number [illegible]

Continue Cancel



Quick Links
ATM Card Services
e-Cards
My Certificates
Apply SBI Credit Card
Submit 15G/15H
Document Management Portal (For NRI)
Social Security Schemes (PMJJBY / PMSBY / APY)
Transfer of Savings Account

You are here / e-Services / ATM Card Services / Block ATM Card

ATM Card Details

Account Details

Account Number [illegible]

Account Type Savings Account

Select the ATM card number that you want to block

ATM Card Number	Card Holder Name	Card Status
● [illegible]	[illegible]	ACTIVE
○ [illegible]	[illegible]	ACTIVE

Already Permanently Blocked ATM card number(s)

ATM Card Number	Card Holder Name	Card Status
[illegible]	[illegible]	[illegible]

Selected Card Number [illegible]

Type of blocking [illegible]

Submit

STEP 3:

Select ATM Card Number and type of Blocking and click on Submit

UPI Platform

01 UPI is a banking facility provided by default to every customer to perform easy and convenient banking transfers to persons and any merchants.

02 UPI transactions can be performed using VPA (Virtual payment identifier), registered mobile number or account numbers.

03 UPI payments can also be done through QR scans.

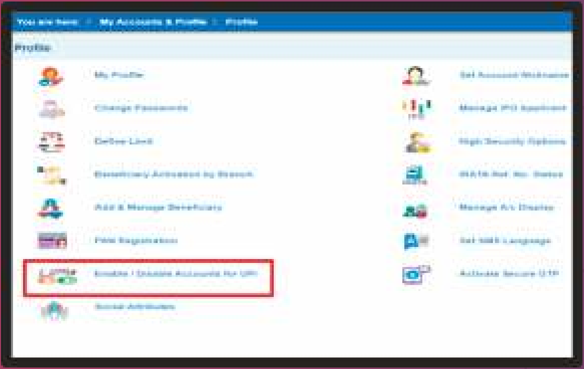
04 In case you suspects any fraudulent transactions through UPI channels, you should immediately disable the UPI Platform.

05 You can disable the UPI Platform account by going to the Internet Banking Portal shown in the next page.

06 You can also block your UPI channel on your account by calling on these helpline numbers: 1800111109, 1800 2100,1800 1234.

Enable / Disable UPI

If you notice any unauthorized transactions or suspect that your UPI account has been compromised, disabling your UPI bank account can help prevent further losses and protect your funds.

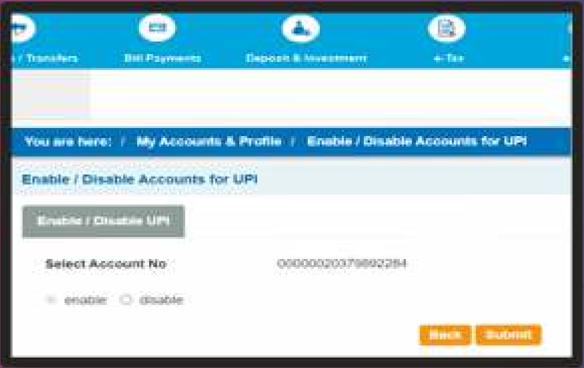


STEP 1:

Go to the option Enable / Disable Accounts for UPI from the Profile Page

STEP 2:

Select whether you want to Enable or Disable Account for UPI


/ Transfers
Bill Payments
Deposit & Investment
e-Tax
You are here: / My Accounts & Profile / Enable / Disable Accounts for UPI
Enable / Disable Accounts for UPI
Enable / Disable UPI
Back
Submit

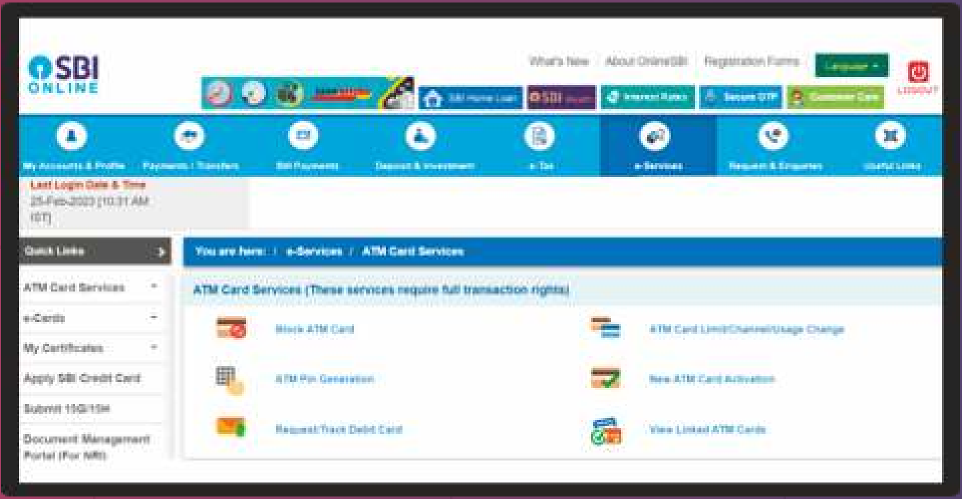
Select Account No 00000020379892284

● enable ○ disable

Safe Logout

Always logout from your INB account after performing the banking activities to prevent any unauthorized access to your account. Click on the LOGOUT Button on top right corner to safely logout from your SBI Bank Account.

Always remember you should not save your Internet Banking login credentials on your browsers as it will allow other person having access to your devices to access your INB account.



Last Login Date & Time
25-Feb-2023 [10:31 AM IST]

You are here: / e-Services / ATM Card Services

ATM Card Services (These services require full transaction rights)

Safe Mobile Banking Practices

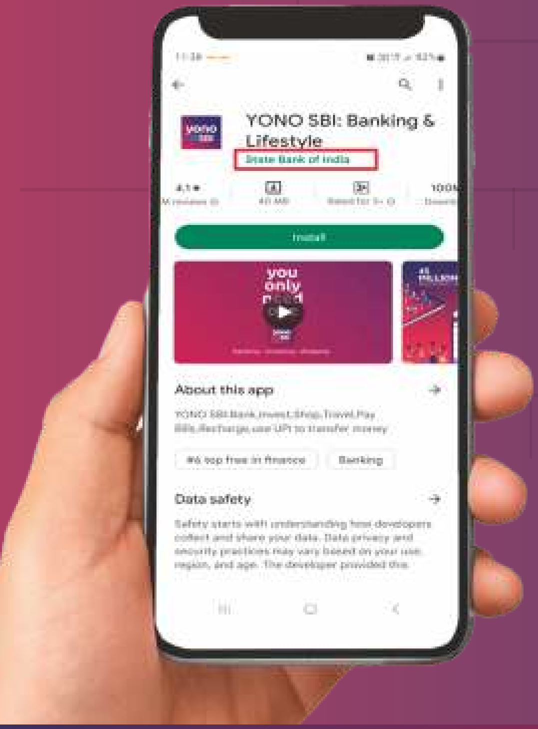
Download and Login SBI Yono App

STEP 1:

Download YONO SBI App only from official stores like Play Store or App Store and check the organization name to validate the app

STEP 2:

Tap on LOGIN Tab to go to your account



11:38

YONO SBI: Banking & Lifestyle

State Bank of India

4.1 ★ M reviews | 40 MB | Rated for 3+ | 100M+ Downloads

Install

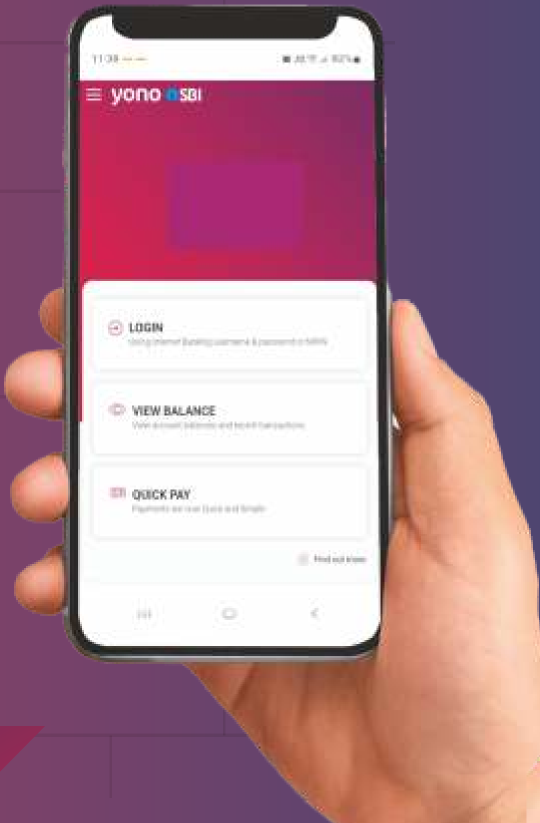
About this app →

YONO SBI:Bank,Invest,Shop,Travel,Pay Bills,Recharge,use UPI to transfer money

#6 top free in finance | Banking

Data safety →

Safety starts with understanding how developers collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this



11:38

yono SBI

LOGIN

Using Internet Banking username & password or MPIN

VIEW BALANCE

View account balances and recent transactions

QUICK PAY

Payments are now Quick and Simple

Find out more

Download and Login SBI Yono App

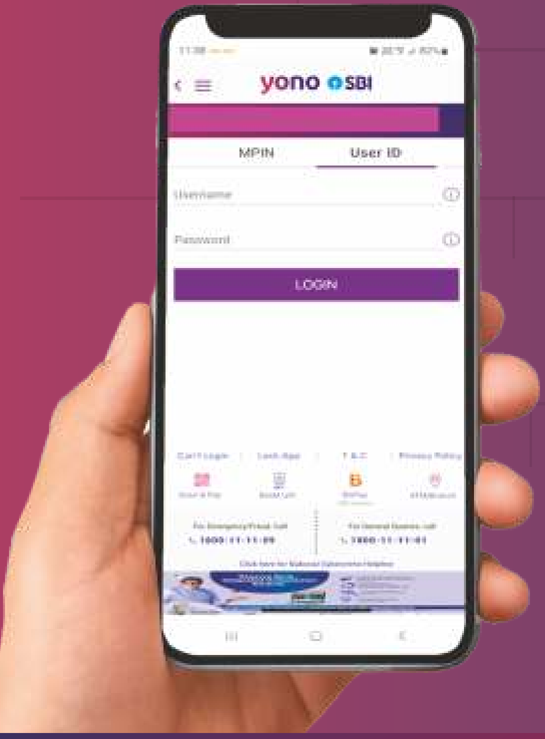
STEP 3:

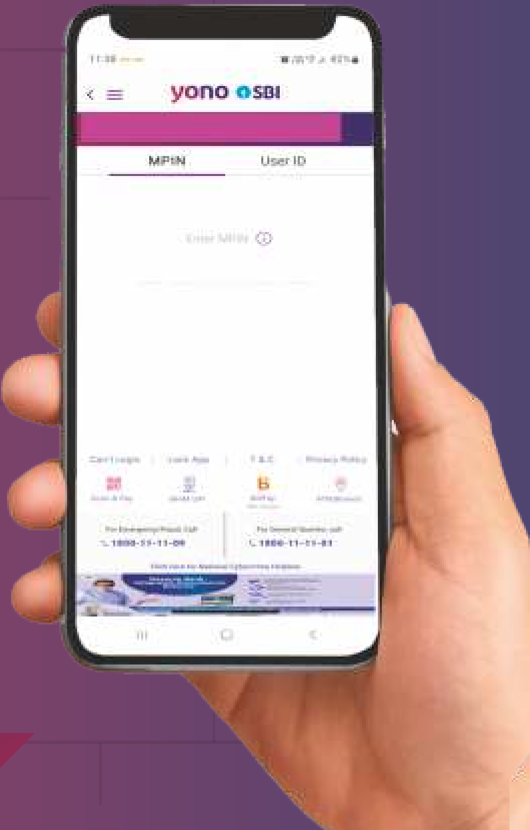
Enter your Username and Password to LOGIN

STEP 4:

If MPIN has been enabled, use a unique and strong MPIN

Never share your MPIN and password with anyone





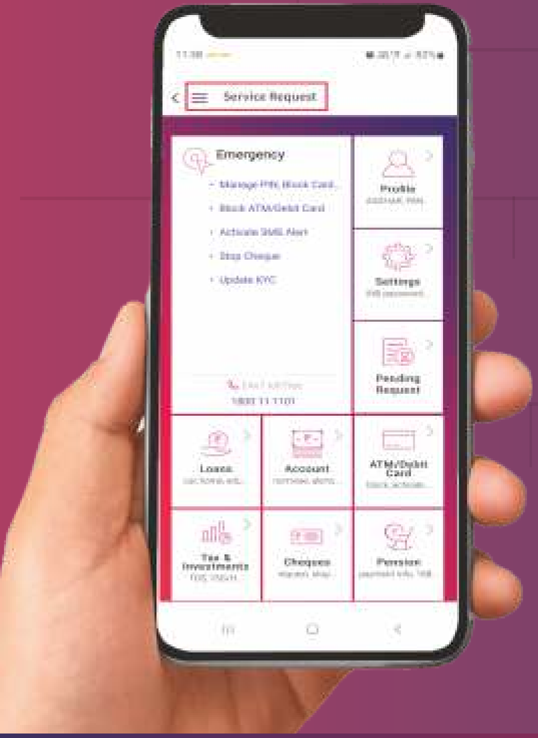
Set ATM/Debit Card Limit

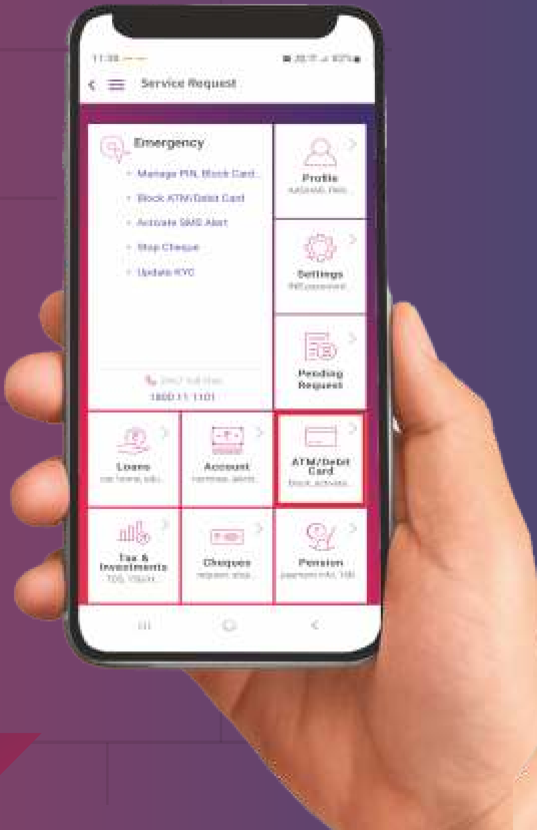
STEP 1:

Tap on the 3 Lines on top left corner and go to Service Requests

STEP 2:

Go to ATM / DEBIT Card Option





Set ATM/Debit Card Limit

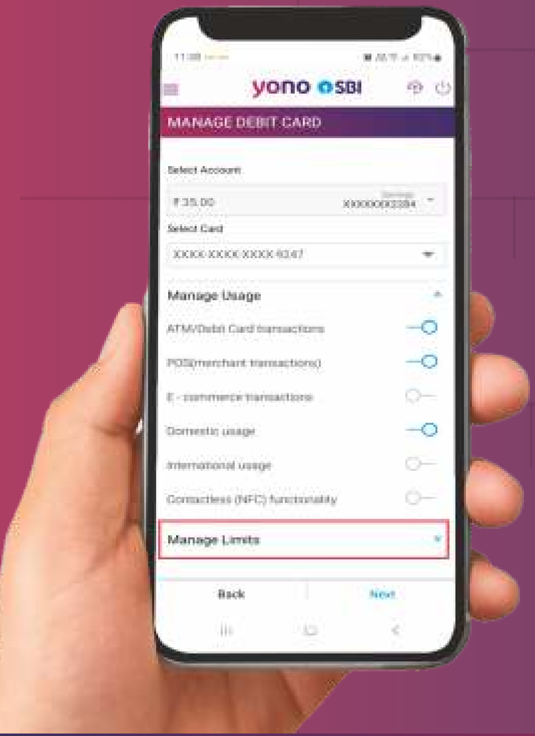
If your debit card is lost or stolen, a lower withdrawal limit can help reduce the amount of money that can be taken from your account by limiting the amount that can be withdrawn from an ATM.
This can minimize the impact of any unauthorized transactions.

STEP 3:

Click on Manage Limit Option

STEP 4:

Select Account, Card Number and Set ATM/Credit Card Limit



yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2284

Select Card

XXXX XXXX XXXX 9247

Manage Usage

ATM/Debit Card transactions ●

POS(merchant transactions) ●

E - commerce transactions ○

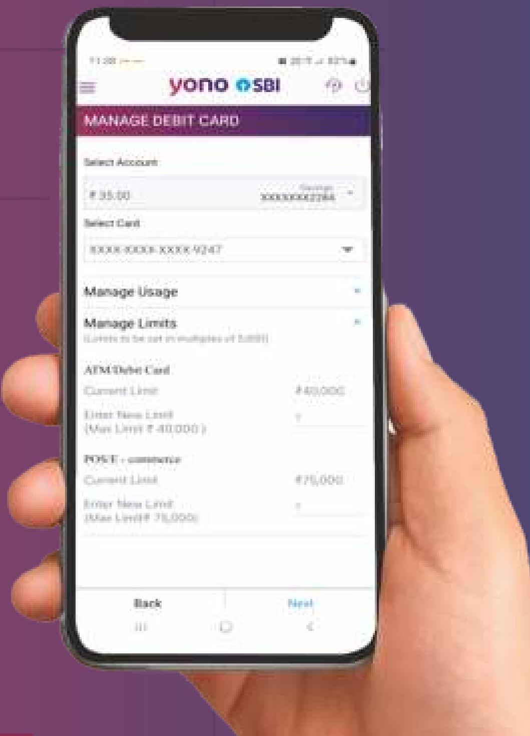
Domestic usage ●

International usage ○

Contactless (NFC) functionality ○

Manage Limits

Back | Next



yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2284

Select Card

XXXX-XXXX-XXXX-9247

Manage Usage

Manage Limits
(Limits to be set in multiples of 5,000)

ATM/Debit Card

Current Limit ₹40,000

Enter New Limit
(Max Limit ₹ 40,000) ₹

POS/E - commerce

Current Limit ₹75,000

Enter New Limit
(Max Limit₹ 75,000) ₹

Back | Next

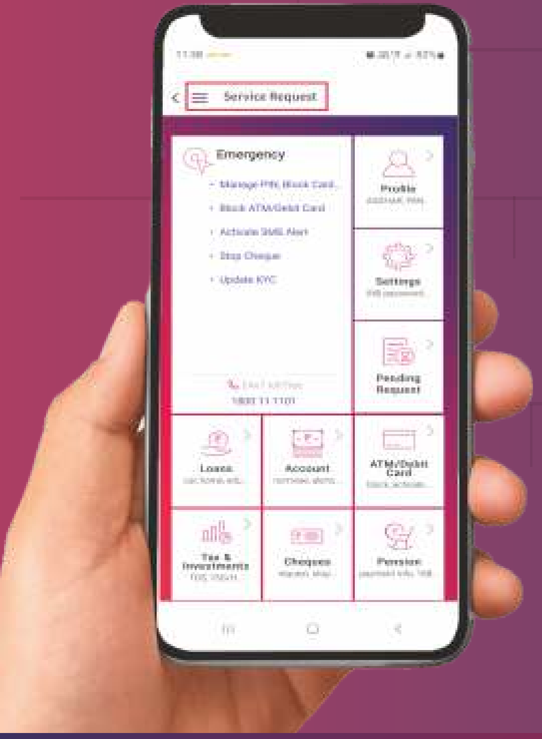
Manage Transactions

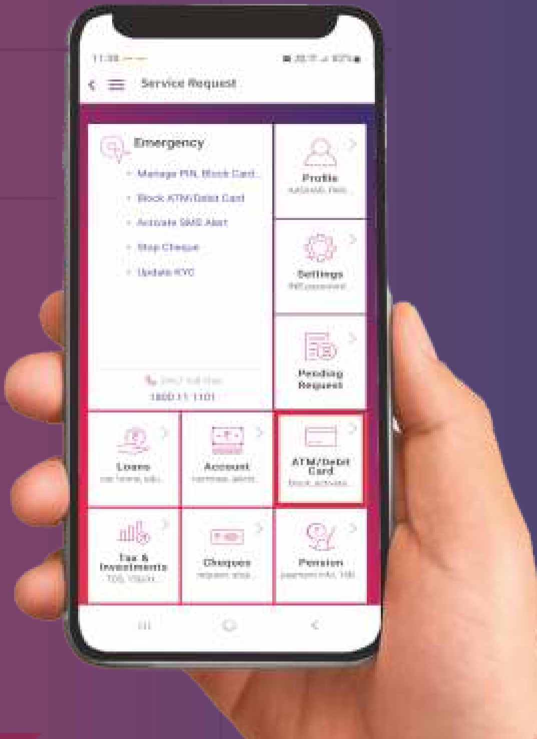
STEP 1:

Tap on the 3 Lines on top left corner and go to Service Requests

STEP 2:

Go to ATM / DEBIT Card Option





Set ATM/Debit Card Limit

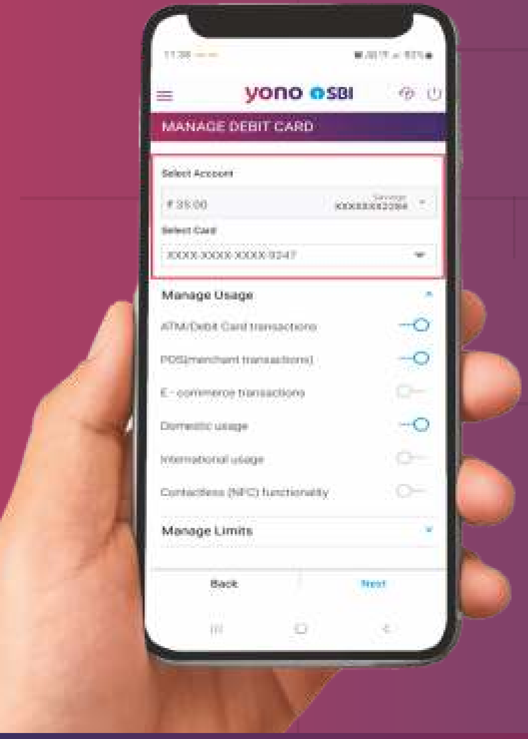
If your debit card is lost or stolen, a lower withdrawal limit can help reduce the amount of money that can be taken from your account by limiting the amount that can be withdrawn from an ATM.
This can minimize the impact of any unauthorized transactions.

STEP 1:

Select your Account and the Card for which you want to manage transactions

STEP 2:

Select whether you want to Enable or Disable ATM/ Debit Card Transactions



MANAGE DEBIT CARD

Select Account

₹ 35.00 XXXXXXXX2284

Select Card

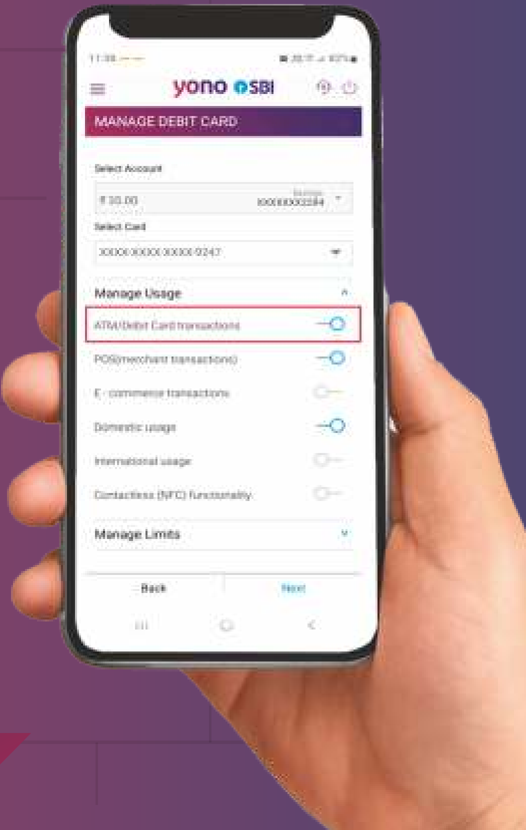
XXXX-XXXX-XXXX-9247

Manage Usage

- ATM/Debit Card transactions
- POS(merchant transactions)
- E - commerce transactions
- Domestic usage
- International usage
- Contactless (NFC) functionality

Manage Limits

Back Next



MANAGE DEBIT CARD

Select Account

₹ 10.00 XXXXXXXX2284

Select Card

XXXX-XXXX-XXXX-9247

Manage Usage

- ATM/Debit Card transactions
- POS(merchant transactions)
- E - commerce transactions
- Domestic usage
- International usage
- Contactless (NFC) functionality

Manage Limits

Back Next

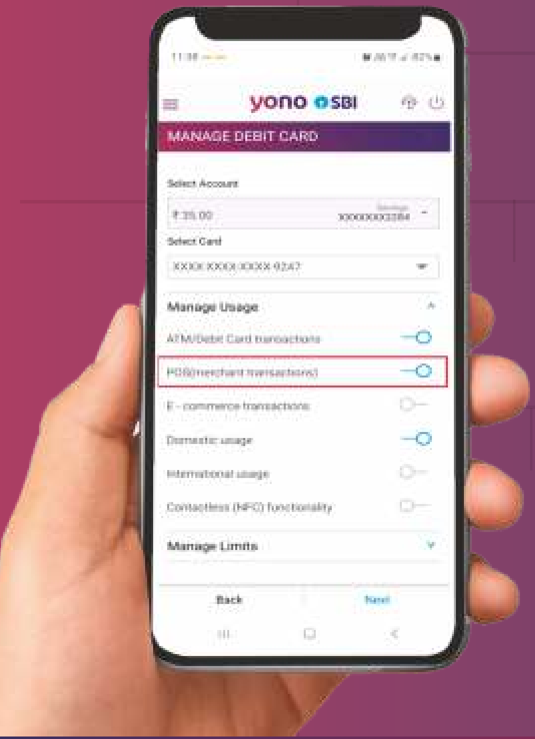
Disable or Enable POS and E-commerce Transactions

STEP 1:

Select whether you want to Enable or Disable POS Transactions

STEP 2:

Select whether you want to Enable or Disable E-Commerce Transactions



11:38

yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2384

Select Card

XXXX XXXX XXXX 9247

Manage Usage

ATM/Debit Card transactions ●

POS(merchant transactions) ●

E - commerce transactions ○

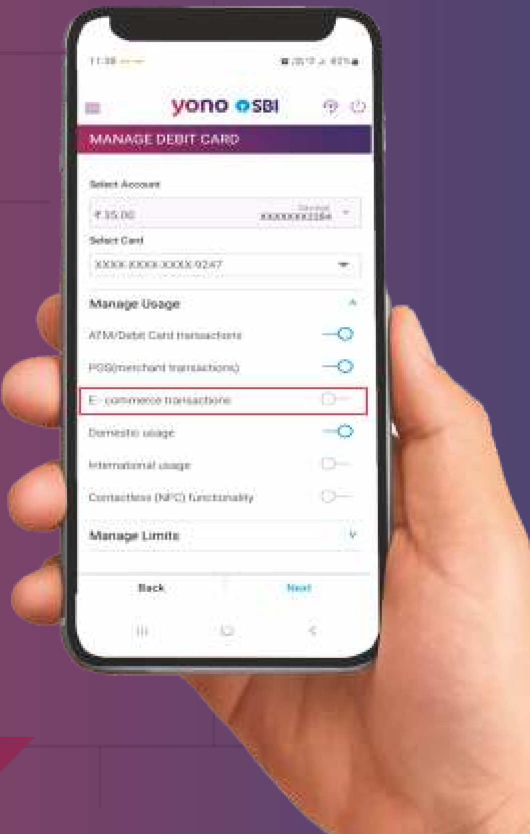
Domestic usage ●

International usage ○

Contactless (NFC) functionality ○

Manage Limits

Back Next



11:38

yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2384

Select Card

XXXX XXXX XXXX 9247

Manage Usage

ATM/Debit Card transactions ●

POS(merchant transactions) ●

E - commerce transactions ○

Domestic usage ●

International usage ○

Contactless (NFC) functionality ○

Manage Limits

Back Next

Disable or Enable International and NFC Transactions

International transactions can also be performed through ATM card without any second factor authentication such PIN or OTP. Hence, it is recommended to keep international transaction on your ATM card disabled to prevent any fraudulent transactions in case the card is lost or stolen.

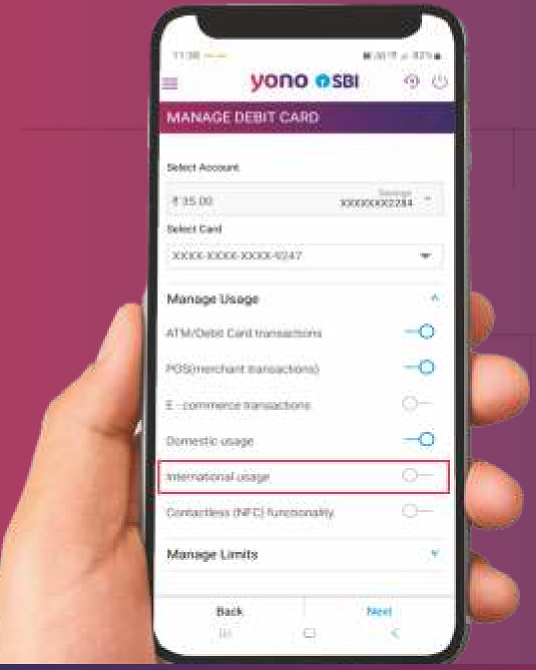
NFC is a facility provided to make transaction of up to Rs. 5000/- daily without entering the ATM PIN. If NFC transactions are not performed by you, it is recommended to disable the NFC usage on your card. If your card is lost and NFC is enabled, anyone can perform NFC transaction of Rs. 5000/- daily.

STEP 1:

Select whether you want to disable or enable International Transactions

STEP 2:

Select whether you want to Enable or Disable Contactless (NFC) Transactions



yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2284

Select Card

XXXX-XXXX-XXXX-9247

Manage Usage

ATM/Debit Card transactions ●

POS(merchant transactions) ●

E - commerce transactions ○

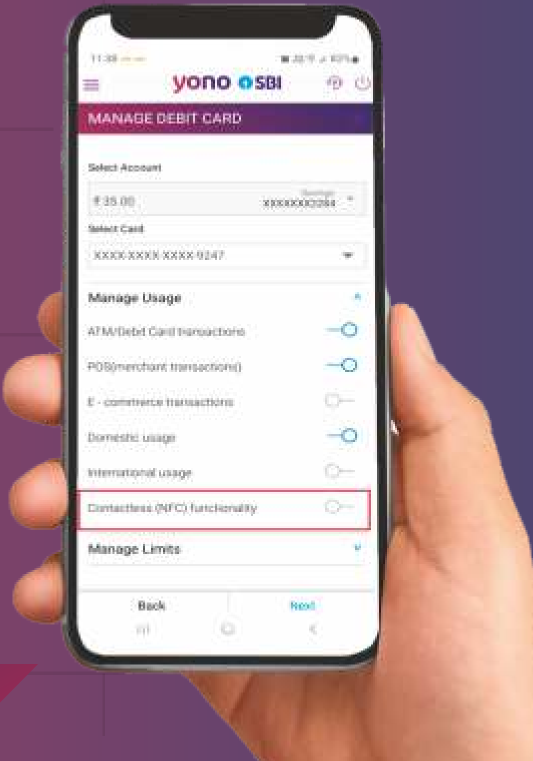
Domestic usage ●

International usage ○

Contactless (NFC) functionality ○

Manage Limits

Back Next



yono SBI

MANAGE DEBIT CARD

Select Account

₹ 35.00 Savings XXXXXXX2284

Select Card

XXXX-XXXX-XXXX-9247

Manage Usage

ATM/Debit Card transactions ●

POS(merchant transactions) ●

E - commerce transactions ○

Domestic usage ●

International usage ○

Contactless (NFC) functionality ○

Manage Limits

Back Next

ACTIVATE SMS ALERT

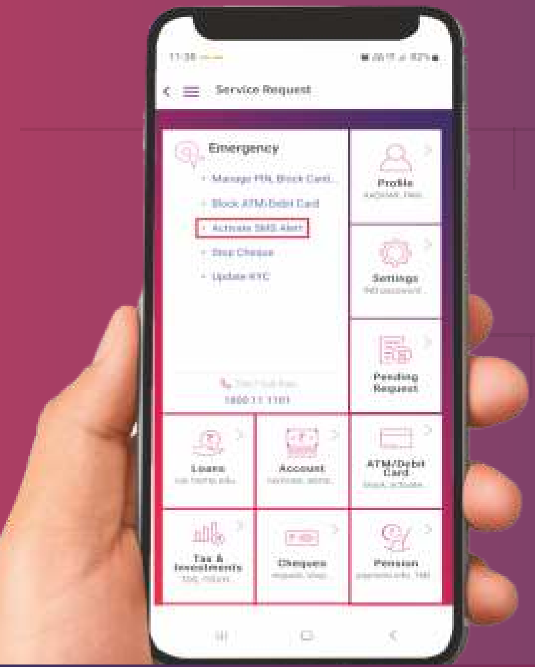
SMS alerts can help you identify suspicious activity on your account. If you receive an SMS alert for a transaction that you did not make or authorize, you can immediately contact your bank to report the incident.

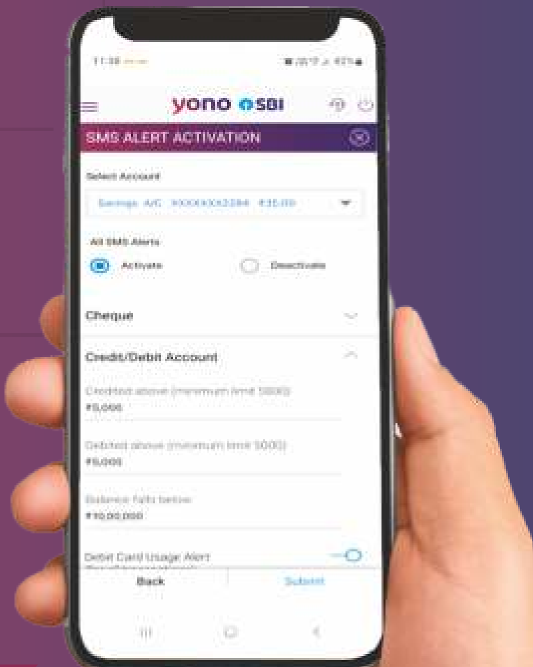
STEP 1:

From Service Request go to Block ATM/Debit Card

STEP 2:

Select Account and Click on Activate. Also set the Credit/Debit Parameters for SMS Alert





Select Account

Savings A/C XXXXXXX2284 ₹35.00

All SMS Alerts

● Activate ○ Deactivate

Cheque

Credit/Debit Account

Credited above (minimum limit 5000)
₹5,000

Debited above (minimum limit 5000)
₹5,000

Balance falls below
₹10,00,000

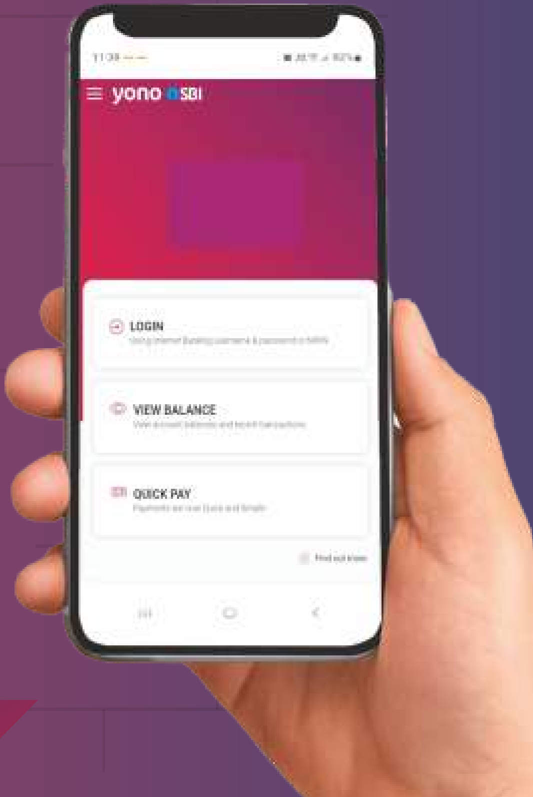
Debit Card Usage Alert

Mobile Banking

Let us understand how can we enable the secure functionality through YONO SBI.

1 Bank provides you mobile banking services through YONO SBI

2 You can also enable the security features for your ATM cards, UPI etc, through YONO SBI



How to Block ATM/Debit Card

You should block your ATM card immediately if you suspect that your card has been lost, stolen, or compromised in any way.

If you suspect any fraudulent transaction through ATM Card or your ATM Card is lost, you should immediately block your ATM Card through following ways:

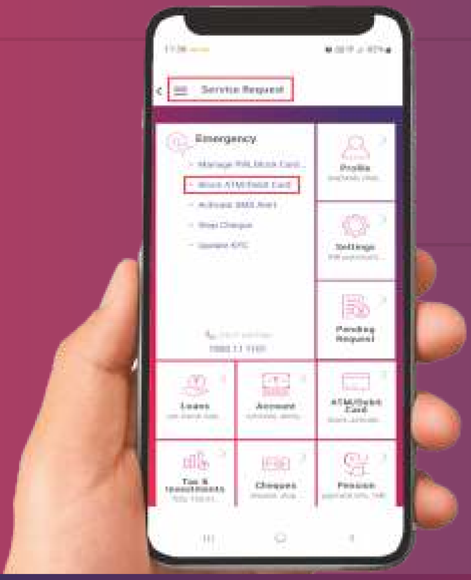
- Go to the Mobile Banking App and Block your ATM Card through the App. Process shown on next page.
- You can also block ATM Card through the nearest SBI branch.
- You can also block your ATM Card by calling on these helpline numbers: 1800111109, 1800 2100, 1800 1234.

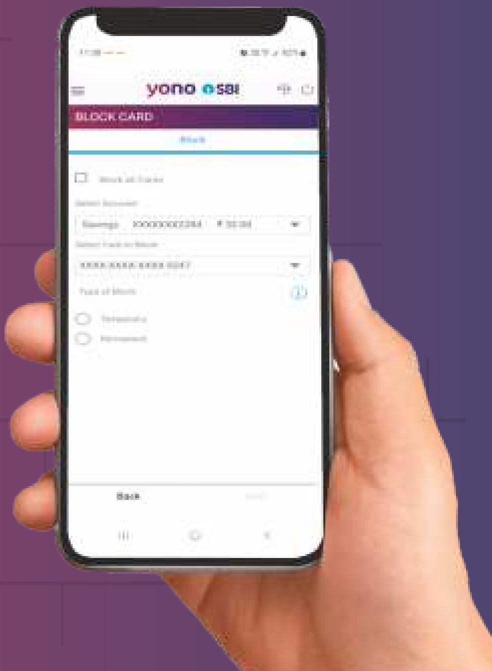
STEP 1:

From Service Request go to Block ATM/Debit Card

STEP 2:

Select Account , Card Number and Type of Block(Temporary or Permanent)





UPI Platform

1. UPI is a banking facility provided by default to every customers to perform easy and convenient banking transfers to persons and any merchants.

2. UPI transactions can be performed using VPA (Virtual payment identifier), registered mobile number or account numbers.

3. UPI payments can also be done through QR scans.

4. In case you suspects any fraudulent transactions through UPI channels, you should immediately disable the UPI Platform.

5. You can disable the UPI Platform account by going to SBI YONO App shown in the next page.

6. You can also block your UPI channel on your account by calling on these helpline number: 1800111109, 1800 2100,1800 1234.

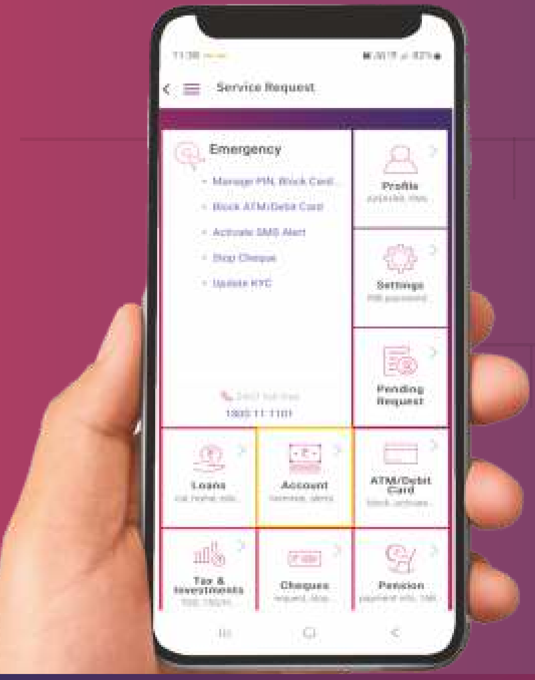
UPI Enable / Disable

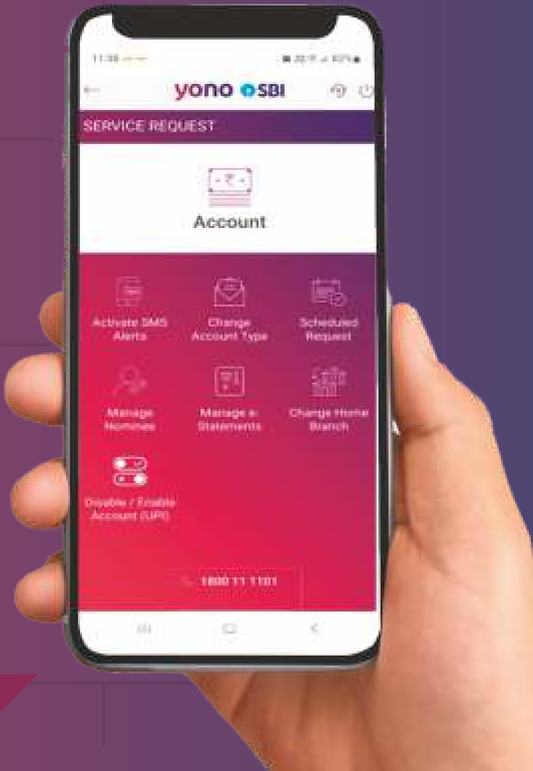
STEP 1:

From Service Request go to Account

STEP 2:

Click on Disable/Enable UPI Account

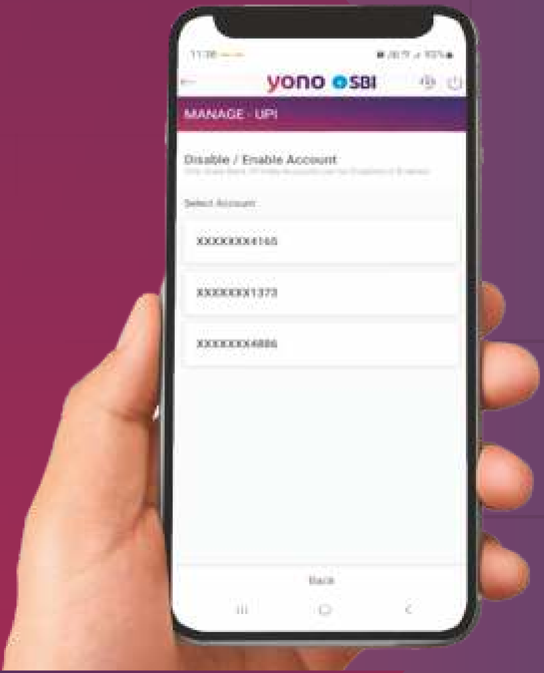




UPI Enable / Disable

STEP 3:

Select the Account Number and then Choose whether you want to Disable or Enable UPI Account



MANAGE - UPI

Disable / Enable Account

Select Account

XXXXXXXX4165

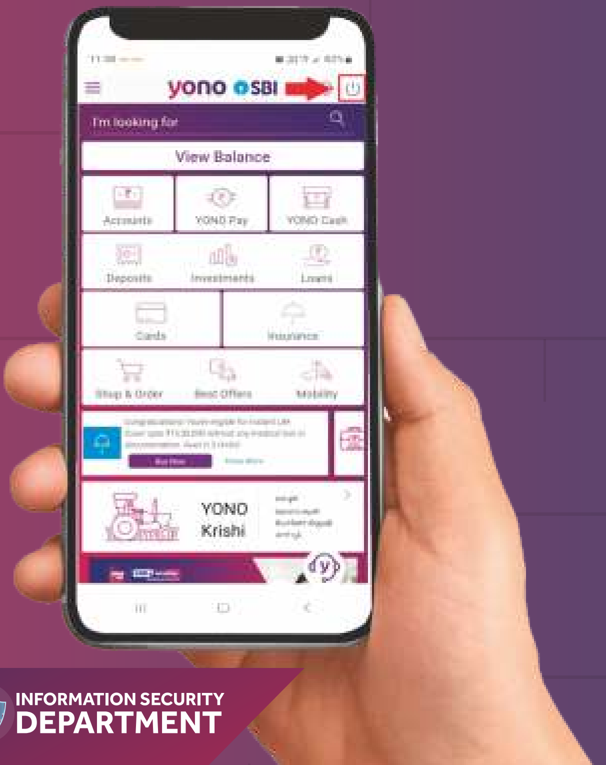
XXXXXXX1373

XXXXXXXX4886

Safe logout

1 Always logout from your YONO SBI account after performing the banking activities to prevent any unauthorized access to your account. Click on the Power Button on top Right corner to safely logout from your SBI Bank Account.

2 Always remember you should not save your Mobile Banking login credentials on your browsers as it will allow other person having access to your devices to access your YONO SBI account.



Golden Hour reporting refers to the practice of promptly reporting a cyber fraud incident to the relevant authorities or organizations within the first hour of detection.

- Report fraud on Cyber Crime Helpline Number 1930 immediately or register complaint with National Cyber Crime Reporting portal https://cybercrime.gov.in/
- Register complaint of unauthorized transactions through SBI portal https://bank.sbi/web/customer-care/ or report to nearest SBI branch
- For blocking of Account/Debit card to stop further unauthorized transactions please call SBI's 24X7 helpline number 18001234, 18002100

SBI

The banker to every indian

INFORMATION SECURITY DEPARTMENT