RAJASTHAN GRAMIN BANK
Scheduled Bank owned by Government

Customer Awareness Guide

Safeguard yourself from online frauds
Stay Alert and Safe

Dear Customers,

Awareness is the key to prevent cyber frauds

As the world continue to digitize and become more linked, cyber security has become a serious concern 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-attack 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 keep 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. We are confident that the booklet will assist you in better understanding cyber threats and guide you on a safe and secure digital journey with Rajasthan Gramin Bank.

Be a cyber aware customer.
With Best Wishes,

ITS DEPARTMENT
(RGB)

27 February 2026

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 frauds and unauthorized 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 attributed 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!

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 Return Fraud

IT return fraud is prevalent and cybercriminals send bulk SMSs asking users to submit an application for initiative 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
- Aadhar Number
- PIN Code
- Address
- Mobile Number
- Email Address
- Gender

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

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 loan 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.

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".

- **Due to fear of the account getting blocked, the victim navigates to the link to download fake APK File.**

- **Once the APK file is downloaded on the victim's phone, the app requests permissions 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.**

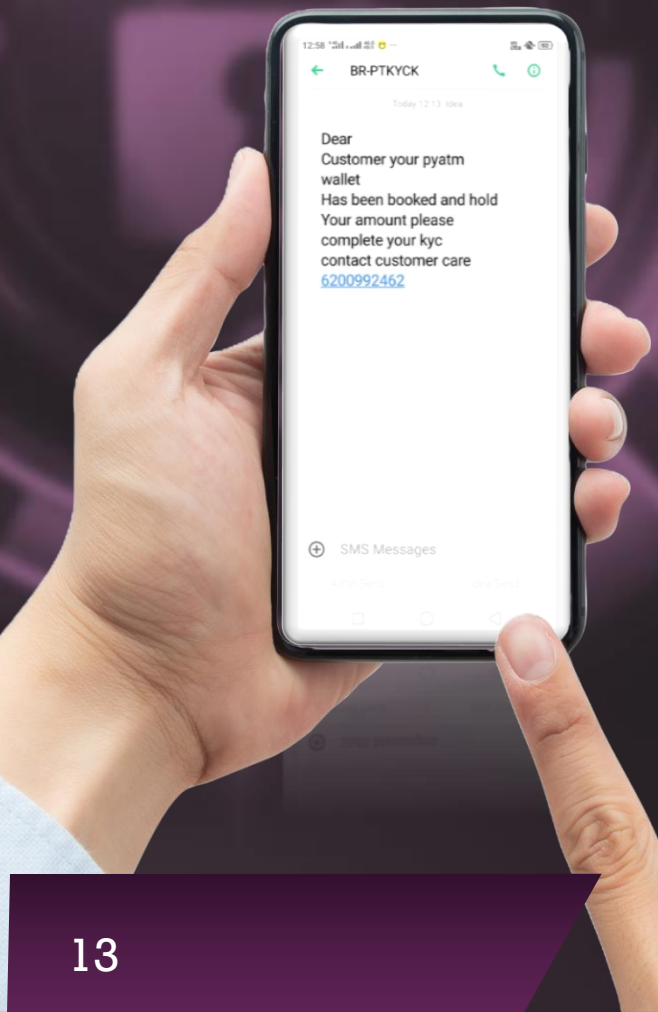
As the malicious app looks like the genuine one, the victim submits all the information and falls prey to such frauds.

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

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.**



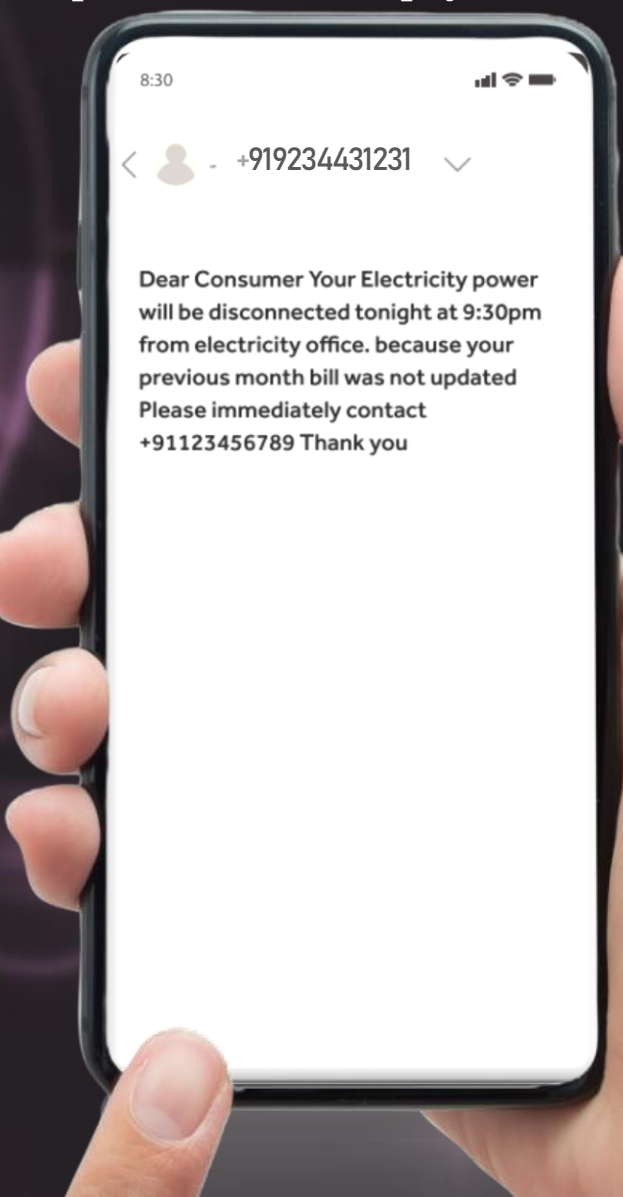
- Victim enters the OTP and fraudsters get access to the victim's account which they misuse to siphon off the money.

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

ELECTRICITY BILL FRAUD

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

- **Due to genuine fear and 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.**

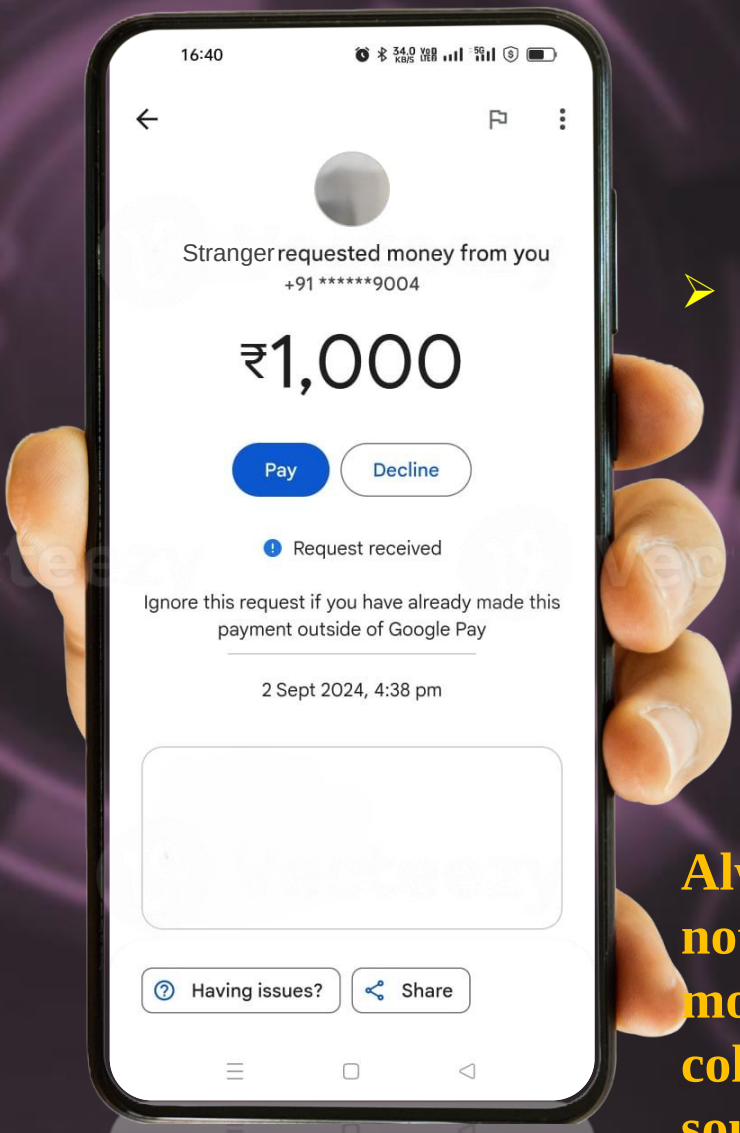


Do not download any app on the advice of any stranger.
Think before you act.

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.



- **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”.**

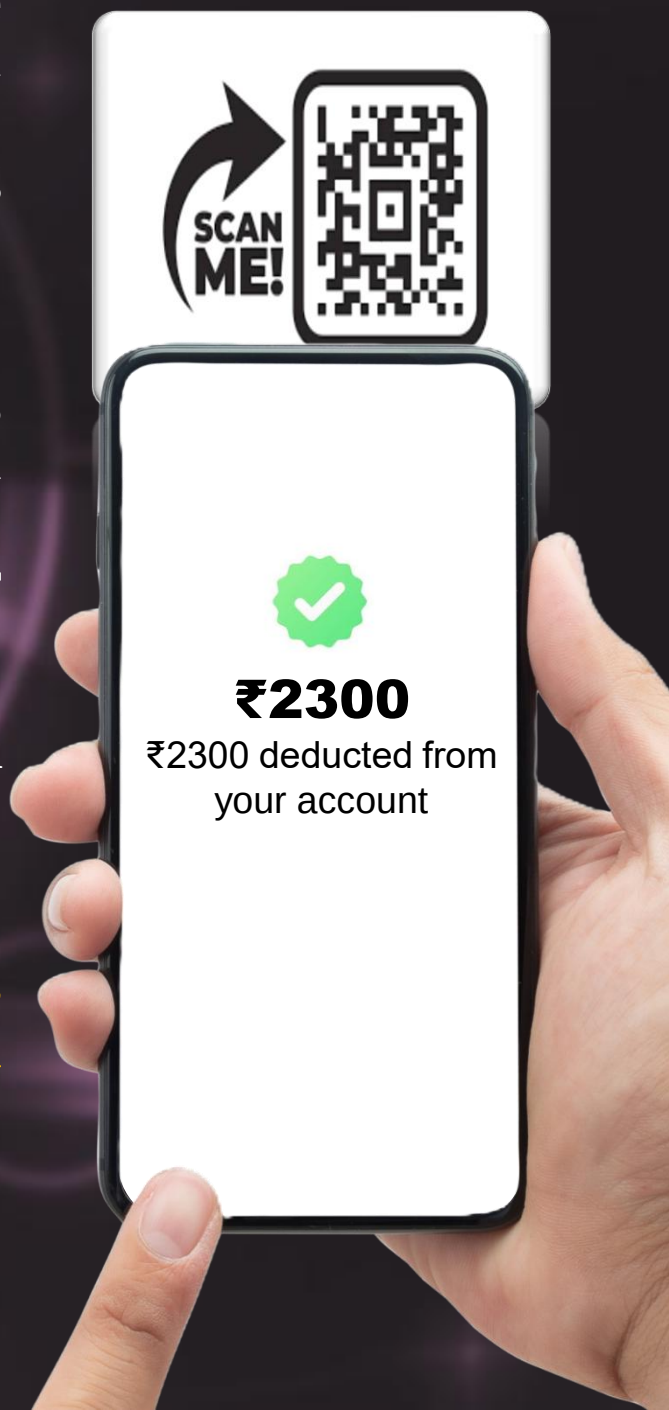
Always remember UPI PIN is not required to receive money. Do not accept UPI collect request from unknown sources.

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

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 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

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."

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

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

Ramesh 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.

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

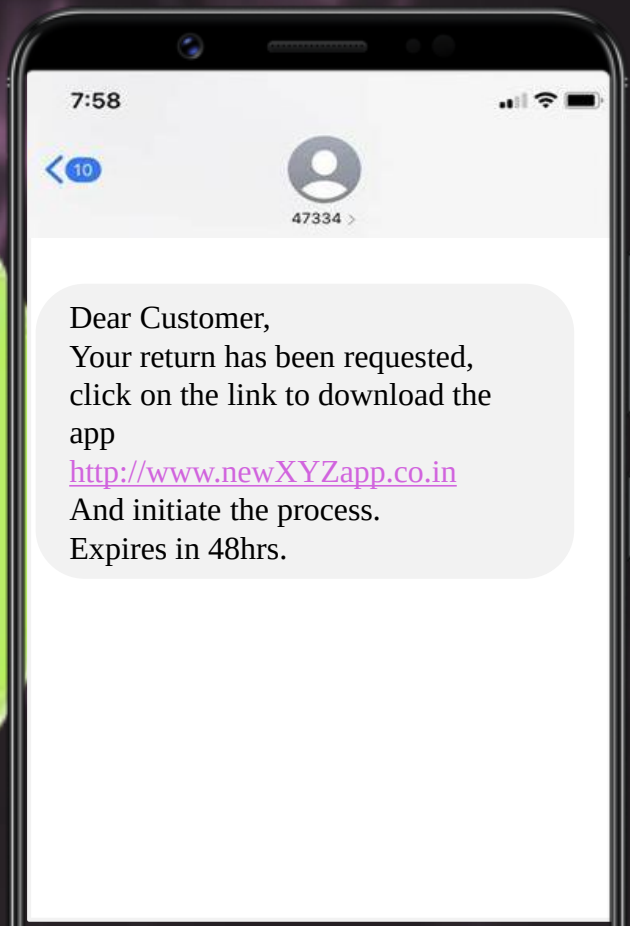
The fraudster is happy to receive a call from the trap she has set. She now knows how to CON this man.

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

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

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

Ramesh Downloads the application!



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, Ramesh shares the desk ID with the caller.

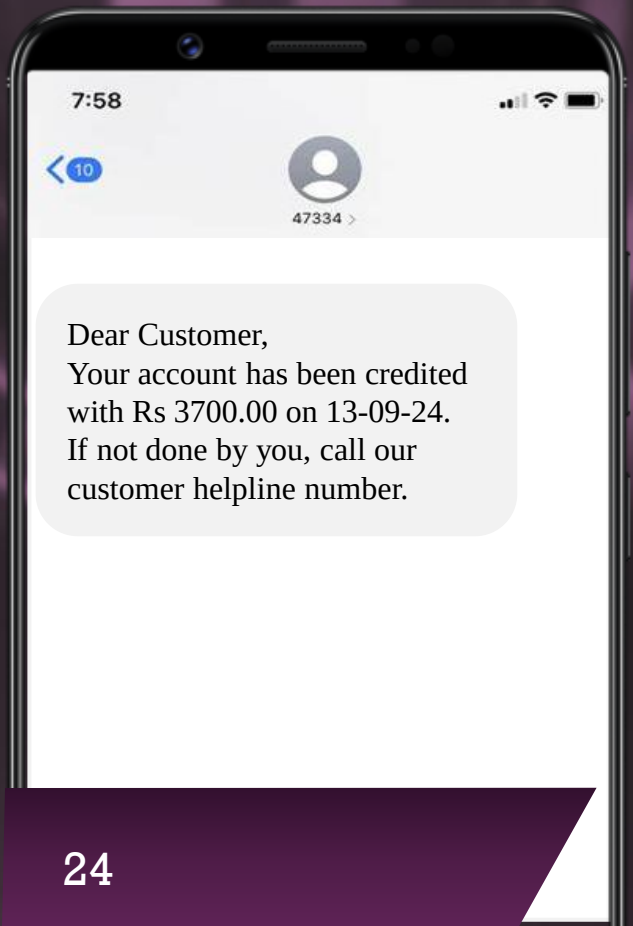
Ramesh: “Sure, the desk ID is 233 XXX XXX.”

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

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.

Ramesh receives an SMS about money being credited to has bank account.

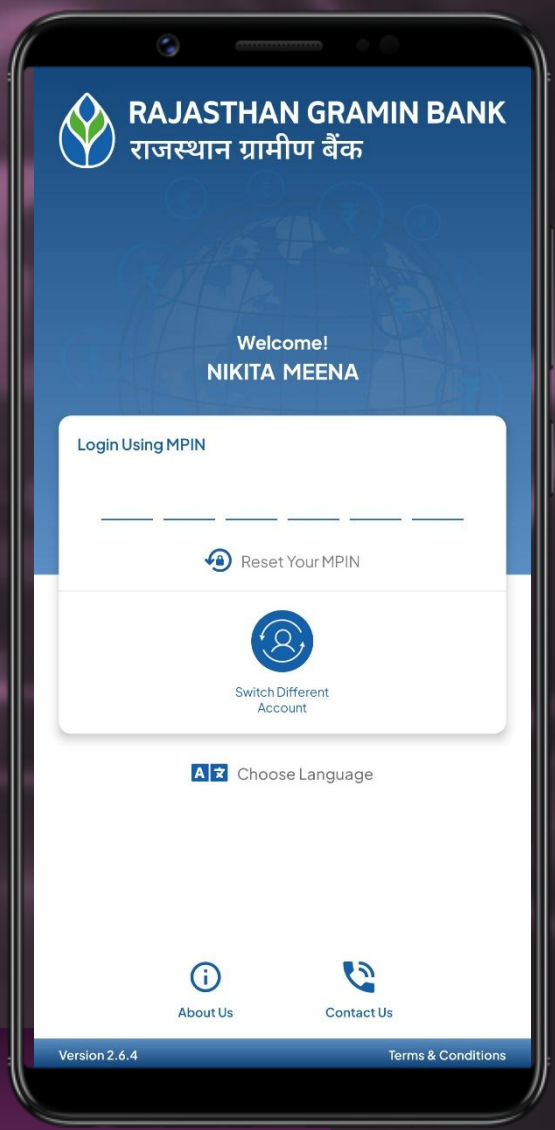
Ramesh: "Yes, I have received an SMS"

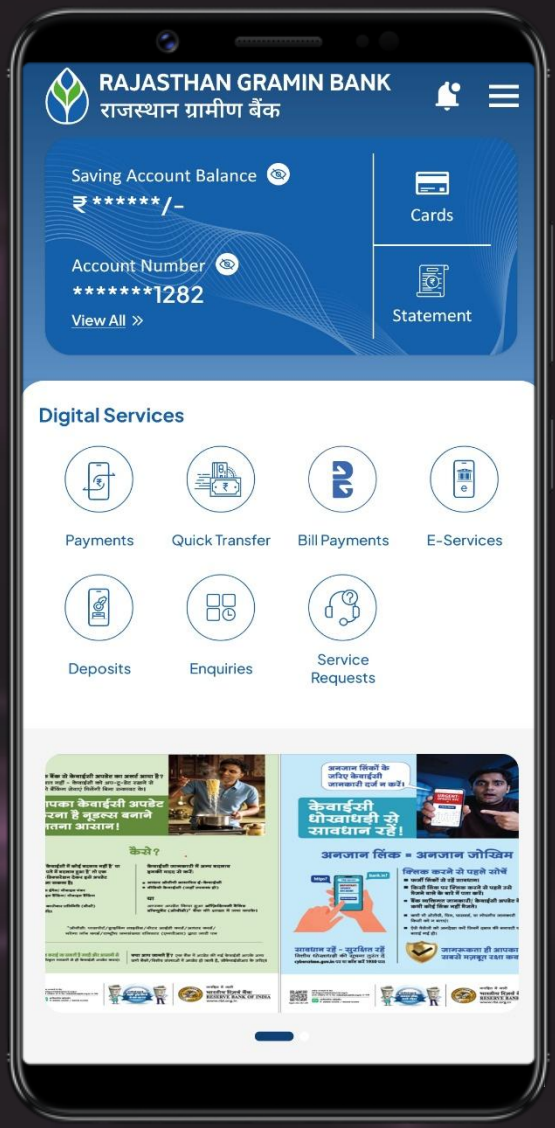


Ramesh logs into his account without realising the screensharing app is still running on his device.

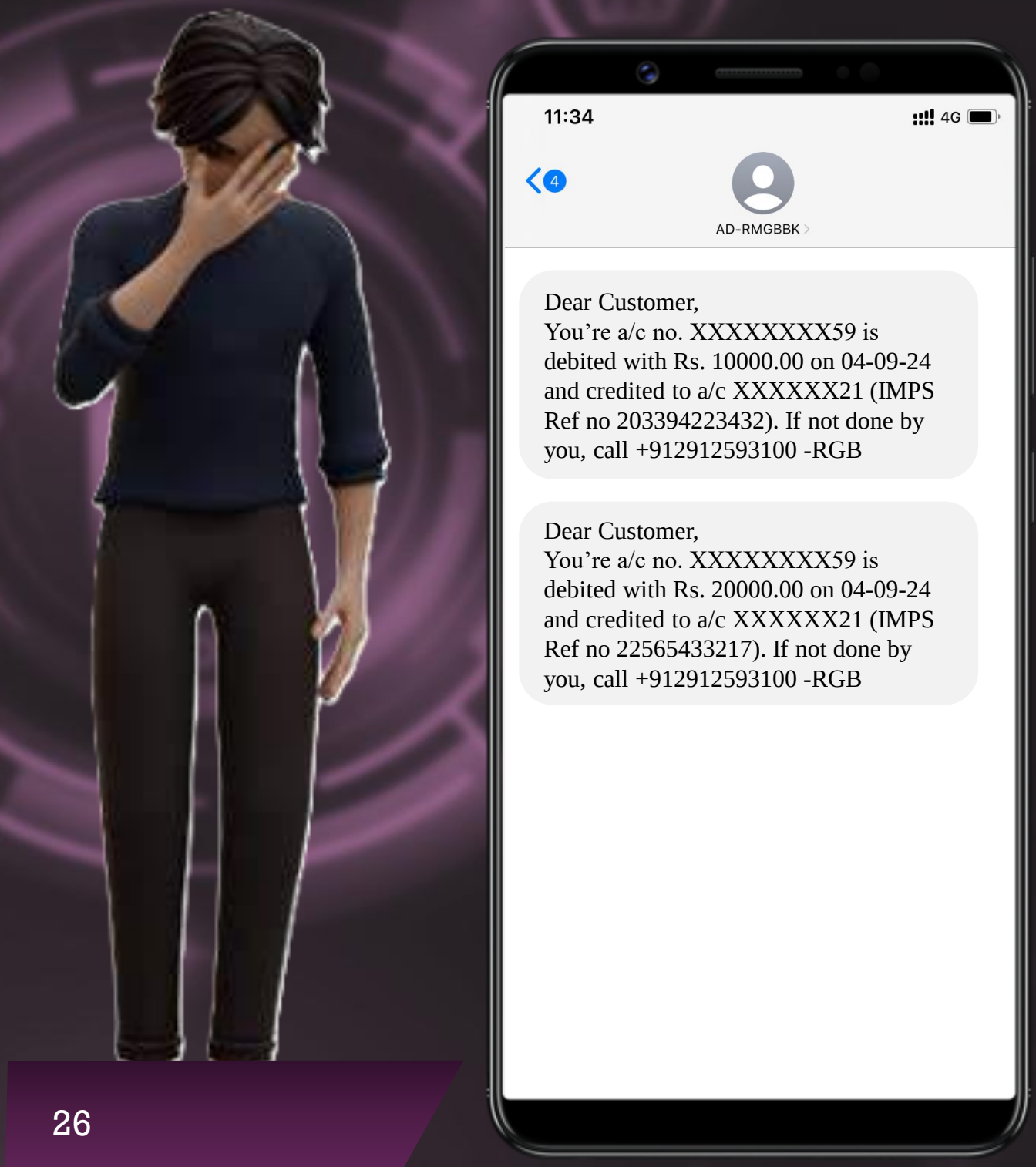
With the remote access app working in the background, the fraudster gets access to Ramesh's bank account and initiates withdrawing money.

Fraudster: "Oh, let me check again."





Ramesh starts receiving debit message on his phone.

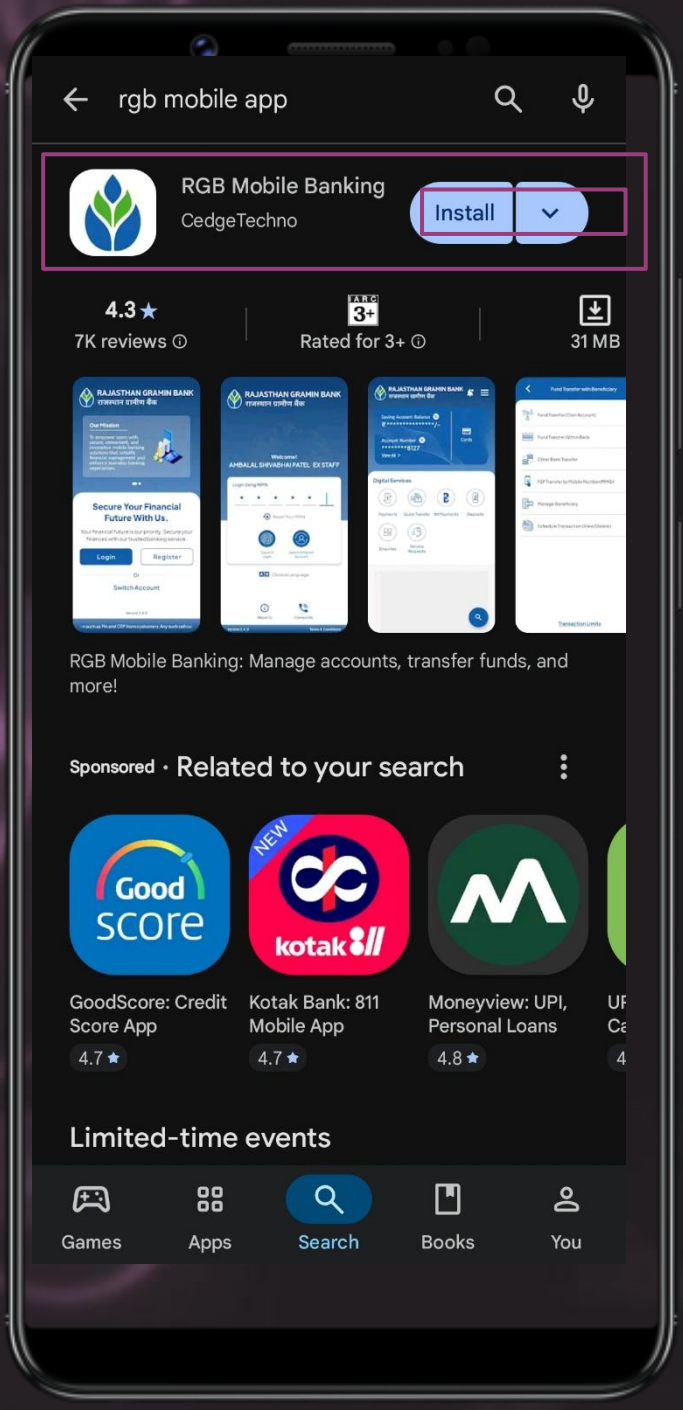


How remote access scam can be avoided

1. Never search Customer care number online. Always visit the official website and look for the Customer Care Number you can visit https://rgb.bank.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.

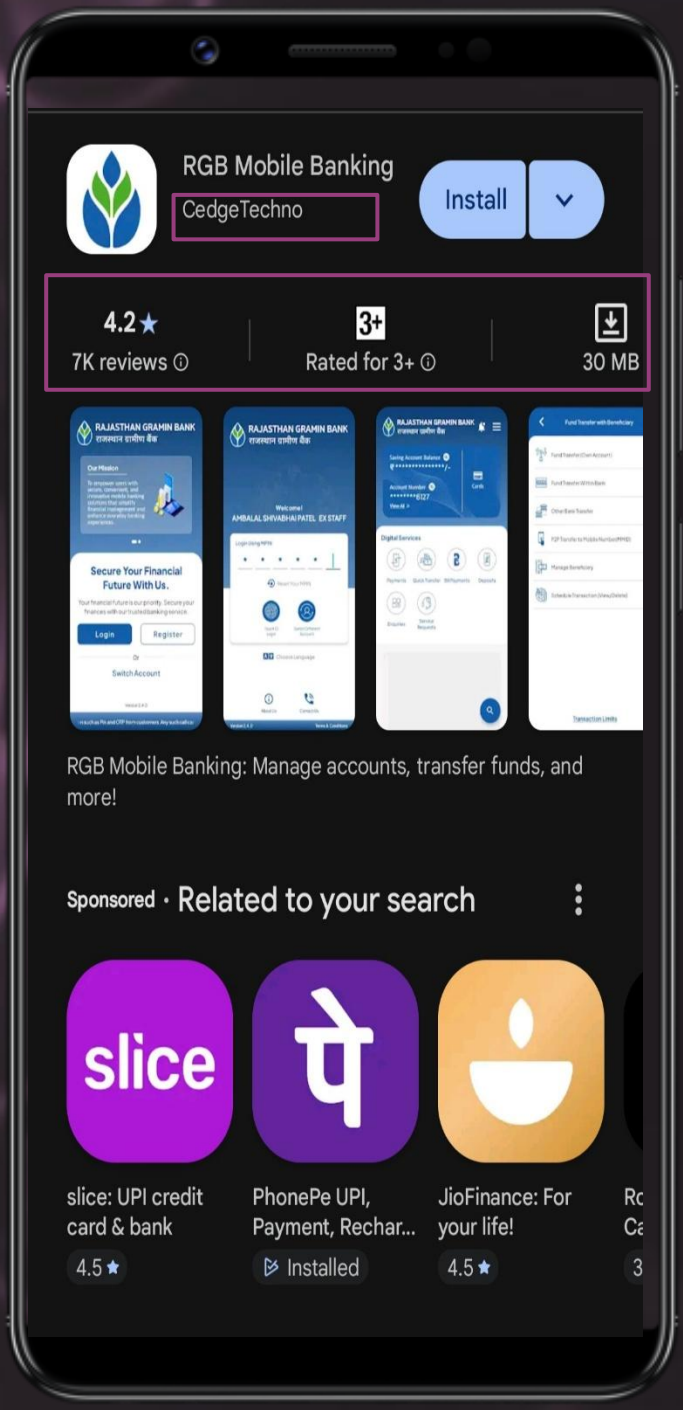
3. Before downloading any app always check if the app is from a genuine provider by going through its reviews, number of downloads and always read the "About this app" page to understand the functionality of the app.



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 your Device.
of the app.



Stay Alert & Safe

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.

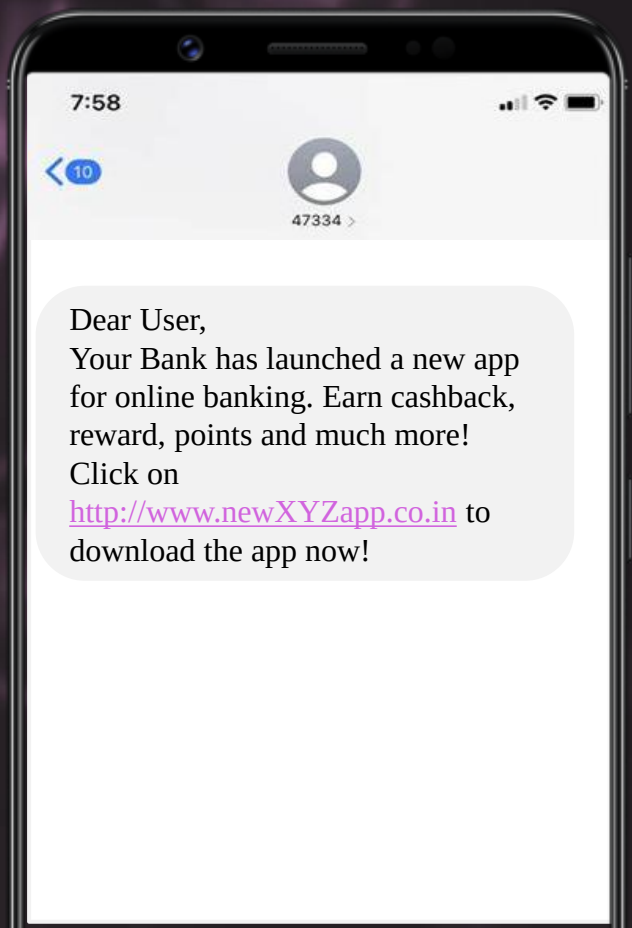
Fraudster: "Ha! This will be the perfect way to steal people's money!"

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 suspecting victmis 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.

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

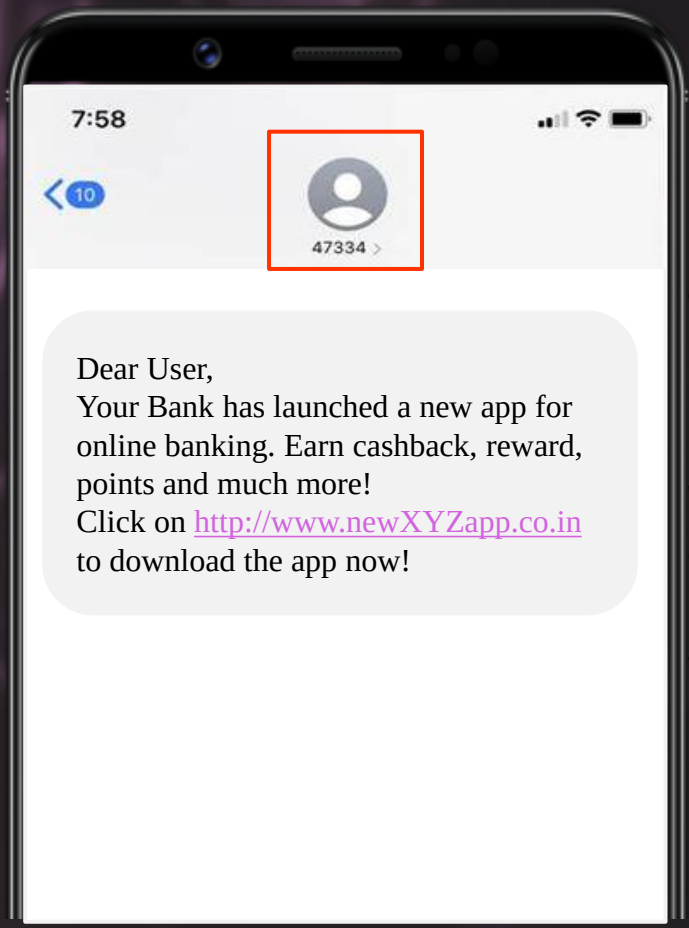


Riya looks at the message suspiciously.

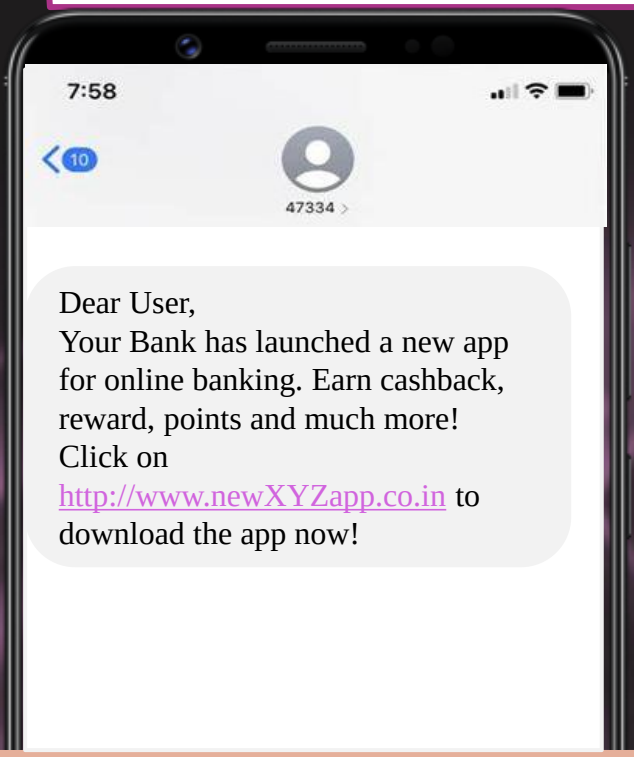
Riya : "Hmm, this looks like a suspicious SMS."

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

Riya: "First let me check the sender's details to understand if the message is from verified source.
RGB never sends SMS from a phone number or any random shortcode such as SGCLSC, SGMRBY etc.
It comes from a short code containing RGB or RMG or RM.



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



Riya: "Ah, there it is! That's a fake link. RGB never sends any unsolicited link to download an app via SMS."
It's important to download apps only from

GET IT ON Google Play

Download on the App Store

Riya goes to official app store and downloads the legitimate RGB 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 short code 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 !

SOCIAL ENGINEERING ATTACKS

Social engineering is the use of psychological manipulation to influence individual 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 downloading a malicious file.

03 Pretexting

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

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 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 positon 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

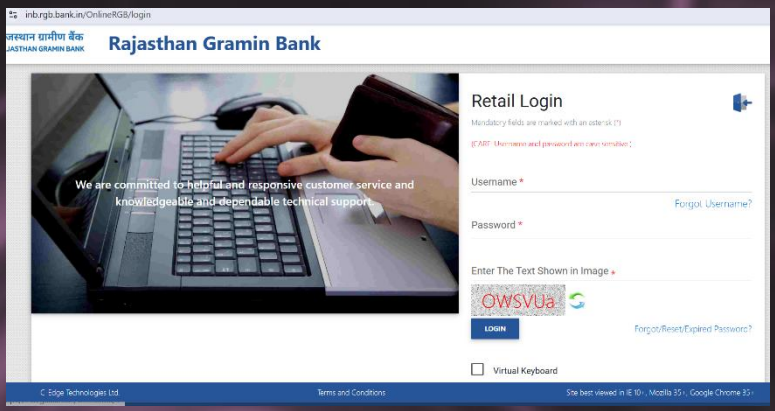
- **Keep your login credentials safe:** Your internet banking login credentials (i.e. username and password) are sensitive information that should not be shared with anyone.

- **Use secure internet connection:** 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 SECURITY

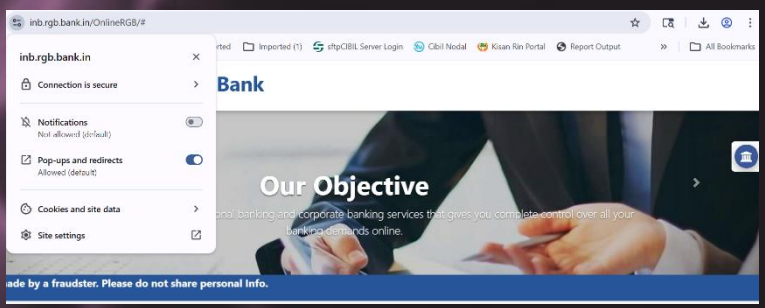


STEP 1:

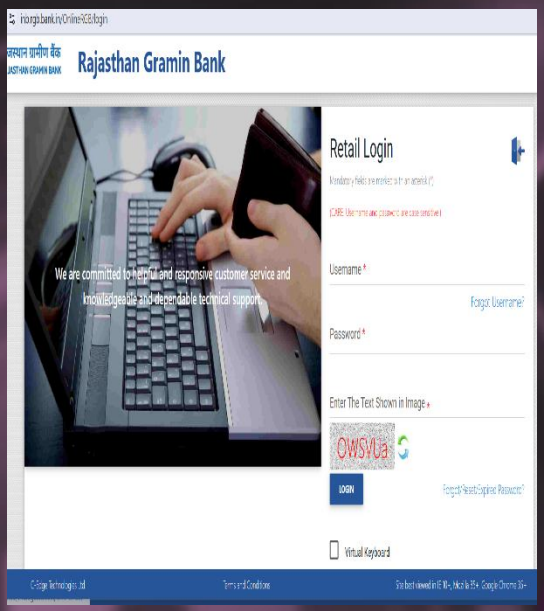
Go to the Online RGB official page

STEP 2:

Check if the website is secure by clicking on the padlock and verifying that the certificate belongs to “RGB” and is valid.



HOW TO ACCESS THE INTERNET BANKING PORTAL SECURITY



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 RGB 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.

< RGBBK

Dear Customer, OTP to login to RGB Internet banking (personal) is 344241. Do not share with anyone. -RGB

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:

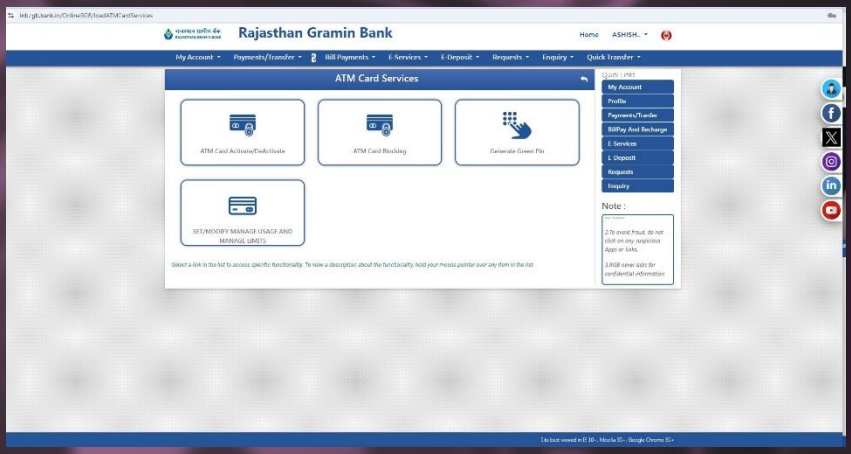
- ATM cards can be used to withdraw money from ATM machines, to carry out transactions at POS machines and to perform e-commerce transactions.

- 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/POS 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.

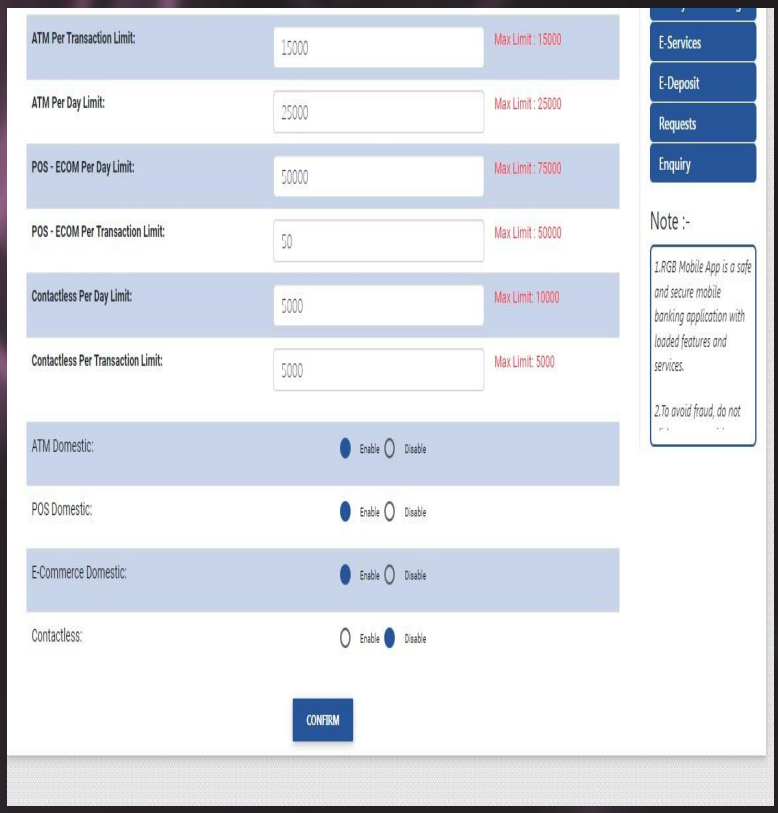


STEP 1:

Under E Services go ATM Card services than set/Modify Manage Usage and Manage Limits

STEP 2:

Select account number and then change limit according to requirement.

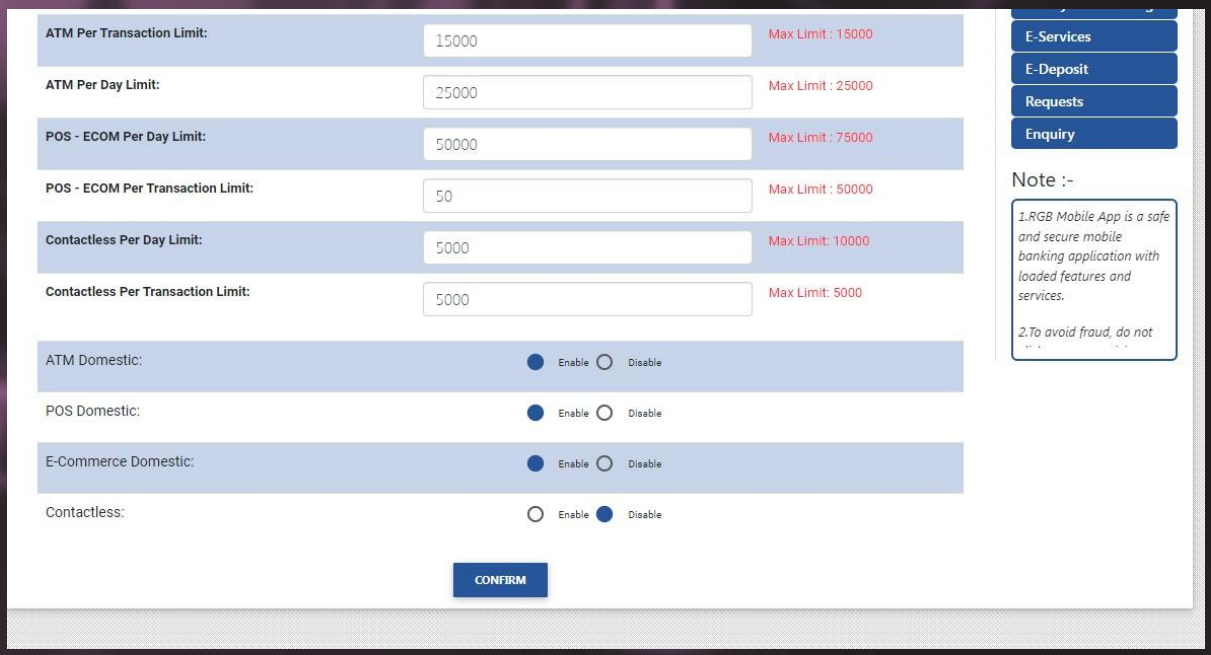


ENABLE/DISABLE INTERNATIONAL USAGE OF ATM CARD

International transactions can also be performed through ATM Card. Hence, it is recommended to keep international transaction on your ATM card disabled to prevent any fraudulent transaction in case the card is lost or stolen.

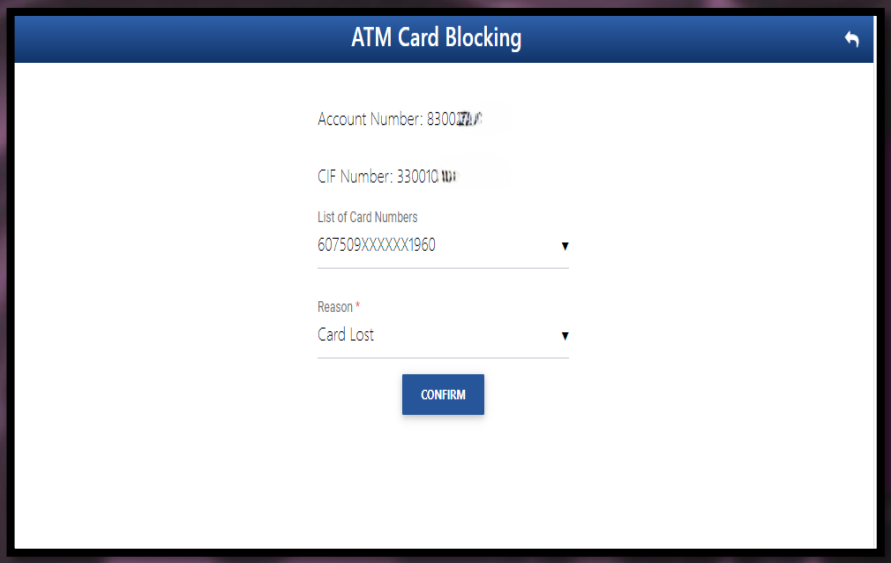
STEP :

Go to ATM Card Switch on/off. Select your card number and choose the options as per requirement.



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:

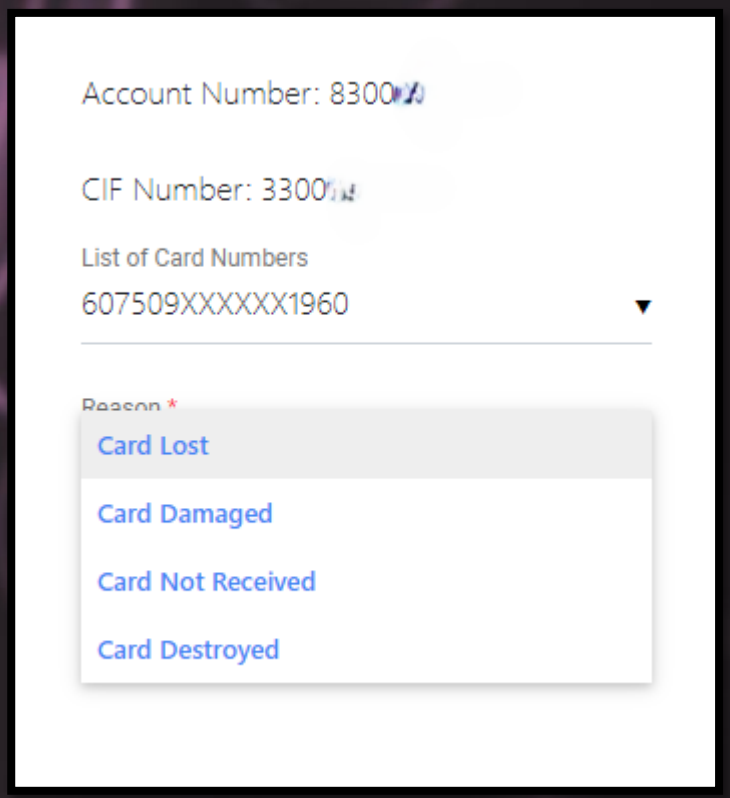


STEP 1:

Go to ATM Card Blocking And choose the card number.

STEP 2:

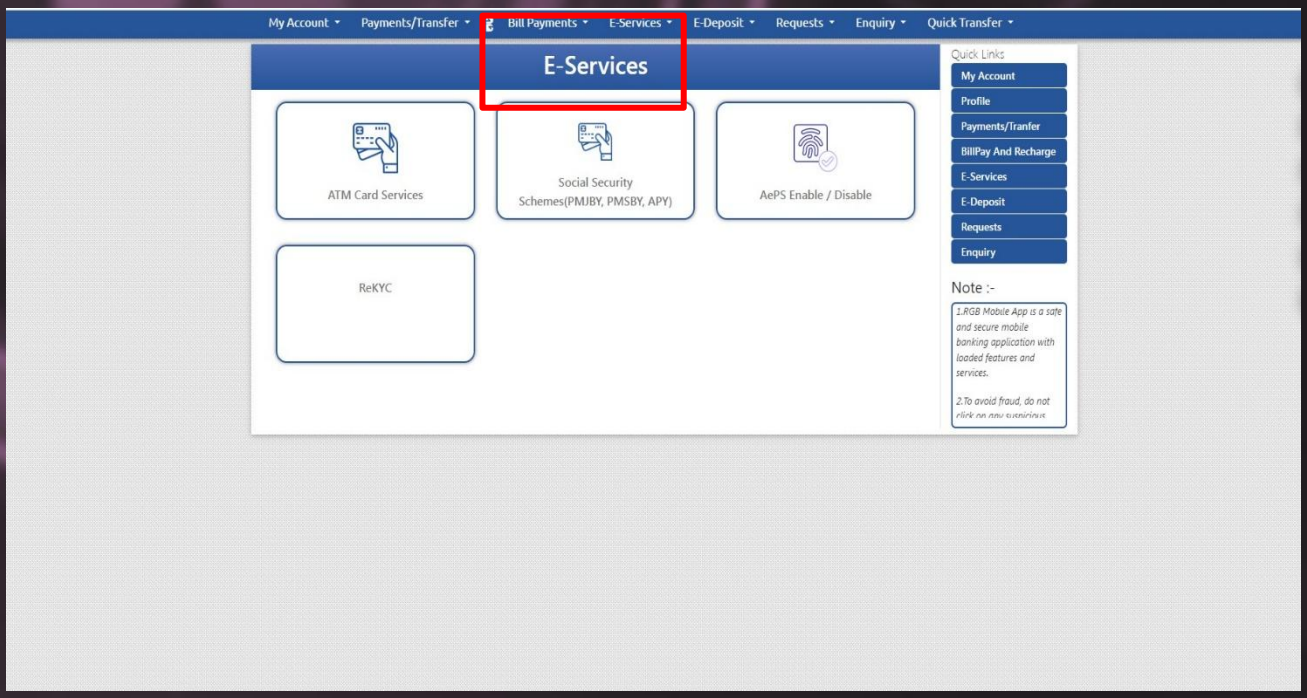
Choose the reason of card block and submit.



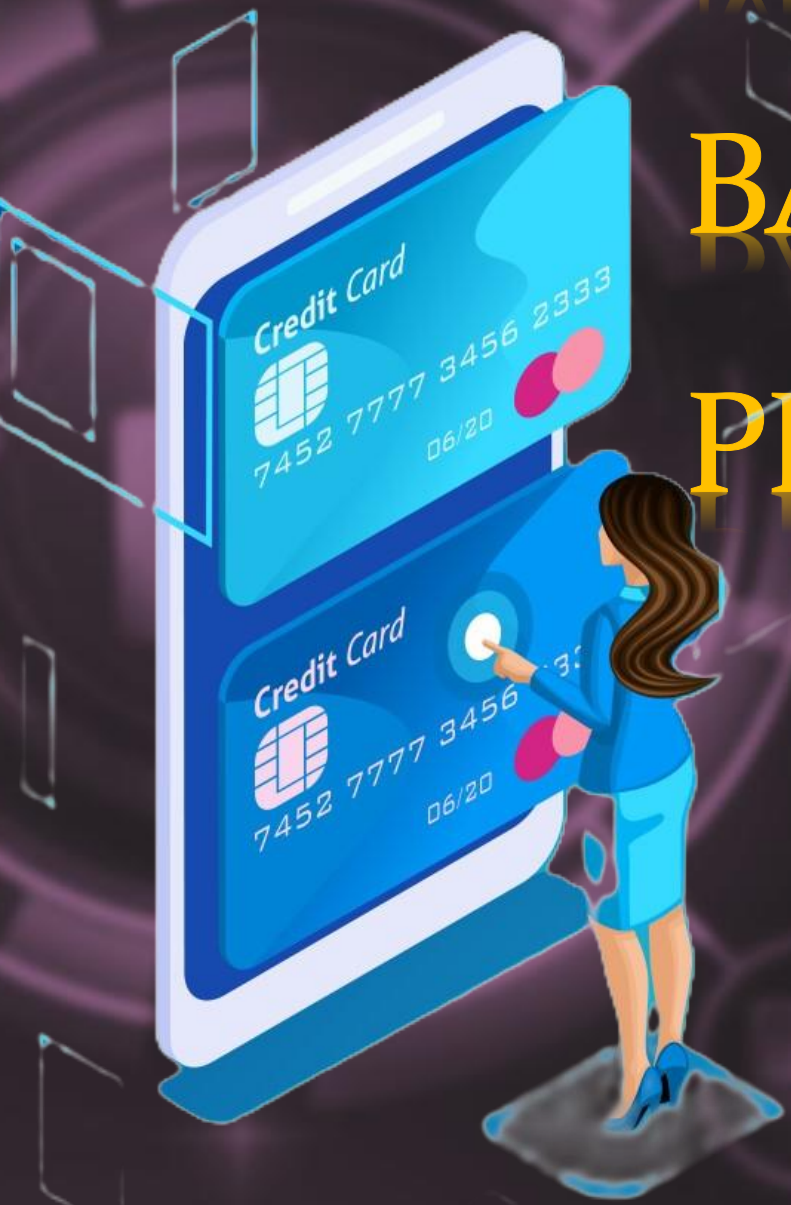
SAFE LOGOUT

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 the top right corner to safely logout from your RGB 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.



SAFE MOBILE BANKING PRACTICES



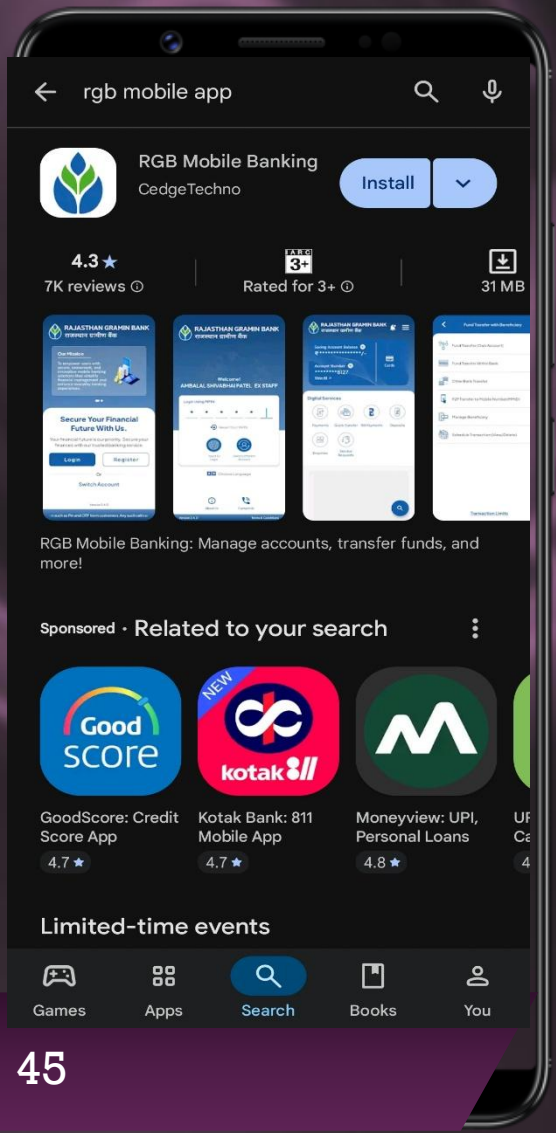
DOWNLOAD AND LOGIN RGB APP

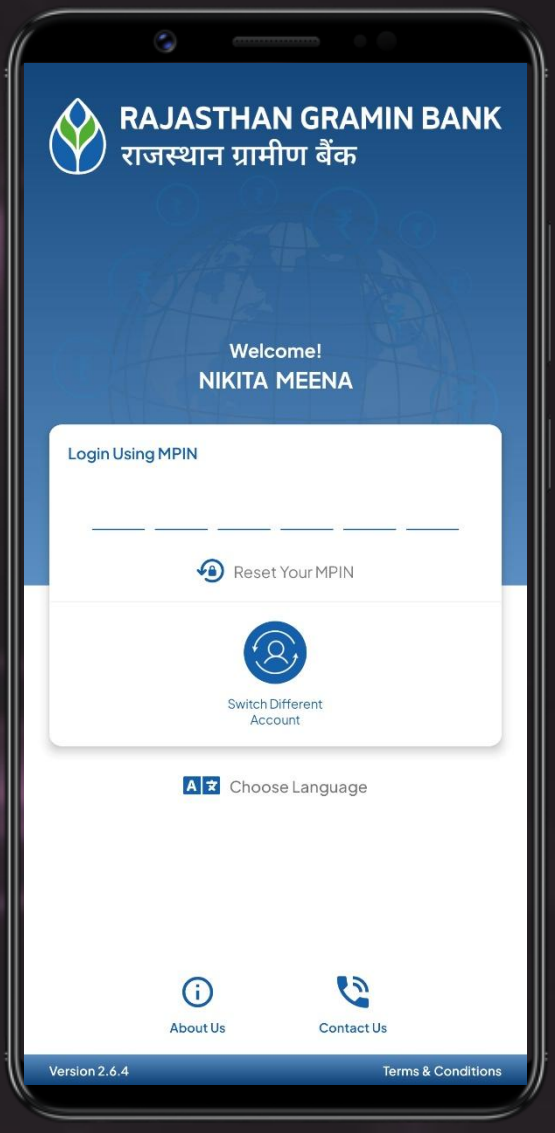
STEP 1:

Download RGB Mobile application 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 and enter MPIN to login.





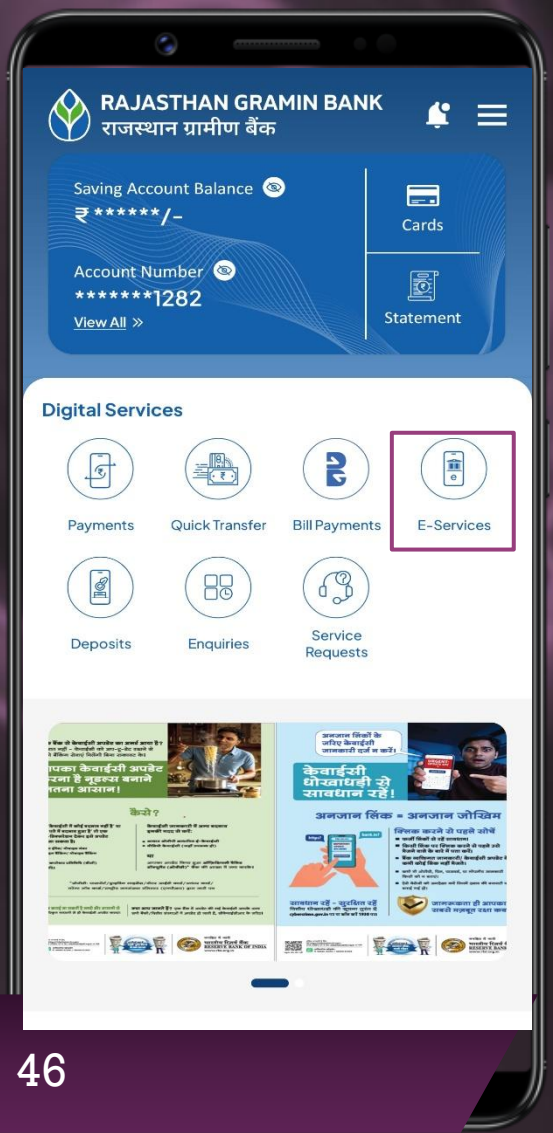
SET DEBIT/ATM CARD LIMIT

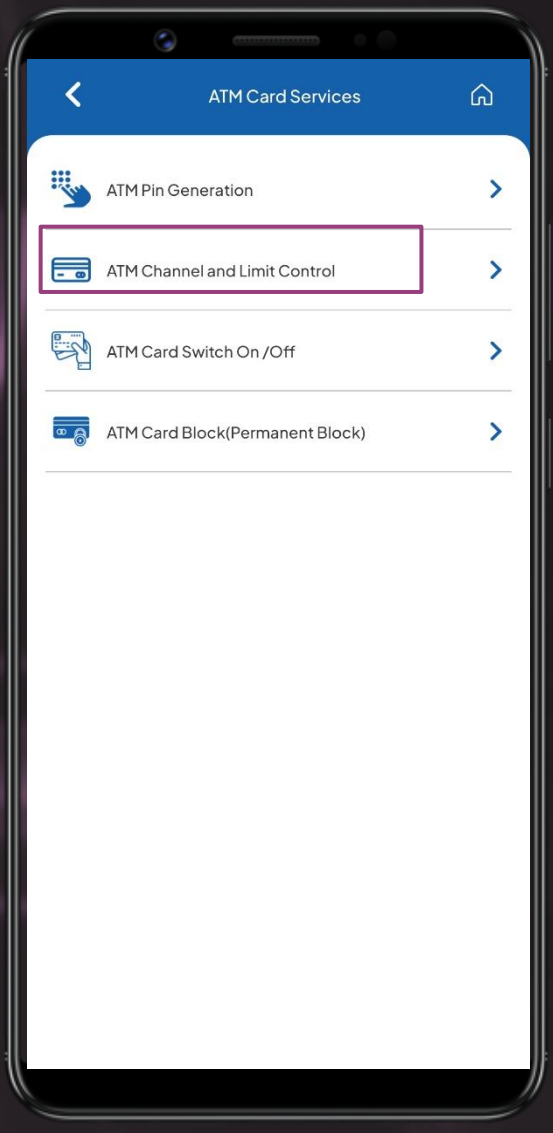
STEP 1:

Go to E-Services and than ATM Card Services.

STEP 2:

Click on ATM Channel and Limit Control.



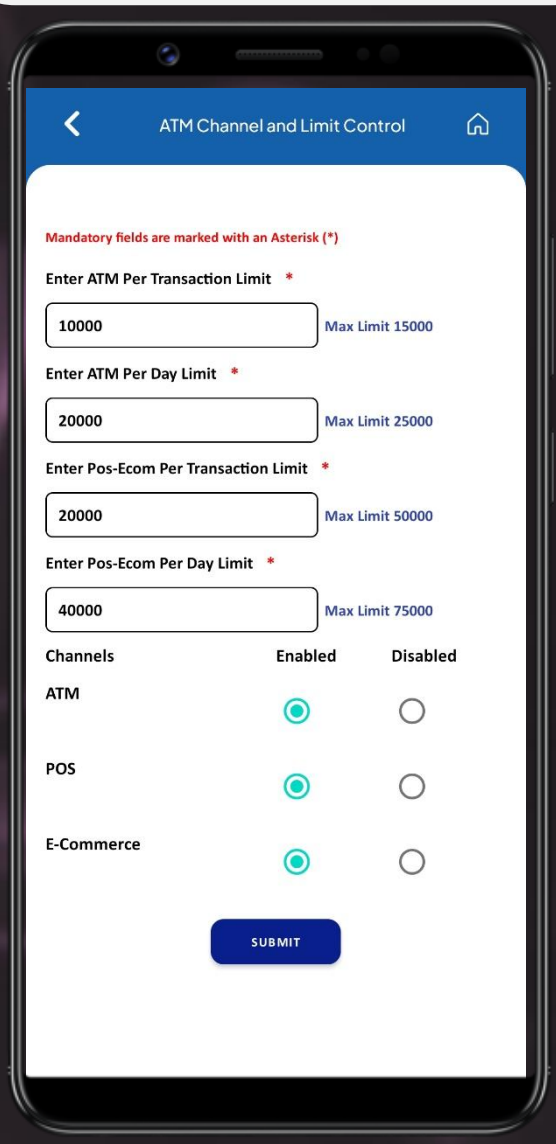


SET DEBIT/ATM CARD LIMIT

STEP 3:
Select Account Number and card number from the drop down.

STEP 2:

Enter the desired limit for transactions and click submit.



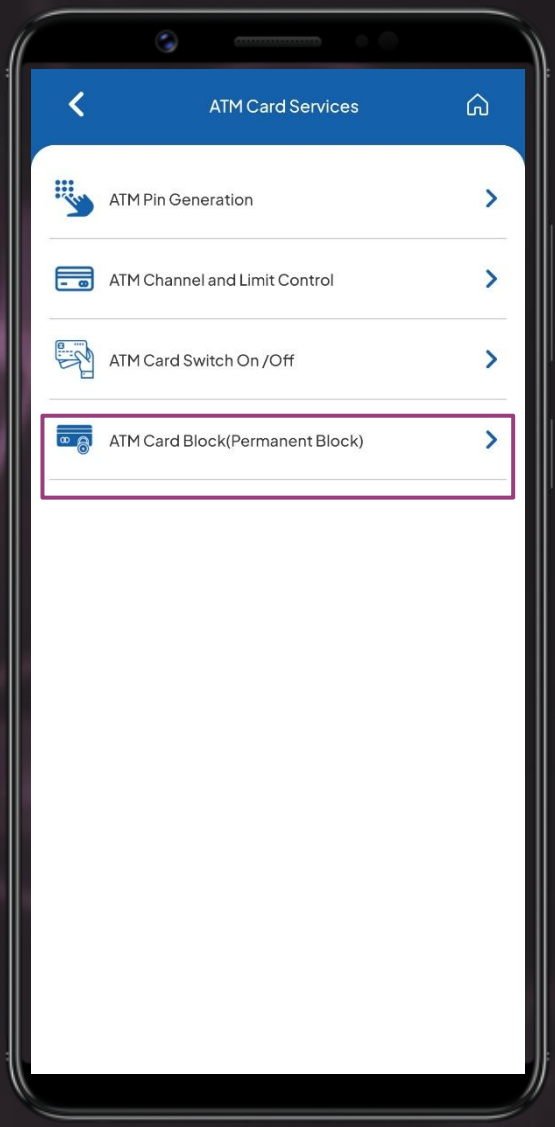
HOW TO BLOCK ATM/DEBIT CARD

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 Card through following ways:

- Go to the mobile Banking App and block the ATM card through the App.
- You can also block ATM Card through the nearest RGB Branch.
- You can also block ATM Card through the nearest RGB Branch.

STEP 1:

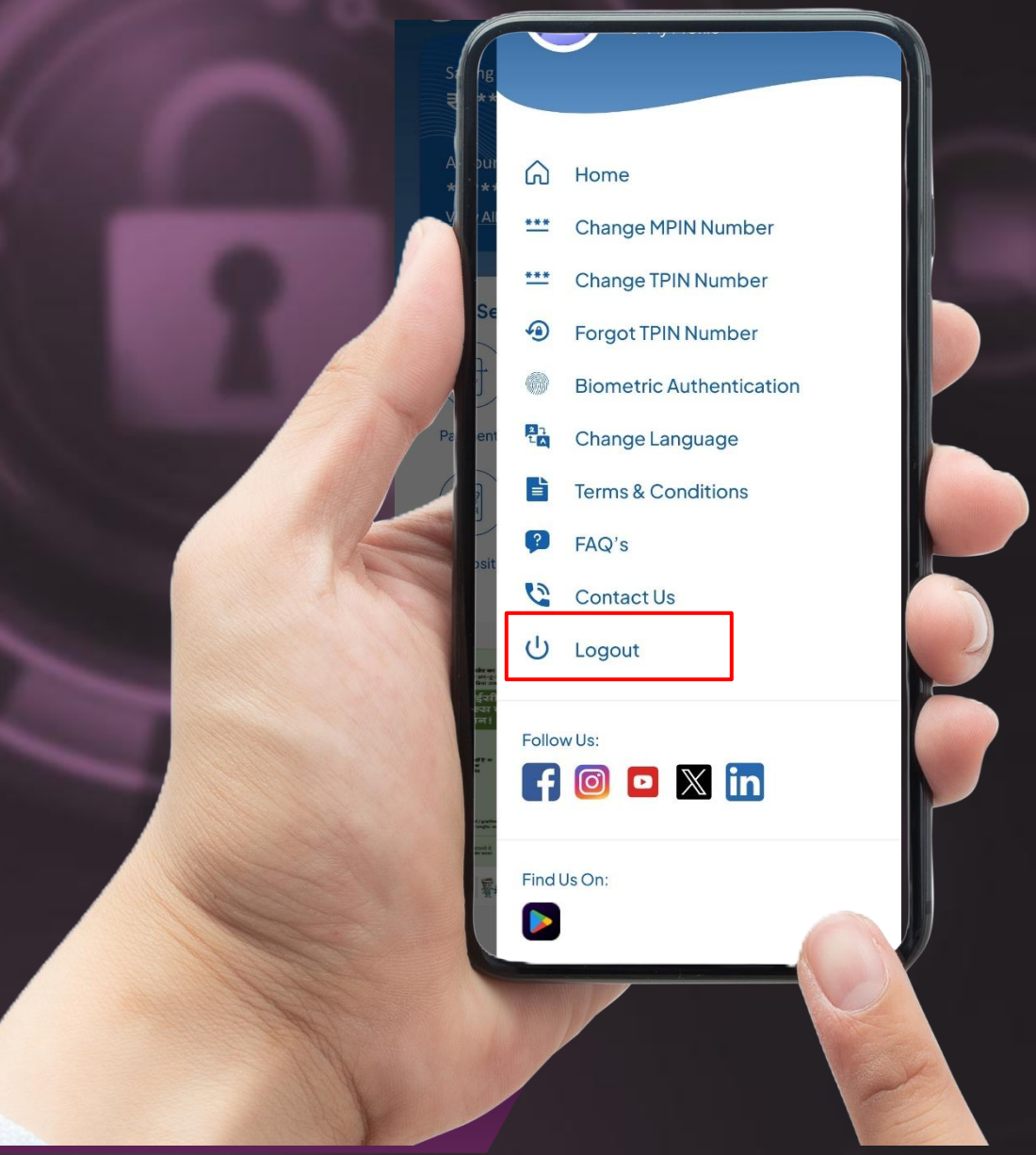
Click on the ATM Card Block(Permanent Block) from ATM Card Service menu. Select account number and card number and submit.



SAFE LOGOUT

1. Always logout from your RGB Mobile banking app 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 you 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 device to access your RGB 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/

- For blocking of Account/Debit card to stop further unauthorized transactions please call RGB's helpline number 1800-532-7444 ,1800-833-1004 , 1800-123-6230