

Digital Banking Frauds



IFE Academy

Education Simplified

INVESTORS FINANCIAL EDUCATION ACADEMY

Phone : 044 - 2814 3044

email : bulletin@ifea.in

www.ifea.in

Is it necessary to buy Life Insurance when you are young?



- Would your **loved one** be responsible for looking after any loans or expenses in any unforeseen situations?
- Are you expecting or do you have **dependents**?
- Do you have a **mortgage**?
- Would you want your family to **manage financially** if you aren't around?

If the answer is YES to any of these, now may be the time to consider life insurance.

And remember...

**THE YOUNGER AND HEALTHIER YOU ARE,
THE BETTER YOUR RATES CAN BE !**



Digital Banking Frauds

First Edition, 2021

All Rights Reserved

Rs. 40/-


Published By
Investors Financial Education Academy
Parkview, Basement, 85/17, G.N.Chetty Road,
T. Nagar , Chennai - 600017.



Introduction:

Online banking, also known as Internet banking or Web banking or e-banking, is an electronic system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Any service can be selected and further



interaction can be made depending on nature of service. Banks give their banking services through Electronic modes such as mobile banking, Telephone banking, debit card, credit card, Automated teller machine (ATM), Unified Payments Interface (UPI), Cheque Transaction payment system. Due to the internet banking, need for customer to visit the branch has been significantly reduced.

Emergence of Online Banking:

Over a last few decades, technology had drastically changed the banking industry which gave rise to a new concept called E-Banking. E-Banking became popular in late 80s where the system could be accessed with phone lines. But nowadays with computers and internet, e-banking continues to grow.



Advantages of Online Banking:

Online Banking allows customers to do almost everything without having to visit any branch of their banks. It offers a range of advantages and they are mainly the same around all countries and they are:-



- **Informational:** They provide clients with information about the products and services offered by banks which are free of cost.
- **Communication:** Clients can get information about their accounts and can update their profiles as they can get access to the bank's main system.
- **Transactional:** Customers can pay their bills, transfer money, make loan application without any inconvenience of going to bank, waiting for their turn and complete their transactions.
- More over, with e-banking, banks can target customers of other countries not necessarily the home countries alone.
- 24/7 the Bank account can be accessed by the client anytime and anywhere. This facilitates in **time saving**.
- The Online Banking portal of bank can easily access all past banking activities such as transfers, deposits, cleared cheques and more. No matter if the transaction was done last week, last month or last year, can quickly go through the **entire history with only a few clicks**.
- Online banking also helps in promptly paying the tax within minutes and get instant confirmation. Some of the banks also offer exclusive **tax assistance services** to their account holders.





Disadvantages of Online Banking:

While online banking is always improving, there are some disadvantages for clients on immediate and constant access to their banking services.

- **Technology disruptions:** Online banking relies on a strong internet connection. If internet is disrupted by a power outage, server issues at bank, or in a remote location, ability to access the accounts might be affected. Scheduled site maintenance also means accounts cannot be accessed and may have to seek an alternative.
- **Lack of a personal relationship:** A personal relationship with bank may be able to offer an advantage over online banking. If the client need a business loan, a new line of credit, a waived fee or to make changes to their current banking needs, having that relationship can help. But in online banking there wouldn't be any personal relationship contact with the banker.
- **Potential to Overspend:** The ability to check account balances in the spur of the moment could potentially cause some people to overspend the limits of their accounts. Without a careful look at the passbook or record of uncleared debit transactions, the account balance may not accurately reflect the true amount that is available. Overdrafts and fees might occur if close look of the transaction is not being done.

Online Banking Frauds:

With the advances in information technology, all banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space. Internet Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet



Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing, lottery fraud scam etc. Now internet banking is widely used to check account details, make purchases, pay bills, transfer funds, print statements etc. But due to ignorance or silly mistakes customer can easily fall into the trap of internet scams or frauds done by the fraudsters. The following are the various types of frauds done in Online Banking.

· **Phishing:**

Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing).

Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

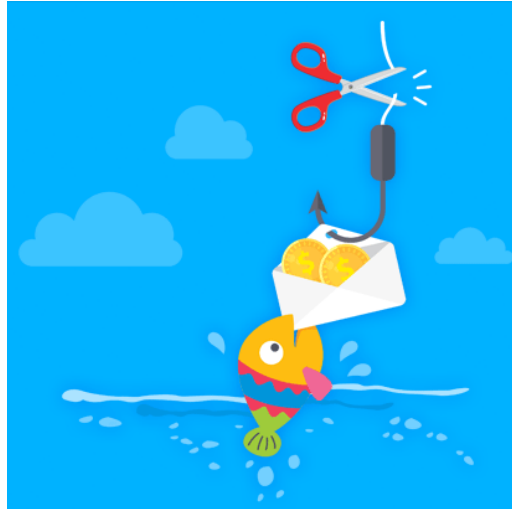


Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information.

Information so acquired is then used to conduct fraudulent transactions on the customer's account.


Tips To Protect from Phishing

- The Bank will never send e-mails that ask for confidential information. If you receive an e-mail requesting your Internet Banking security details like PIN, password or account number, you should not respond.
- Whenever you use a link to access a website, be sure to check for the URL of the website and compare it with the original. Beware of such websites! It is recommended to type the URL whenever you access or bookmark/store the URL in your list of 'Favourite's.
- Delete suspicious e-mails without opening them. If you happen to open them, do not click any link or attachment they may contain.
- If you receive a job offer via e-mail, ensure that it's from a genuine and reputed company.



Spoofing:

Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate,



hackers use the names, logos, graphics and even codes of the actual websites. They can even fake the URL that appears in the address field at the top of the browser window and the Padlock icon that appears at the bottom right corner. Hackers send e-mails with a link to a spoofed website asking to update or confirm account related information. This is done with the intention of obtaining sensitive account related information like Internet Banking user ID, password, PIN, payment card / bank account number, card verification value (CVV) number, etc.



Tips To Protect from Spoofed Websites

- Check for the Padlock icon: There is a default standard among web browsers to display a Padlock icon somewhere in the window of the browser. For example, Google Chrome displays the lock icon at the top in front of the url. Click (or double-click) on it in your web browser to see details of the site's security. It is important for you to check to whom this certificate has been issued, because some fraudulent websites may have a padlock icon to imitate the Padlock icon of the browser.

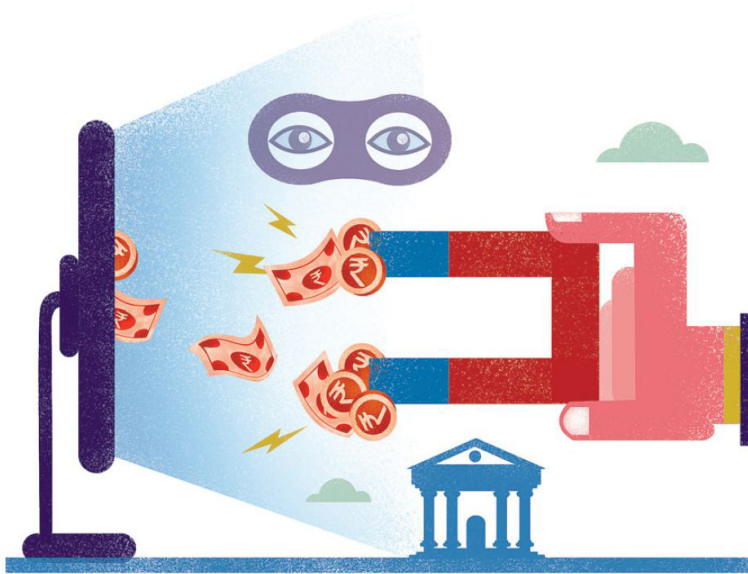
Tips To Protect from Skimming



- Be alert - keep your card in your sight at all times during transactions to ensure your card is not swiped through a foreign device.
- Protect your PIN - shield the keypad when you enter your PIN at an ATM or point-of-sale terminal.
- Check your receipts - ensure they display the correct amount, date, time.
- Review statements regularly - report unauthorized transactions to the Bank immediately.

Payment Fraud:

Payment fraud is any type of false or illegal transaction completed by the hacker. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet. This payment fraud generally happens in online shopping. The hackers would do unauthorized online payment transactions using your credentials.



Tips To Protect from Payment Frauds:

- Be aware of the latest trends in online fraud
- Have a verified payment processor
- Use antivirus software that will run constant checks
- Regularly change login and token credentials

- Set-up strict policies for accessing crucial and sensitive information
- Emails and transactions with confidential information need to be encrypted
- Do the online payment in the known gadget and computers and not in browsing centres or other people computers.

Scams using UPI PIN:

UPI PIN is a kind of fraud in which the hackers would be sending "request money" links to the customer. Once the customer clicks on the link and authorises the transaction thinking they'll receive money, the amount gets deducted from their account. In few cases they would even convince the customer to disclose their UPI PIN over phone and would deduct money from the account. These days this UPI is being popularly used by all Online shopping sites, Food delivery sites, Google Pay, PhonePe, Paytm etc.

Tips To Protect from UPI PIN fraud:

- It is important to know that the receiver in a UPI transaction does not need to do anything to get their money.





- To transfer money or make a transaction using the UPI apps, users need to enter their M-PIN, which differs for every linked bank account. The M-PIN is like a digital ATM PIN. Do not disclose or share your M-PIN with anyone.
- Do not disclose your UPI Login and Password to others. To be on the safer side, put a lock on your payment apps.
- If someone sends you unwanted money request on your UPI app you can simply decline it. The amount will not be deducted from your account unless and until you accept the request and put in your M-PIN.
- It is recommended to not write your M-PINs anywhere on your phone as with remote access, hackers used to exploit the data on the phone as well as banking apps.

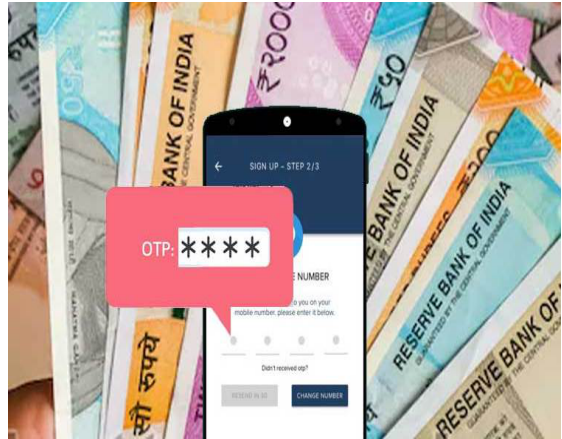
Scams using OTP

When a transaction is done through net banking / using your debit /credit card, an OTP is also sent as a two factor authentication. For OTP authentication, the bank sends an OTP through SMS on the registered mobile number with the bank records. Once the OTP is verified, the transaction is processed. OTP should not be disclosed to anyone. Once fraudster gets the details, they can authenticate the transactions and steal money from your account.



Tips To Protect from OTP fraud:

- Your OTPs are meant to be a secret, so you must never share your OTP with anyone over calls, SMS or emails. No banks or reputed companies will call asking for the OTP.



- **OTP is required** only when you are sending money, not while receiving money. Many people have been cheated by fraudsters who claim that they need to share OTPs for receiving money into their bank accounts.
- Fraudsters use fake apps to steal OTPs from your phone. You must be careful while downloading any apps on your phone. Download apps only from the reputed app stores and make sure to do a thorough background check.
- If you want to contact the customer support team of any company; make sure the number you are dialling is genuine. This is because fraudsters have set up many fake customer support teams with the intention of collecting personal information like card details and OTP.




Debit and Credit Card Frauds done in online payments:

Debit and Credit card fraud occurs when a criminal gains access to your debit card number — and in some cases, personal identification number (PIN) to make unauthorized purchases or withdraw cash from the account. A fraudster steals the card data and creates counterfeit cards. This typically happens with withdrawal cash at an ATM or by using the card at the time of online payments. Fraudsters attach a foreign device on ATMs or the debit card machine and capture your encrypted data.

Tips To Protect from Debit and Credit card frauds:

- The easiest way to spot debit card fraud is to sign up for online banking and monitor your account for suspicious activity.
- Getting bank alerts, going paperless, destroying old debit cards, and protecting mobile devices are recommended ways to help prevent debit card fraud.



- 
- If you find evidence of debit card fraud, contact your bank immediately and report the activity.
 - Use a secured network when using your mobile devices or computer in a public place for online transactions. It is better to avoid transactions in public places.

Remote Screen Monitoring:

In these frauds, the unsuspecting victim gets one of those messages that are sent in bulk to unspecified targets by the fraudsters. These messages come from a message ID that looks deceptively similar to their payment wallet and the gist of the message is that the recipient needs to get the KYC done for his or her account otherwise the account would be blocked. The fraudsters mention a mobile number that the recipient needs to call in order to get the KYC done.

When the recipient calls on the given number, the fraudster pretends to be someone working for wallet and asks the caller (the unsuspecting victim) to install a remote viewing Application such as Anydesk or Quick Support App. He, then, induces the victim to share the Anydesk (or other similar App) ID. After convincing the victim that it is an important step in the verification process, the fraudster, using the Anydesk App installed on his mobile, takes the remote access of the mobile phone of the victim by urging him to accept the remote access attempt. After that, the fraudster gets access to the bank account and e-wallets of the victim and illegally transfers as much money as he can to his own accounts or to



that of his associates. In these frauds, the victims end up losing several lakhs of Rupees. It must be noted that while all this goes on, the fraudster does not let the victim hang up the phone lest he/she should see the bank messages regarding the unauthorized transactions that are being done by the former. Once the fraud is complete, the swindler cuts the connection. By the time victim realizes what has happened, they end up losing a lot of money; sometimes even their life savings.

There are other variants of the fraud. Thus, fraudsters pretend to be Customer Care executives of a company in whose services the victim has shown interest, either through online search or through portals such as JustDial. To provide the online service, they ask the victim to download the remote viewing App and also make a small, token payment (Rs.1/2/5). While the victim makes payment, they capture the card credentials and using the remote access to victim's phone, make multiple, unauthorized UPI transactions.

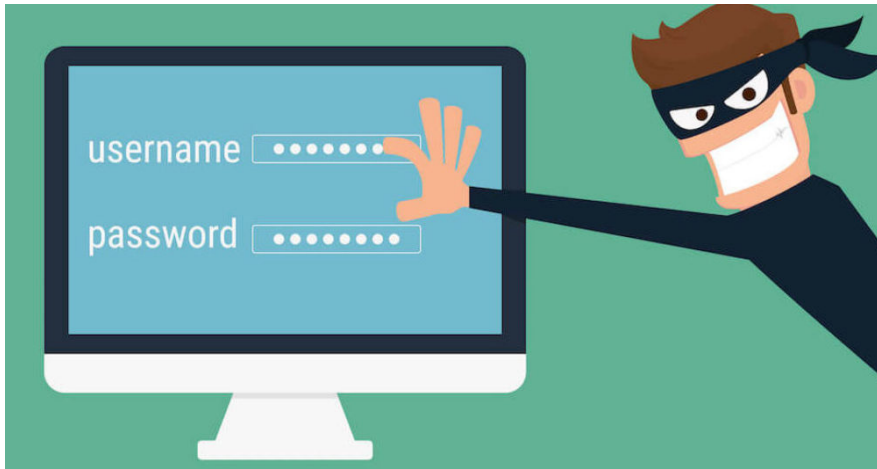


Safety Precautions:

1. Always treat unsolicited callers/emails/SMSes with suspicion.
2. Never share credit/debit card details with anyone claiming to be bank official or customer care executive.
3. Never enter card details in online form sent by the caller. Your credentials might be stolen.
4. Do not download remote access Apps as fraudster will get access to all your messages and emails.
5. Never click on links in Phishing messages/emails appearing to come from government organizations, officials, banks, etc. They install malware/spyware on your device.
6. Be cautious while scanning a QR code sent for receiving payment. You may lose money from your account.
7. Be careful of fake customer care number appearing in web search. Use two-factor authentication (Password + OTP) for all online accounts.


Steps to be followed in case of fraudulent activities happened in your Banking account:

- The moment you come to know that a suspicious transaction has been done on your credit/debit card or net banking



account, it is required to inform your banker immediately. A formal complaint is to be lodged with the bank and ideally customer care number can be called to block the card or the account immediately.

- A written complaint should be raised to the banker with the following documents:
 - o Bank statement of the last six months of the concerned account.
 - o Make a copy of SMS that was being received related to the alleged transactions.
 - o Take copy of ID proof and address proof as shown per the bank records.
 - o Lodge a complaint in nearest police station explaining the complete incidence along with the above documents.

- 
- In case of any financial fraud committed through an app, in addition to the above mentioned documents, also furnish the screenshot of the malicious app and the location from where it was downloaded.

RBI Rules and regulations with respect to Online Banking Frauds:

- RBI states that if the fraud happens and the bank is not at fault and it was committed by a third-party through an act of scamming, phishing etc, the customer is not required to pay if the breach that has been reported within three days of the fraudulent transaction.
- A transaction reported after that but within seven days, the per transaction liability of the customer will be limited to the transaction value or an amount set by the central bank, whichever is lower.
- In case the third-party fraud is reported with a delay of four to seven working days, RBI further stated that the resolution has to be over within 90 days. Banks have to credit or reverse the unauthorised electronic transaction to the customer's account within 10 working days from the date of notification by the customer.
- In cases where the loss is due to negligence by the account holder (such as sharing of payment credentials), the customer will bear the entire loss until the unauthorised transaction is reported to the bank.

Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions:



- RBI states that with the increased thrust on financial inclusion and customer protection considering the surge in customer grievances relating to unauthorised transactions resulting in debits to their accounts/ cards, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions was introduced.
- As per the Customer Protection by RBI there will be "zero liability of a customer" in case of third-party breach where the deficiency lies "neither with the bank nor with the customer but lies elsewhere in the system".
- RBI further said that banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.

5 Golden rules to be followed to avoid Online Banking frauds:

- **Change your password periodically**

It is very important to reset the password periodically as it will help you from potential hackers and will also reduce the risk of banking frauds.

- **Avoid using public computers for online banking**

Make a rule that you should never use a public computer or someone else's computer for online banking as it makes it easy for the fraudster to hack it and they can find ways to record your bank details and activity and that will land you into trouble.



- **Report about the lost card immediately**

If you lose your card then make sure that you report it immediately to the bank, so that the bank can block your card and it will prevent you from any future fraud.



- **Avoid clicking on suspicious mails**

Do note that you should avoid clicking on the suspicious email that has several links in it as it may help a hacker get unauthorized access to your account.

- **Don't share the bank details or OTP with someone on the phone**

It is to be noted that the bank never calls asking for details about the PIN, password, or account number over the phone. If you receive any such call then you should hang up the call and should report it to the bank immediately.

Don't let anyone score against you

Never share your Password, PIN, OTP, CVV, UPI-PIN, etc., with anyone



Rasika Raje

Indian Badminton Player and
RBI Employee

Poorvisha S. Ram

Indian Badminton Player and
RBI Employee

- Register your mobile number and email with your bank to get instant alerts
- Never store important banking data in mobile, email or purse
- Use only verified, secure and trusted websites for online banking
- Avoid banking through public, open or free networks
- Change your online banking password and PIN regularly
- Block your ATM Card, Debit Card, Credit Card, Prepaid Card immediately if it is lost or stolen



**RBI Kehta Hai...
Jaankar Baniye,
Satark Rahiye!**

For more details, give a missed call to 14440
or visit www.rbi.org.in/digitalbanking
For feedback on this advertisement, write to rbikehtahai@rbi.org.in

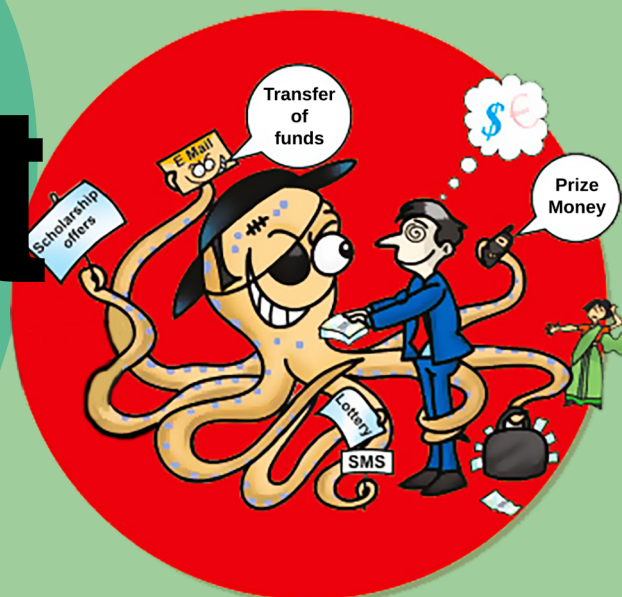


Issued in public interest by

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

Don't

get cheated by
Emails/SMSs/Calls
promising you
money



Have you received an Email/SMS/Call informing you that you have won a lottery or will get huge sums from abroad?

Or have you been offered cheap funds for your business?

Or have you received an email on a letterhead of the Reserve Bank of India with the Governor's photo on it and quoting a senior RBI official's name stating that RBI is holding funds for you which will be released if you pay some amount or part with the important details of your bank account like customer id and password?

Do not believe these. They are fake, howsoever official or attractive they may look. RBI never sends such emails.

- Don't send any money as an initial deposit/ commission/transfer fee to any unknown party in India or abroad
- Don't reveal your bank account number/details or any other related information to anyone, either on phone or through email.
- **Don't enter into any correspondence with any party - Indian or foreign - in the hope of receiving any money from them.**
- RBI does not hold funds or accounts for any individual/organisation/trust.
- Inform your friends/family members to be careful.
- Please inform the Cyber Cell/other Law Enforcing Agency of such fictitious offers.
- Please visit the official RBI website (www.rbi.org.in) for more details.

Remember... No one gives money for free to anyone

Issued in public interest by



भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in



Ministry of Consumer Affairs, Food and Public Distribution
Department of Consumer Affairs, Government of India
Krishi Bhawan, New Delhi - 110001
Website : www.fcamin.nic.in

Don't get clean bowled by a fraudulent or an unauthorised transaction in your bank account

Notify the bank immediately



Umesh Yadav

Indian Cricketer and RBI Employee

- The longer you take to notify the bank, the higher will be the risk of loss
- If the fraudulent transaction is due to your negligence, you will bear the loss till you report to the bank
- Ask your bank to provide you an acknowledgement when you notify it. It has to resolve your complaint within 90 days
- Always keep your bank's contact details handy to report fraudulent transactions



RBI Kehta Hai!

For more details, dial 14440 or visit www.rbi.org.in/LimitedLiability
For feedback on this advertisement, write to rbikehtahai@rbi.org.in



Issued in public interest by

भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

Convenience of digital transactions

Transact anytime,
anywhere



- Banking on your fingertips, from the comfort of your home
- Saves time through quick and safe payments
- Multiple digital payment options for various transactions
- NEFT, IMPS, UPI and BBPS available 24x7



Issued in public interest by
भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in



**RBI Kehta Hai...
Jaankar Baniye,
Satark Rahiye!**

Terms & conditions apply

About IFE Academy

IFE Academy was established in 2011 as a Not-for-Profit entity to promote Financial Education. IFE Academy conducts Investor Awareness Programs across the country with the support of other market participants. www.ifea.in is a comprehensive website on Financial Education. It has various sections such as Videos, Puzzles & Games, Financial Calculators and Library. It gives a holistic view on financial education combining various aspects such as Savings, Investments, Credit, Insurance and Pension at a single place. IFE Academy periodically publishes Investor Educational materials and distributes it to general public.



Investors Financial Education Academy

Regd. office : Park View, Basement, 85/ 17, G.N.Chetty Road, T.Nagar, Chennai - 600 017.
email : bulletin@ifea.in www.ifea.in