ICICI BANK CUSTOMER EDUCATION SERIES

BE AN INFORMED CONSUMER

ICICI Bank
khayaal aapka

Next

ICICI Bank presents

Customer Education Series

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

The booklet contains

- Safety tips to manage bank accounts and cards
- Efficient use of modern banking technology
- Knowledge on how to avoid frauds

We hope you find the information useful as well as interesting.

ICICI Bank
www.icicibank.com

Next

ICICI BANK CUSTOMER EDUCATION SERIES

INDEX

ICICI Bank
khayaal aapka

Don't Let Your Banking Details Fall Into The Wrong Hands

Consider these scenarios: An SMS on your account balance is sent to someone else's mobile number. An e-mail with your credit-card statement lands in a colleague's inbox.

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

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

ICICI Bank
khayaal aapka

Make sure that your latest contact details are always available with your bank. Whenever there is a change, call your bank's Customer Care, visit your branch or visit your bank's website and inform them.

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

PROTECT YOURSELF FROM IDENTITY THEFT.

Mr. Sharma received a call from someone claiming to be from his bank, offering a free Platinum credit card. The person visited at the agreed time, helped him fill the application form, took his signatures, collected the required documents, thanked him and went away.

One fine day Mr. Sharma 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 sales executive visiting you before parting with any information.
- Make a note of his name, contact phone numbers and ID number for future reference.
- Keep photocopies of documents that you need to submit with the application. Never hand over original identity documents like the PAN card, election ID card, etc. to strangers.
- Never hand over your current credit card for exchange or upgrade.
- 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 for utilities, payment receipts of premiums for insurance policies and copies of driving licence, passport, ration card, etc.

Your Dormant Account Can Be A Target For Fraud

Savings and current accounts are classified as dormant when there are no customer-originated transactions in them for more than two years. Bank-induced credits of interest and debits of service charges are not considered as customer-originated transactions in this context.

A dormant account is vulnerable to fraud.

- Dormant 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 house and do not update your bank with your new address, account statements and other sensitive documents could land in the wrong hands. Fraudsters could use them for theft of identity or to siphon off funds.

ICICI Bank
khayaal aapka

Keep track of all your bank accounts.

Ensure that your bank's records are updated with your current contact 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, while entering the amount in words, do not leave any space after 'RUPEES'. Draw a line through the unused spaces to prevent unauthorised additions/ alterations.

Strike out 'OR BEARER', unless issued for cash withdrawal.

Do not leave any space between 'Rs.' and the amount in figures that you write. Remember to use '/-' to clearly specify the rupees and paise values.

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

Safety Measures For The Handling Of Cheques

- When writing cheques, use permanent ink, write clearly 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. Also, verify that the unused cheque leaves are intact.
- 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.
- 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 the bank.
- 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 your bank.
- If you close your account, return all unused cheques and requisition slips to the bank.

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

Ensure Safety

When You Travel Abroad

The pre-paid travel card is a secure option for carrying foreign currency when you travel overseas.

Benefits Of The Pre-Paid Travel Card

- **Safety**
  The pre-paid travel card comes with a replacement card. If you lose your card while abroad, just call up the bank that issued the card, get the card deactivate and the replacement card activated.

- **Convenience**
  Shop using the card or withdraw money in local currency from ATMs -- 24x7 in any country.

- **Shop online**
  Use the card to buy air tickets, make hotel bookings and shop online, when abroad.

- **Customer Service**
  Banks that offer pre-paid travel cards usually offer 24-hr customer service, an international toll-free number, SMS alerts, tracking of transactions, etc. to make your experience hassle-free.

Security Tips for the Usage of Credit Cards

When you receive your card

- Sign on the signature panel of your credit card as soon as you receive the card.
- Never write the PIN on your credit card or keep it along with the card.
- If you happen to get a pre-approved credit card that you have not applied for, inform the issuing bank immediately to cancel it.

For the safety of your card

- Inform your bank immediately when you change your address.
- While travelling, carry only those cards that you intend using.
- Keep your card number and the issuing bank's phone number handy so as to be able to contact them quickly if your card gets lost or stolen.

Tips regarding payment

- Save the receipts of your credit card till you verify the entries in your monthly statement. This will help in the event of any dispute.
- Remember to collect your credit card after making payment at a merchant establishment and make sure that the returned card is your own.

To discard your card

- Never hand over your card to anyone for cancellation or upgradation. Cut it across the magnetic strip and discard the pieces.

Your card is your personal responsibility.
Never lend it to anyone and never leave it unattended.

ICICI Bank
khayaal aapka

Use 3D Secure To Safeguard Your Online Transactions

3D Secure (Three Domain Secure) is an additional layer of protection for online purchases that allows you to make online financial credit/debit-card transactions with greater security.

How does it work?

- You need to register for 3D Secure. Registration is an easy, one-time activity, carried out through the Internet.
- To register, you need to key in relevant information on the card-issuer's website. The system will then send you a code at your e-mail address or through SMS at your registered mobile number.
- This code will enable you to create your own secret password, which you will need to use for all your subsequent online payment transactions.
- Every time you use your card for an online purchase transaction and enter the 3D Secure password, the card-issuer's server will verify the authentication details before allowing the transaction to be completed.
- The process is simple and totally automated, hence confidentiality is maintained.

Register all your cards for 3D Secure, including add-on cards, to prevent their misuse.

ICICI Bank
khayaal aapka

Never disclose your secret 3D Secure password to anyone, even if it's a family member or close associate.

Verified by VISA
MasterCard. SecureCode.
Look for these logos when making purchases online.

Keep Your 3D Secure Passcode Secret

Mr. Roy, who has not registered for 3D Secure, receives an SMS from his bank giving him a passcode. He ignores the message. Later, somebody claiming to be from his bank calls and asks him for the passcode for verification. Mr. Roy obliges. Some days later, he finds transactions that he has not carried out billed to his card account.

What happened?

The caller was a fraudster who had used Mr. Roy's credit-card number, mobile number and other personal details to register for 3D Secure, obtained the passcode from Mr. Roy and used it to make online purchases.

- The 3D Secure passcode is an additional layer of security provided to you to reset the 3D security PIN of your card.
- When you register for 3D Secure with your bank, the bank conveys this passcode by SMS to your registered mobile number.
- This passcode enables you to create your own secret password, which you will need to use for all your subsequent online payment transactions.

Thus, someone equipped with your credit-card number and 3D Secure passcode can reset your PIN and use your card to make online payment.

ICICI Bank
khayaal aapka

- ✓ Never reveal your 3D Secure passcode to anyone.
- ✓ If you have not tried to generate or reset your 3D Secure PIN but still receive an SMS giving you a passcode, report it to your bank right away.

Beware of Vishing!

Mr. Sharma received a call from a person claiming to be an employee of his bank, asking him for his confidential banking details. Mr. Sharma 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.

If you get a call from a stranger asking you for your confidential banking details such as account number, debit/credit-card details, PINs, passwords, etc. report it to your bank with the following information:

- The calling number, if you have a caller ID facility.
- Any pertinent details of the conversation or recorded message.
- The call-back number, if indicated during the call.

When you add a payee through Internet banking, your bank will give you a secret code (in the case of ICICI Bank, a Unique Reference Number – URN) that you will need to use to authorise transfer of money online from your account to the new payee's account. Do not reveal this code to any stranger, even if the person claims to be an employee of your bank. If you receive an SMS with such a code from your bank without your having added a new payee, report it to your bank immediately.

Remember, your bank will never call, e-mail, or text you asking for your account number or related information that is already present in its records.

ICICI Bank
khayaal aapka

Never give your PIN, URN or other bank account details on an unsolicited phone call.

What is Phishing?

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

How is Phishing carried out?

Through e-mails

1. Unsuspecting customers are sent e-mails, which look very similar to the authentic mails sent by banks.
2. In these e-mails, the customer is asked to click on a link which redirects him to a fake site resembling the authentic bank site.
3. On this fake site, customers are asked to share their personal details.

Through pop ups

1. A pop up window appears on the screen while the customer is logged into the bank website.
2. These pop ups request the customer to re-enter his or her personal online identity details. Since this pop up appears during the online banking session, it can be easily mistaken to be an authentic request from the bank.
3. This is called 'In-session Phishing' and has surfaced recently.

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

Do not provide your personal details on any links or pop ups, unless you have initiated the transaction.

ICICI Bank
www.icicibank.com

Ensure that you upgrade to latest browsers like IE 6.0, Firefox 3.5, Opera 10, Chrome 2.0 etc. These have inbuilt security features.

BEWARE OF ONLINE FRAUDSTERS TRYING TO CAPTURE YOUR PERSONAL DETAILS.

PROTECT YOURSELF FROM PHISHING.

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

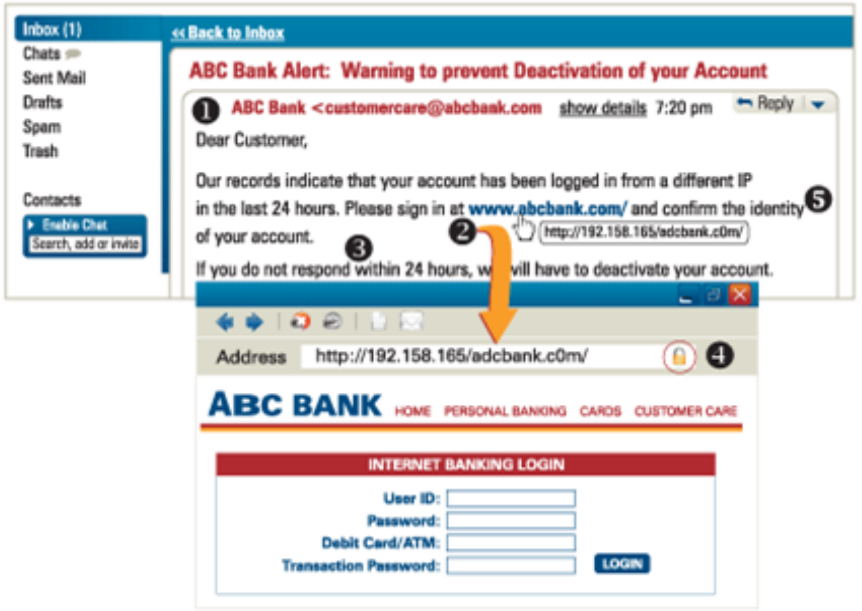
DO's and DON'Ts

- Always type the website address. Be wary of clicking on links; they could lead to false websites.
- Do not transact or share confidential data on non-https websites.
- Do not enter your confidential data in any window that may pop-up while you are carrying out a financial transaction online.
- Do not open e-mails or attachments in e-mails 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 them with anyone.

ICICI Bank
khayaal aapka

How To Identify A Phishing E-Mail



1. The e-mail might appear to have come from your bank or a known website.
2. Some of the characters of the sender's URL might be missing or would closely resemble those of the genuine URL. The URL of the fake site will not match the URL of the legitimate site.
3. The e-mail may show urgency for action.
4. The padlock icon may be missing.
5. Any e-mail request for your personal and confidential details is almost certainly a phishing attempt.

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

ICICI Bank
khayaal aapka

Phishing is a fraudulent act of sending an e-mail under a false pretext to obtain sensitive personal information about a customer like his user ID, password, PIN, date of birth, CVV number etc. These details are then used to siphon off money from the customer's bank/credit-card account.

Safeguard yourself against phishing!

- Never respond to any e-mail that requires you to confirm, upgrade, renew or validate your account details or card details, even if it appears to have come from your bank.
- Do not share your OTP, URN or 3D secure passcodes with anybody, even if the caller claims to be from your bank.
- Always remember to log off once you have completed an online session. Avoid financial transactions from a cybercafé or shared computer.
- Register for e-mail alerts and mobile alerts to get to know well in time about transactions or any changes in your account.
- Upgrade your home computer to a legitimate (non-pirated) operating system with a firewall, latest version of browser and anti-virus / anti-spyware software.

To know more, please visit www.icicibank.com.

ICICI Bank
khayaal aapka

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

Online shopping is now even more safe and secure.

What does this mean?

From August 1, 2009, while making a purchase online, you will be asked to enter a password or PIN in addition to your card details. This is an additional level of security for online purchases, mandated by Reserve Bank of India.

How do I get my PIN/password?

Most banks have detailed instructions on their websites about obtaining this PIN/password. For example, ICICI Bank customers can generate this PIN by visiting www.icicibank.com and following the instructions given. Alternatively, you can also call your bank's customer service and find out.

How do I use this PIN?

- At the time of making an online payment, you will be prompted to enter your PIN/password in addition to your card details.
- From August 1, 2009, online transaction cannot be completed successfully, unless you enter this additional PIN/password.

In the interest of your security:

- It is recommended to visit your bank's website and register for Verified by Visa and MasterCard SecureCode.
- Never click on any links received through e-mails that ask you to enter your card details, user ID or password.
- Do not respond to any SMS that asks you for your card details, user ID or password.

ICICI Bank
www.icicibank.com

Verified by VISA
MasterCard. SecureCode.

Look for these logos while purchasing online.

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.

REMEMBER

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.

ICICI Bank
khayaal aapka

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
- An e-mail from a free e-mail account with the name of a large corporate or an organisation that has no website
- Offers for jobs that you had not applied for, asking you to make a payment for more information
- High-yield investment plans, money-doubling schemes and multi-level marketing schemes offering unrealistic returns on investment
- Intimations of gifts and inheritance coming from a foreign country
- Loan schemes asking for processing fees in advance.

Simply ignore such communications.

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

ICICI Bank
khayaal aapka

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.

Fraudsters send attractive offers through letters, e-mails, calls, SMS messages asking you to deposit money to participate in schemes that "**sound too good to be true**". Later, they withdraw the money and stop further communication.

Here is a list of the most common frauds:

- Contests and lotteries that you had not registered for, asking you to make a payment for receiving your prize
- Emails appearing to have been sent from large corporations, public institutions and regulatory bodies
- Phone calls or SMSes offering jobs that you had not applied for; intimations of gifts or inheritances supposed to originate from a foreign country, asking you for personal information
- High-yield investment plans and multi-level marketing schemes offering unealistic returns on investment; please checks the credentials of the person offering these

ICICI Bank
khayaal aapka

Make sure you don't respond to such fraudulent messages.

How to safeguard yourself from online fraud.

- Never trust e-mails offering overseas employment opportunities that sound too good to be true.
- Ignore e-mails that ask you to deposit money in advance as a condition to your receiving some prize money.
- Fraudsters often operate under names that look very similar to the official names of long-standing and reputed companies. Be vigilant.
- Never deposit cash or cheques 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 illicit activities for which you will be held liable.

ICICI Bank
khayaal aapka

Beware of e-mail scams.
Never part with your money for gifts, prizes, lottery winnings or jobs offered by e-mails from strangers.

SAFE BANKING

One-Time Password (OTP) for Payment Transactions on IVR

IVR (interactive voice response) transactions are those made over the phone where certain credit-card details are to be entered into an automated system in order to make payment to a merchant for the purchase of his goods/services.

Following a recent Reserve Bank of India mandate, credit-card-issuing banks in India have introduced an additional measure of security for IVR transactions on their credit cards – the OTP.

What is an OTP?

An OTP is a six-digit code that you obtain from your card-issuing bank. It is a single-use password, valid for a limited period from the time of placing a request for it. You will need to obtain an OTP before every IVR payment transaction.

How to obtain an OTP?

You can obtain an OTP through various modes like your card-issuing bank's website, the Internet, SMS, etc. The mode varies from bank to bank.

How to use the OTP?

The OTP is required at the time of making payment on the IVR, where you will be prompted to enter it along with the other details like your credit-card number, card expiry date and CVV number.

ICICI Bank
khayaal aapka

With effect from February 1, 2011, every time you pay for a purchase or service through any merchant's telephone system (IVR), you will be asked to input the OTP. Without the OTP, you will not be able to complete the payment transaction.

How to create a hard-to-crack password

Your Internet banking password is the key that opens the door to your account. Therefore, you need to create and choose your passwords carefully and change them often.

Here are a few tips for creating good passwords:

• Avoid your name, pet name, the names of your kids, your birthday, your employee number, car number etc. Complicate them with capitals and small letters; use numbers and characters.

• Adapt an important date, the first line of your favourite song or the name of a movie. "One flew over the cuckoo's nest", for example, can get you "ofotcnest". Here, the initial letters of the words are taken, except the last word, which is retained in full.

• 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, keyboard, in your dairy or on a post-it slip stuck to your monitor!

• Soon after you receive your password, log in to your account, change the password and destroy the twin-layered security paper that brought you the password.

• Avoid typing a password in front of someone. Passwords like "kumar123456" are so easy for peepers to see and remember

ICICI Bank
khayaal aapka

Re-set your password periodically to reduce vulnerability.

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

SAFE BANKING

Precautions while using an ATM

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

- Memorise your PIN. Do not write it down anywhere, and certainly never on the card itself.
- Your card is for your own personal use. Do not share your PIN or card with anyone, not even your friends or family.
- "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, shred it immediately after use.
- If your ATM card is lost or stolen, report it to your card issuing-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.

ICICI Bank
khayaal aapka

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.

SAFE BANKING

ONE LITTLE MISTAKE, AND YOUR ATM CARD COULD END UP IN THE WRONG HANDS.

You can make your ATM (Automated Teller Machine) operations safe, by observing some simple precautions:

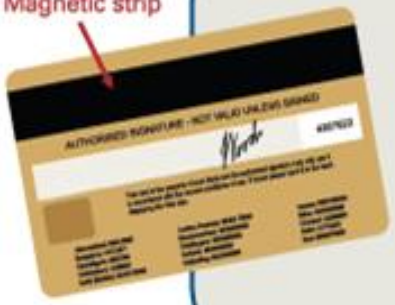
- Memorise your PIN. Do not keep your card and PIN together.
- Do not share your PIN or card with anyone.
- Stand close to the ATM while entering your PIN.
- Do not take the help of strangers for using the card or handling cash.
- Always press the 'Cancel' key before moving away from the ATM.

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.

ICICI Bank
khayaal aapka

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.



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.

ICICI Bank
khayaal aapka

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

Enjoy Safe Banking at ATM's

The automated teller machine (ATM) makes banking transactions easier and quicker. Taking a few precautions can add to the pleasure of your ATM experience and 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.

ICICI Bank
khayaal aapka

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.

SAFE BANKING

Mobile Banking — Ensure safety, empower yourself

With mobile banking, your banking and financial transactions are at your fingertips.

Here are some precautions for safe and secure 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 confidential information such as your debit/credit card numbers, CVV numbers or PIN's on your mobile phone.

ICICI Bank
www.icicibank.com

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.

What are the safeguards that should be taken?

- Never respond to phishing e-mails.
- Do not disclose your mobile phone number on unknown websites.
- Change your banking passwords frequently.

ICICI Bank
www.icicibank.com

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.

Sign the application form only after filling it and reading the terms and conditions.

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.

Here are some helpful 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.

If you do not receive a reply regarding acceptance or rejection of your loan-application within the time specified, contact the bank through their Customer Care or branch.

ICICI Bank
khayaal aapka

Does The Property You Are Buying Have Legal And Technical Approval?

Buying a house is a once-in-a-lifetime event to most. While choosing the property best suited to your needs, technical verification and legal appraisal of the property are of vital importance.

Technical Verification

You need to verify whether the property is approved by the appropriate authorities, with respect to:

- Construction/Building plans
- Permission from the local municipal/town-planning authorities.

Legal Appraisal

You need to verify whether certain legal approvals are in place, like:

- Whether the property has a clear title and is free of dispute
- Whether the developer has ownership/development rights.

It is always advisable to have the documents checked by an advocate to ascertain whether the land- and development-related clearances are in place.

To know more, log on to: www.icicibank.com/home.

ICICI Bank
khayaal aapka

Repay your Home Loan EMI by either submitting post-dated cheques or giving a standing instruction through auto-debit or Electronic Clearing Service (ECS).

Loans, Credit Cards And Credit History

Do you have a good credit history?

- When you apply for a loan or a credit card, the lending institution checks with credit bureaus and tracks your repayment history.
- Your monthly repayment behaviour directly impacts your credit score that the credit bureaus compute and give to the lending institution.
- It is prudent to resolve queries, if any, and clear all pending/accumulated dues on your loan / credit card as soon as possible.
- It is also advisable to maintain a record of all your loan/credit-card repayments - past, present and future. This will help solve disputes, if any.
- With the advent of credit bureaus, the likelihood of a credit defaulter getting fresh credit today is greatly reduced.

ICICI Bank
khayaal aapka

Did you know?

A credit bureau is an organisation that gathers from lending institutions credit information on individual borrowers and makes it available to banks / specified lenders in the form of a credit score of the individual. Credit bureaus provide details of the borrowing and bill-paying habits of individuals.

Be Informed!

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 numbers of senior management
for escalations are displayed at branches.

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

ICICI Bank
www.icicibank.com

Interact with your branch! Know your bank and help the bank know you!
Banks hold monthly customer engagement programmes on a designated day every month. This forum is a window for customers to offer feedback, suggestions and even raise grievances, if any.
Contact your branch for details of their **Customer** meet program.

Read the schedule of charges that are available in branches / bank website for complete awareness of the tariff applicable.

Be Alert!

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.

ICICI Bank
www.icicibank.com

Update all your contact details (e-mail ids, phone numbers, postal addresses) with your bank to ensure that you don't miss out on any important communication.

Register for Mobile updates for instant account information.

Be alert. Be updated. Anytime. Anywhere.

Get SMS alerts for:

... and many more

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

To know more, please visit www.icicibank.com and go to the 'Mobile Banking' section.

ICICI Bank
www.icicibank.com

Safe banking advice
Always register your mobile number with your bank and update it whenever you change the number.

Beware of greetings through e-cards laden with computer viruses. If the 'well-wisher' is not well-known to you, consider the simpler option: delete the e-mail. Even opening such an e-mail could unleash a virus or a Trojan onto your PC.