



इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

Beware of Online frauds

- No bank asks your credit/debit/aadhaar card number, CVV number/PIN/OTP. If anybody asks for it through phone/mail, beware it is fraud. Don't part with the details at any cost.
- Fraudster may ask your credit/debit card details in guise of adding Aadhaar number to release blocked card/ to redeem reward points and for other reasons, what so ever it is, DO NOT DIVULGE THE DETAILS.
- Do not believe any SMS/mail announcing that you are the winner of huge prize money. No such prize is being conducted. The SMS/mail is to cheat you.
- Do not follow any links received through unknown persons to access online transactions, fraudsters may fool you steal information. Always use HTTPS links for online transactions.
- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Destroy the ATM pin number during transaction.
- Please change your ATM PIN regular basis.
- Keep your credit card receipts and check your receipts against your monthly statement. And periodically review account statements to guard against transaction frauds and raise dispute on any unauthorized charges or withdrawals immediately.
- Only carry around credit cards that you absolutely need.
- Shred anything that contains your credit card number written on it. (bills)
- Notify change of your address to your credit card issuers in whenever you change address.
- If you lose your credit card, please report the loss immediately to your Bank and block the card.
- When you dispose a card at the time of renewal/up-gradation, please make sure to cut it diagonally before disposal.
- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.

- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added.
- Don't give away your personal information in the survey forms given in restaurants/shopping malls.
- Always use secure websites for transaction and shopping.
- Please look for signs of security.
Identify security clues such as a lock image at the bottom of your browser,
A URL that begins with https:
(These signs indicate that your purchases are secured with encryption to protect your account information)
- Always shop with merchants/E-commerce Websites you know and trusts.
- Always log off from any website after completing online transaction with your Credit / debit card and delete the browser cookies.
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages asking for personal information including financial information, as banks do not ask for such information.
- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not fully protect from being read by outside parties.
- Please be careful when providing personal information online.
- Please be wary of promotional scams. Identity thieves may use phony offers asking for your personal information.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from outside parties the same way you protect your ATM PIN.
- Always make sure to use the virtual keyboard for net banking.