

SSFB CUSTOMER AWARENESS SERIES

Be An *Informed Consumer*

SAFE BANKING



SHIVALIK

Shivalik Small Finance Bank

NEXT

Shivalik Small Finance Bank presents



Customer Awareness Series

A compilation of an articles published in newspapers, covering a wide range of banking products and services.

The booklet contains :

- Safety tips to manage bank accounts, cards
- Knowledge on how to avoid frauds,
- Systematic use of modern banking technology.

We hope you find the information useful.

www.shivalik.bank.in

NEXT

SSFB Customer Awareness Series

Index

Bank

Online Banking

Cheque

Card

Stay informed

ATM

Mobile Banking

Loans



SHIVALIK

Shivalik Small Finance Bank

PROTECT YOURSELF FROM IDENTITY THEFT.

Mr. Kapoor received a call from someone claiming to be from his bank, offering a zero balance saving account. The person visited at the agreed time, helped him to fill the application form, took his signatures, collected the required documents, thanked him and went away.

One fine day Mr. Kapoor got a call informing him that he had exceeded his credit-card spend limit. He wondered which card.... and then realised that he had never received that upgraded card.

What happened? Someone had stolen his identity and used the card!

Identity theft is a criminal activity where an impostor uses somebody's personal and confidential information such as name, address and date of birth for personal benefit without the owner's knowledge.

How can you protect yourself?

- Confirm the bona fides of the bank executive visiting you before parting with any information.
- Make a note of his name, contact numbers and ID number for future reference.
- Keep photocopies of documents that you need to submit with the application in. Never hand over original documents like PAN card, passport, etc. to strangers.
- Never hand over your existing credit card for upgrade or exchange.
- If you do not hear from the executive after you have handed over the application form, check with the bank.

Destroy old statements of account, unused cards, paid bills, payment receipts of premiums of insurance policies and copies of driving licence, passport, etc.



Don't Let Your Banking Details FALL INTO THE WRONG HANDS

Considering an example: An SMS of your account balance is sent to someone else's mobile number. An e-mail with your credit-card statement lands in a someone else's inbox.

If you do not update your bank's records with your current contact details, you may miss below benefits:

- Timely SMS and e-mail alerts of every transaction made on your accounts. The ability to track your banking and card transactions 24x7.
- Timely receipt of your bank-account statements so that you can keep track of your transactions.
- Receipt of cheque books, debit card at the right address.
- Notices of due dates of payment for your loan accounts

Make sure that your latest contact details are always available with your bank. Whenever there is a change, visit your branch and update your details.

Beware! It could be a fraud. Your bank will **NEVER** send you an e-mail asking you to enter your banking details.



Your Inoperative Account Can Be A TARGET for FRAUD

Saving and current accounts are classified as "Inoperative" when there are no customer induced transactions done for more than 2 years. The credit of interest and debit of service charges are not considered as customer induced transactions.

An Inoperative account is vulnerable to fraud.

- Inoperative accounts are easy targets of money-transfer agents or for phishing scams.
- Such accounts are prone to be used for illegal transactions, laundering money or funding terrorism, any of which could land a bona fide customer in serious trouble.
- If you move to new address and do not update your bank with your new address, account statements and other sensitive documents could be delivered in the wrong hands. Fraudsters could use them for theft of identity or misuse of your funds.





Always keep track of all your bank accounts.

Ensure that your bank's records are updated with your current demographic details.



THINGS TO REMEMBER While Writing A Cheque

Do not fail to write Account Payee or "A/c Payee", unless issued for cash withdrawal.

Do not leave any space between 'Pay' and the name of the payee that you write on the cheque. Similarly when entering the amount in words, do not leave space after 'Rupees'. Draw a cross line through the unused spaces to prevent unauthorized additions.



Strike out the 'OR BEARER' unless Issued for cash withdrawal.

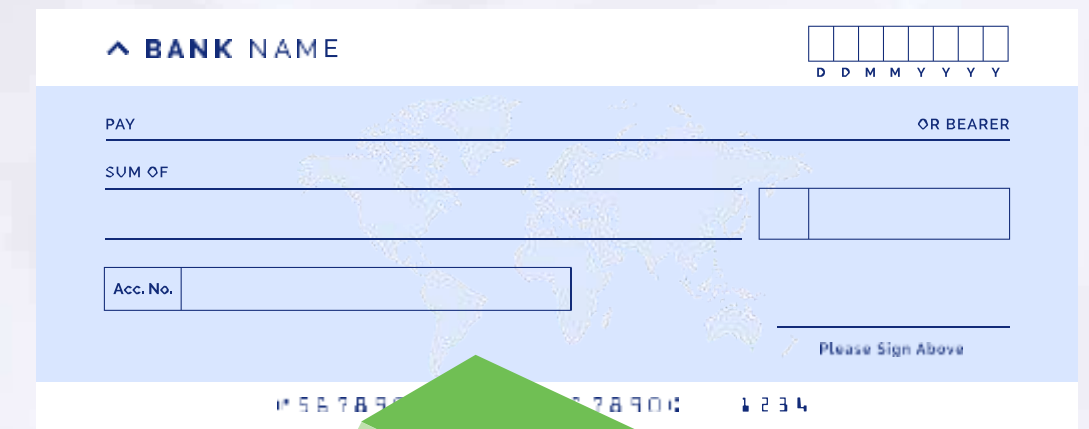
Do not leave any space between "Rs." and the amount in figures that you write.

- Destroy old cancelled cheques, unless needed for tax purposes.
- Always use a pen with dark or permanent ink.
- Always write the full credit card number on cheques issued for the payment of credit card bills.
- Never sign a cheque leaving the amount blank.
- In the case of other bill payments, write the particulars such as connection number on the reverse side of the cheque.



Safety Measures For **THE HANDLING OF CHEQUES**

- Count the leaves of a new cheque book as soon as you receive it.
- If you fail to receive the cheque book you requested within a reasonable time, check with your bank.
- When writing cheques, use permanent ink, without leaving any blank spaces, and cross the cheque "A/c payee" before signing it.
- Follow the practice of periodically tallying the cheque numbers with the amounts on your passbook or bank account statement.
- Keep your cheque book in a safe place when not in use, separate from credit cards, ATM cards or any documents that bear your signature.
- Report lost or missing cheques to your bank immediately along with the serial numbers of the lost/missing cheques.
- If you close a loan or choose not to avail of it, take your unused cheques back from the bank.
- If you close your account, destroy all unused cheques.



When using a drop box to deposit a cheque, ensure to choose a drop box that belongs to the bank in which the payee's account is held.



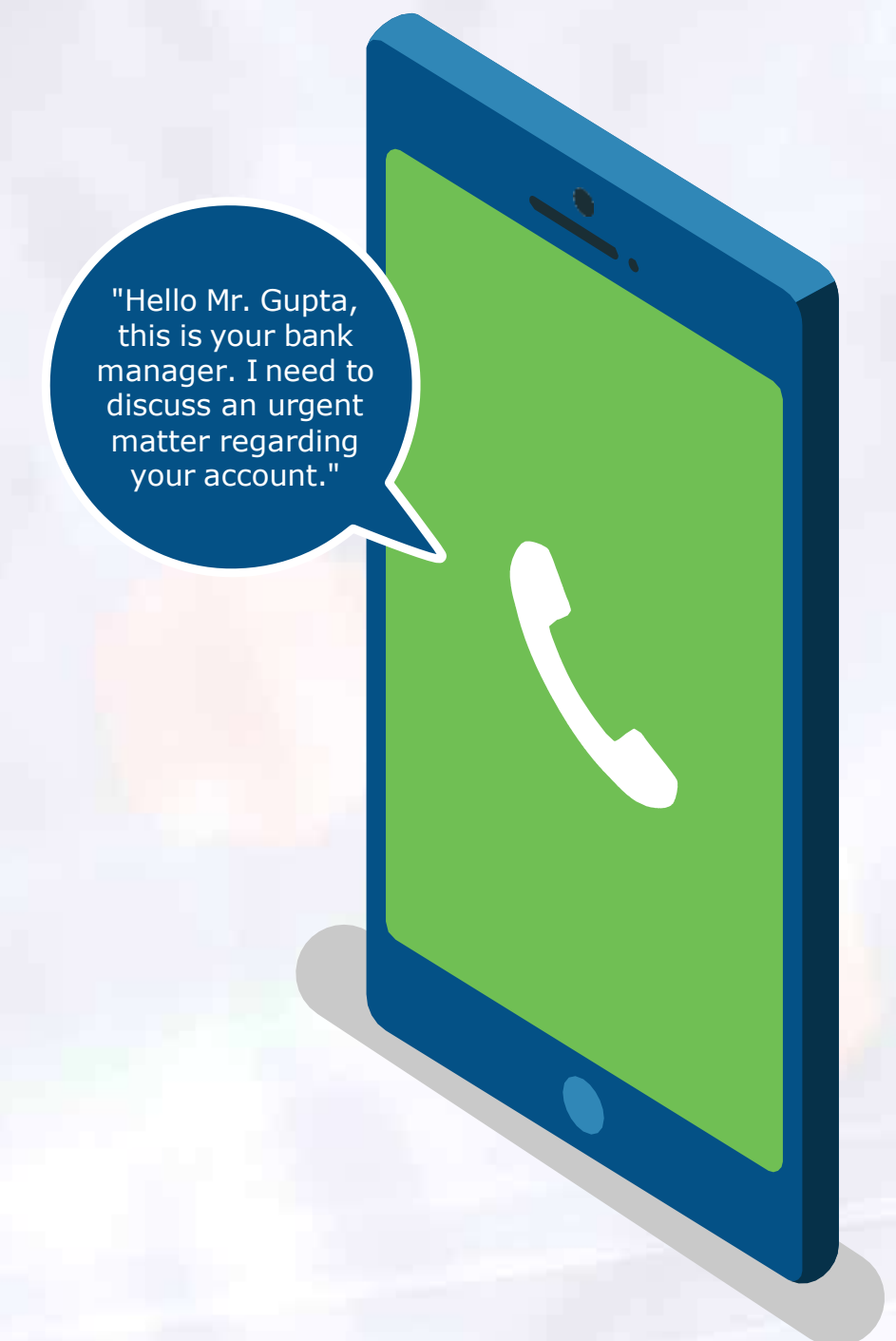
Beware of OF VISHING..

Mr. Gupta received a call from a person claiming to be an employee of his bank, asking him for his confidential banking details. Mr. Gupta obliged and later discovered unauthorised transactions in his account that left him poorer.

This is "vishing", a form of phishing where a fraudster uses the phone instead of e-mail to lure people into revealing their confidential banking details to them.

If you get a call from a stranger asking you for your confidential banking details such as account number, debit -credit card details, PIN's, passwords, OTP, CVV etc. report to your bank immediately.

Never give your PIN, OTP, CVV or other bank account details on an unsolicited phone calls.



"Hello Mr. Gupta, this is your bank manager. I need to discuss an urgent matter regarding your account."



What is **PHISHING?**

'**Phishing**' is an act of sending a fraudulent e-mail or creating a forged screen, in an attempt to capture a customer's sensitive personal details like user ID, password, PIN, CVV, etc.

How is Phishing carried out ?

Through e-mails

- Unsuspecting customers are sent e-mails, which look very similar to the authentic mails sent by bank.
- In emails, the customer is asked to click on a link which redirects him to a fake site resembling the authentic bank site.
- On this fake site, customers are asked to share their personal details like PIN, CVV, OTP etc.



Once the personal online information is submitted, the fraudster can then use it to make online transactions, posing to be the genuine customer.

Through pop ups

- A pop up window appears on the screen while the customer is logged into the bank website.
- These pop ups request the customer to re-enter their personal details. Since this pop up appears during the online banking session, it can be mistaken to be an authentic request from the bank.

DO NOT PROVIDE YOUR PERSONAL DETAILS LIKE PIN, CVV, ETC ON ANY LINKS, UNLESS YOU HAVE INITIATED THE TRANSACTION.



Beware Of Fraudsters Trying To CAPTURE YOUR PERSONAL DETAILS.



Phishing is an attempt by fraudsters to "fish" for your personal and confidential details, like User ID, Password, PIN, etc. through e-mails. This information is then used to take money out from your bank account through a fund transfer.

DO's and DON'Ts

- Always type the website address. Be wary of clicking on links; they could lead to false websites.
- Do not share confidential data on non-https websites.
- Do not enter your confidential data in any window that may pop-up while carrying out a financial transaction via online.
- Do not open e-mails or attachments sent from people you don't know.

Beware of phishing e-mails.

Your bank or Reserve Bank of India will never ask for your personal details Do not share your personal details with anyone.



How To Identify **A PHISHING E-MAIL ?**

- The e-mail might appear to have come from your bank website.
- The URL of the fake site will not match the URL of the legitimate site.
- The e-mail may show urgency for action.
- Any e-mail requesting for your confidential details is almost certainly a phishing attempt.

Do not respond to such phishing e-mails. Remember, your bank and RBI will never ask you for your confidential banking details.

Phishing is a fraudulent act of sending an e-mail under a false pretext to obtain sensitive confidential information about a customer like his user ID, password, PIN, DOB, OTP, CVV etc. These details are further used to siphon off money from the customer's bank account.



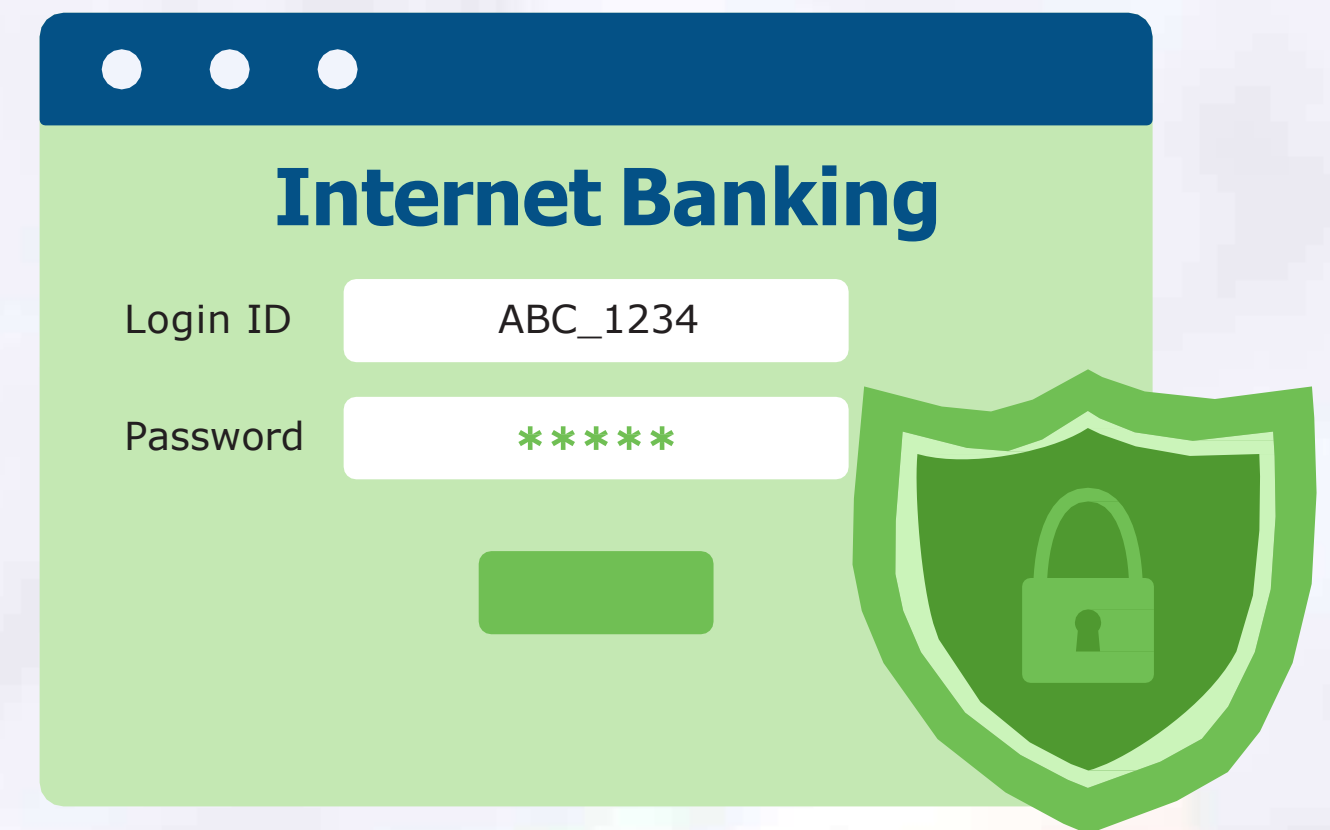
Safeguard Yourself AGAINST PHISHING!



- Never respond to any e-mail that requires you to confirm, upgrade, renew or validate your account details, even if it appears to have come from bank.
- Do not share your OTP, CVV with anybody, even if the caller claims to be from bank.
- Always remember to log out once you have completed an online session. Avoid financial transactions from a unknown devices or shared PCs.
- Register for e-mail and mobile alerts to get to know well in time about the transactions or any modification in your account.

To know more, please visit www.shivalik.bank.in

Check your bank statements regularly. If you notice an unauthorised transaction in your bank account or card account, report it to your bank immediately.



BEING A MONEY MULE

Might be Against The rules.

Money transfer agents, or 'money mules' as they are commonly known, are people who offer their bank accounts for use by fraudsters to transfer funds through the Internet.

The fraudsters normally advertise seemingly legitimate jobs in newspapers or the Internet, offering a commission for using an applicant's bank account. Little does the innocent respondent realise that such an activity could lead to criminal offences such as money-laundering or cheating through phishing and other scams.

The advertisements may call for people with accounts in certain banks, especially banks with online banking facilities.

How can you avoid becoming a money mule?

- Be cautious about any unsolicited offers or opportunities offering you easy money or jobs with work-at-home and flexi-time facilities.
- Do not participate in bids for lending your bank account for use by strangers.



Even if you have nothing to do with the actual theft of funds from the bank account of another person, allowing your account to be used for such movement of funds is illegal. If caught, you may suffer severe penalties including imprisonment.



How To Identify **AN E-MAIL SCAM**

If your reaction to an e-mail offer is "This seems too good to be true", the offer is almost certainly a scam.

Be cautious and suspicious of the following:

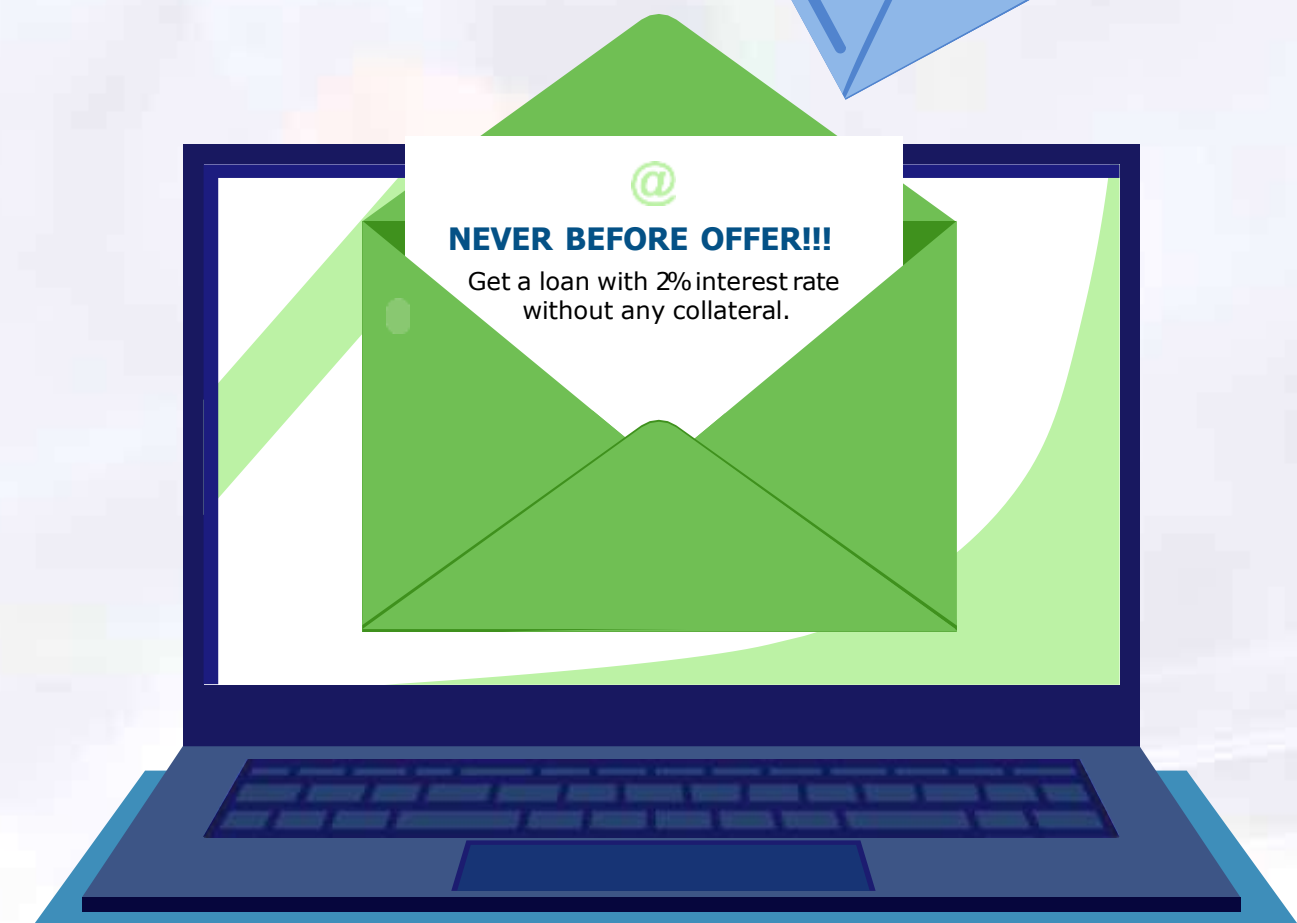
- Sweepstakes and lotteries that you had not registered for, asking you to make a payment in order to receive your prize amount.
- An e-mail from a free e-mail account with the name of a big corporate or an organisation that has no authorized website.
- Offer for jobs that you had not applied, asking you to make a payment for more information for getting jobs.
- High-yield investment plans, money-doubling schemes.
- Intimations of gifts and inheritance coming from a other countries.
- Loan schemes asking for processing fees in advance.

Simply ignore such communications.



Be alert, these are frauds. Do not respond to such e-mails.

Reserve Bank of India issued Circular no. 54 on May 26, 2010 advising that making remittances in any form towards participation in lottery schemes or any other money-circulation schemes can be fraudulent and is prohibited under Foreign Exchange Management Act, 1999.



How to safeguard yourself **FROM ONLINE FRAUD.**

- Never trust e-mails offering overseas employment opportunities.
- Ignore e-mails that ask you to deposit money in advance as a condition to your receiving some large amount of prize money.
- Fraudsters often operate under names that look very similar to the official names of reputed companies.
- Never deposit cash, cheques or DD in any unknown bank account.
- Do not make a hasty decision to reply to any e-mail that makes big promises.

Caution! Never share your bank account details with strangers, they could be fraudsters aiming to use your account for illegal activities for which you will be held liable.

Beware of e-mail scams.



How to create **A HARD-TO-CRACK PASSWORD**



SHIVALIK
Shivalik Small Finance Bank

Your password is a key that opens the door to your banking account. So, you need to create your password Carefully and change them often.

Here are a few tips for creating strong passwords:

- Avoid your name, nick name, the names of your patents, your birthday, your car number etc. Complicate them with capitals and small letters; use numeric character along with characters.
- Do not create a password so complicated to remember that you need to write it down somewhere.
- At the same time, never yield to the temptation of leaving your password below the mouse pad, in your dairy or on a post-it slip stuck to your PCs.
- Soon after you receive your password, log in to your account, change the password immediately and destroy the security paper that brought you the password.
- Avoid typing a password in front of someone.



Re-set your password periodically.

***Do not disclose your password to anyone.
Keep it to yourself.***



PRECAUTIONS *whilg using an ATM*

The automated teller machine (ATM), along with the ATM card and PIN, has proved to be a boon for bank-account holders. You can make your ATM operations safe, if you remember some simple precautions:

- Memorize your PIN. Do not write it down anywhere.
- Your card is for your own personal use. Do not share your PIN or card with anyone.
- "Shoulder surfers" can peep at your PIN as you enter it. So, stand close to the ATM and use your body and hand to shield the keypad as you enter the PIN.
- Do not take the help of strangers for using the ATM card or handling your cash.
- Press the "Cancel" key before moving away from the ATM. Remember to take your card and transaction slip with you.
- If you choose to take a transaction slip, destroy it immediately after use.
- If your ATM card is lost or stolen, report it to your bank immediately.
- When you deposit a cheque or cash into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.

If you have any complaint about your ATM/debit/credit card transaction at an ATM, you should take it up with the bank that issued the card to you.

If your card gets stuck in the ATM, or if cash is not dispensed after your having keyed in a transaction, call your bank immediately.



One Little Mistake, Your ATM Card Could END UP IN THE WRONG HANDS.



SHIVALIK
Shivalik Small Finance Bank

You can make your ATM operations safe, by observing below simple precautions:

- Memorize your PIN. Do not keep your card and PIN together.
- Do not share your PIN or card with anyone.
- Stand close to the ATM while entering your PIN.
- Do not take the help of strangers for using the card.
- Always press the 'Cancel' key before moving away from the ATM.

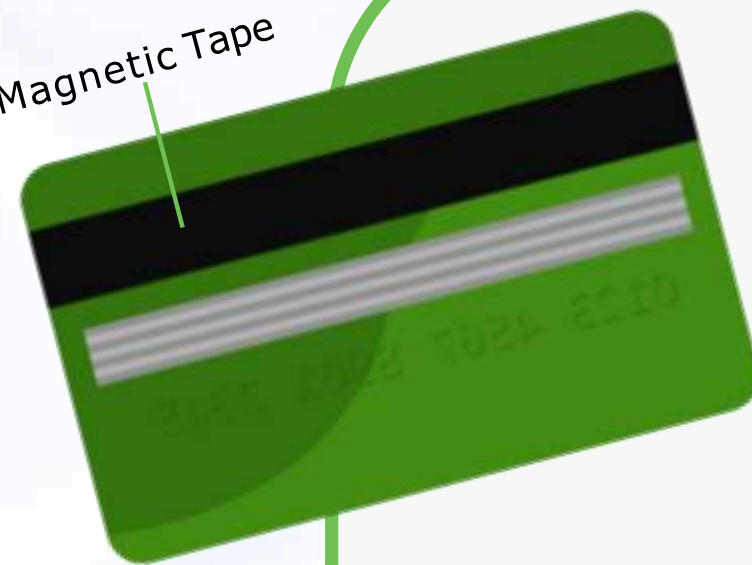
*If your card gets stuck in the ATM, or if cash is not dispensed after you have keyed in a transaction, press the "Cancel" key and call your bank immediately.



How can you safeguard YOURSELF AGAINST SKIMMING?

- Skimming is the fraudulent collection of confidential information from a credit/debit/ATM card by reading the magnetic strip on the reverse of the card.
- Skimming can occur in restaurants, shops or other locations where you physically give control of your card to someone who can run it through their skimming machine without your knowledge.
- The fraudsters use the captured information for shopping online or at merchant establishments.

Magnetic Tape



Tips to protect yourself from skimming

- Keep your card in view when you give it for payment at merchant establishments, to ensure that it is not swiped on multiple devices.
- Register with your card-issuing bank for SMS alerts to keep track of your card transactions.
- Make sure you collect your card immediately after every transaction.
- Beware of strangers offering to help you with using the card.



*Check your account statements regularly to ensure that all payments/debits are for genuine transactions.

Protect your money.



ENJOY SAFE BANKING at ATM's



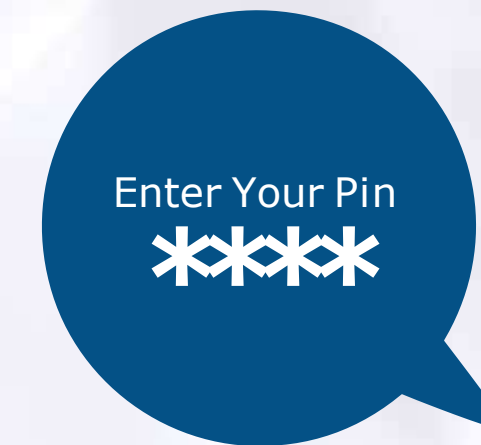
SHIVALIK
Shivalik Small Finance Bank

The ATM makes banking transactions easier and quicker. Taking a few precautions can make it ~~totally~~ hassle-free and safe.

- Do not write your PIN anywhere; never on the card itself.
- Do not share your PIN or card with anyone, not even your friends or family.
- Do not take the help of strangers for using the ATM card or handling your cash.
- If you choose to take a transaction slip, shred it immediately after use.
- If your ATM card is lost or stolen, report it to your card-issuing bank immediately.

If you have any complaint about your ATM/debit/credit card transaction at an ATM, you should take it up with the bank that issued the card to you.

If your card gets stuck in the ATM, or if cash is not dispensed after your having keyed in a transaction, call your bank immediately.



MOBILE BANKING

Ensure safety, empower yourself

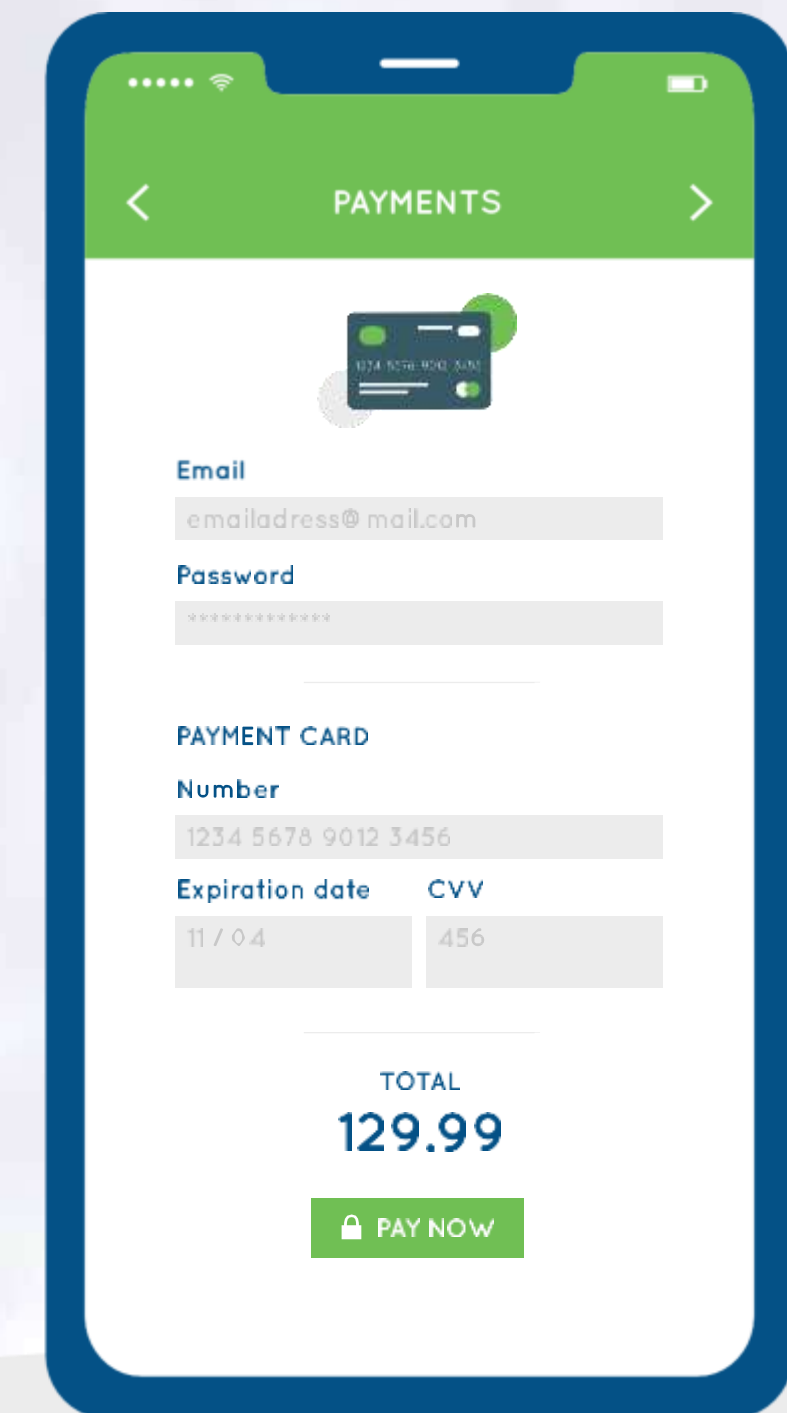


With mobile banking, your banking and financial transactions are at your fingertips. Here are some precautions for safe mobile banking:

- Set up a PIN/password to access the handset menu on your mobile phone.
- Delete junk messages and chain messages regularly.
- Do not follow any URL in messages that you are not sure about.
- If you have to share your mobile with anyone else or send it for repair/maintenance.
 - > Clear the browsing history
 - > Clear cache and temporary files stored in the memory as they may contain your account numbers and other sensitive information
 - > Block your mobile banking applications by contacting your bank, You can unblock them when you get the mobile back

Do not save personal information such as your debit card numbers, CVV numbers or PIN's on your mobile phone.

Do not part with confidential information received from your bank on your mobile.



Beware of SIM-SWAP FRAUD!

Your mobile phone is now also a convenient banking channel; but it can make you vulnerable to SIM-swap fraudsters if you do not take some simple precautions.

How do SIM-swap frauds occur?

- The fraudster obtains your mobile phone number and bank account details through a phishing e-mail.
- He asks your mobile-phone-service provider for a replacement SIM card under some pretext, like changeover to a new handset or loss of SIM/handset.
- The service provider deactivates your SIM card and gives him a replacement SIM.
- The fraudster introduces a payee into your bank account using the phished data, transfers funds from your account to his and withdraws the money through an ATM.
- All this while, your service provider's alerts don't reach you because your SIM card has been deactivated.

If you find your mobile number inactive for an unusually long period or abruptly barred from calls; or if it displays limited access or says the SIM is inactive; contact your service provider without delay and find out the reason.



CAR LOANS: *Have A Smooth Drive!*

Taking a car loan from a bank is a common and popular means to buy a car, From making the loan application to closing the loan, it becomes an easy drive when you bear the following in mind:

- Check with the bank officials the credentials of the agency through whom you are applying for the loan.
- Confirm the details on the proforma invoice before submitting it to the bank.
- Ensure that the hypothecation in the Registration Certificate (RC) Book and insurance cover note is in favour of your lending bank. This is in line with all the leading banks' loan process.
- Make sure that Form-34 for car registration is submitted to the transport authority, signed by you and carrying your banker's stamp and signature.
- Ensure that the numbers of the car's engine and chassis are indicated in the final invoice.
- Do not hand over documents to anyone. Always keep photocopies ready to avoid misuse.
- If you decide not to avail of the loan after submitting the documents, inform the bank immediately to ensure cancellation.
- Do not make payment in cash to anyone, Always issue crossed, post-dated cheques and security PDCs in favour of the lending bank only.
- After you have cleared your loan ensure you seek an NOC from your lending bank.
- Visit the bank's website for all relevant information related to the loan.

Delay of a single day in payment of EME customer as a defaulter and this can affect his credit record with CIBIL (Credit Information Bureau India) Limited



Safety Tips When Taking **A HOME LOAN**

A home loan is a long-term commitment. It is wise to exercise prudence and take extra care while going through the process of loan.

Here are some helpful and important tips:

- Ask the bank executive you are dealing with for proof of his/her identity.
- Keep all documents with attested photocopies ready.
- Make sure you sign every photocopied page before you attach it to your application.
- Check all the filled-in details with care before finally handing over your application to the bank executive.
- Avoid giving the original documents to the executive.
- If you issue any cheques for charges or fees, remember to issue them in favour of your bank, and not any individual.
- After submission of the documents if you decide not to avail of the loan, inform the bank immediately.

Check the Most Important
Information note before signing
loan documents

Ensure that the title of
the property is clear



BE INFORMED!



SHIVALIK
Shivalik Small Finance Bank

In a continuously evolving banking industry, banks strive to make their products and processes transparent and keep their customers informed. The channels of information and communication for you are:



Branch notice boards and Tariff guides provide all relevant guidelines and information.



Branch-customer meets usually held on a monthly basis to register your views and suggestions.



Complaint box and register are available for you to put up all your concerns/issues.



Contact information of senior management for escalations are displayed at branches.



Write to the Banking Ombudsman if you are not satisfied with the resolution of your issue.



BE ALERT!



SHIVALIK
Shivalik Small Finance Bank

Safeguarding your money and interests is most important while carrying out a banking transaction, whether at your bank branch/ATM or from your home/office. Here are some best practices that will help:



Do not share your PIN or password with anyone.



Do not leave your cash, signed cheques or debit/credit cards unattended.



Do not take the assistance of strangers for filling your account details or for counting cash.



Ask the loan executive for proper identification before giving him your EMI cheque.

Always ensure that you check your account statements for debits and report any irregularity within 30 days of receipt of the statement.

Register for Mobile updates
for instant account information.



BE ALERT. BE UPDATED.
Anytime. Anywhere.



SHIVALIK
Shivalik Small Finance Bank

Get SMS alerts for:

**Your account
XXXXX12345 has
been credited
with Rs.31,000
on 23-Jul-23
by Salary.**

**You have made
a Debit Card
purchasg of
Rs,5,000 on
21-Jul-23 at
Bun Stort.**

**Payment of
Rs. 20,000 on
Your ABC Bank
Credit Card is
due on
14-Aug-23.**

Visit your bank's website, register for Mobile Banking and subscribe to mobile alerts.

To know more, please visit www.shivalik.bank.in and go to the "Mobile Banking" section.

