Safety & Security Tips

1. Security measures adopted by IDBI Bank

IDBI Bank has a strong online security policy to ensure our customers have a safe and secure online experience with us.

- We have 256 bit Secure Sockets Layer (SSL) encryption technology to secure all your online transactions.
- You can check the Security Certificate by clicking on the padlock icon that appears with the URL in the browser bar when you type the URL.
- The Bank insists that customers set a strong password for online banking. We also indicate how strong or weak your password is basis the character combination you opt for i.e. combination of Alphabets in small case & caps, Numerals and Special characters. Last few passwords are disallowed by the system while re-setting the password.
- All online transactions are verified through One Time Password (OTP) which is sent on registered mobile number to the customer.
- The IDBI Bank Credit Card account gets automatically blocked on typing the password incorrectly 3 times in succession.
- The IDBI Bank Credit Card account gets automatically logged off after a defined inactive period to prevent frauds.
- We ensure that only the last 4 digits of your Credit card no. are displayed in all our communication to you to avoid any frauds.

2. Safety Tips that customers should adopt

a. Safety Tips for the Card:

- Before signing or using your card, please read the 'Cardholders Agreement' to understand your card better and make the best use of it. Please refer to IDBI Bank website for more details.
- At the time of receiving your IDBI Card, make sure that the welcome kit is sealed. If not, call Customer Care immediately.
- Please remember your 16-digit card number and quote it in all your letters to us for identification
- Always keep a list of your credit cards, credit-card numbers and toll-free numbers handy, in case your card is stolen or lost.
- Your card has a magnetic strip with EMV chip so do not bend or expose your card to Electronic devices, gadgets or sunlight. Also make sure that you do not scratch your card's magnetic strip and the chip or expose it to magnets and/or magnetic fields such as handbag clasps, TV sets, speakers, etc.
- Do not courier your credit card along with the documents in case of cancellation

- Never give a photocopy of your card or statement to anybody.

b. Safety Tips for PIN & Password:

- Once you receive your PIN, memorize it and destroy it as soon as possible.
- When selecting the password, we recommend a password that ensures-
  - a minimum length of 8 characters
  - a minimum of 1 alpha numeric character [a-z]
  - a minimum of 2 numbers which must be embedded (i.e. the number cannot be the first or last character of the password)
  - no use of username or username in reverse
  - use of Special characters [@,-,_,Space,] and uppercase alpha characters [A-Z]
- Always choose your new PIN carefully, if you change your PIN.
- Always choose a “strong” password and change it regularly.
- Do not disclose your Personal identification Number (PIN) to anyone or store your PIN along with the credit card.
- When you use your card at an ATM, enter your PIN in such a way that no one can memorize your keystrokes.
- Do not allow anyone else to use your card, PIN, password or other security information.
- Do not store your password(s) in your mobile / browser.
- Always inform us of the disclosure or possible disclosure of your PIN or Password as soon as you are aware or suspect your PIN or Password has been disclosed. You should also change your Password / PIN as soon as you are aware or suspect that someone else knows them.
- Consider using a different PIN or Password for different cards.

c. Safety Tips for E-commerce/Online transactions:

- Always transact on trusted/ known E-commerce websites only.
- Ensure you register your mobile number with IDBI Bank so you can receive the One Time Password (OTP) for all your online transactions
- Check the site for Secure symbols like https:// or the padlock icon.
- Always type the URL of the site concerned in the browser bar and avoid accessing the site through links sent in e-mailers.
- Use a virtual keyboard if available for entering your personal information for transacting online. The virtual keyboard facility is uniquely designed to provide secured online transactions
- Do not use the same user name and password to log in social networking sites that you use to access your IDBI Bank Credit Card account

- Never share personal information such as: User ID, PIN, CVV, Credit Card number on any social media sites even with a friend.
- Never respond to emails, websites, phones that request your Credit Card details (Card number, PIN, Card expiry date, CVV number) & personal information
- The Bank never calls /send Emails to customers asking for card and other personal information. Do not share such confidential information even if the person pretends to be a Bank employee or any service provider representative.
- Ignore any e-mails / websites / Pop-ups on your computer screen offering good business opportunities with enormous income potential by working from home
- Ignore all phishing e-mails asking your card details to transfer funds / lottery prize etc. in your card
- Beware of all websites asking your card details for Free Registration or to verify your Age.
- For further details on Do's and Don'ts of Banking and Phishing please refer the following URL http://www.idbi.com/Dos-Donts-Banking.asp and http://www.idbi.com/phishing.asp.

d. Safety Tips for Point of Sale (POS) transactions:

- Shield your PIN from onlookers by Covering the Keypad of Point of Sale (POS) terminal or ATM while entering the PIN.
- Make certain you get your card back after you make a purchase (one good habit to observe is to leave your wallet open in your hand until you have the card back). Also, make sure that you personally rip up any voided or cancelled charge slips.
- Even when you place the call to a legitimate merchant, never give out your card number over phone.
- Check all details and the total on charge slip before signing it. Draw a line through blank spaces on charge slips above the total to prevent any changes in the amount.

e. Safety Tips for your Computer

It is important to secure your personal computer/laptop properly, otherwise you, your family and friends might be at risk of online frauds.

- Always back-up your data periodically so that you recover your information if a virus destroys your files, or your computer is stolen or damaged.
- Install and regularly update anti-virus and anti-spyware software. You may also consider installing a firewall.
- Activate automatic updates so that your anti-virus receives the latest fixes and can detect any new threats.

- Do not leave your computer unattended in any public place. Always secure your laptop/computer with a password.

f. Safety Tips for Mobile Security

- Put a password on your mobile device. Check the security settings on your phone to put a Security PIN on your SIM Card Setup so that your device locks automatically
- Install security software from a reputable provider. Access and download from reputable websites and mobile applications (Apps) only.
- Be careful before allowing access to third party unsigned applications to your personal information.
- Check your bill at regular intervals for unusual data charges or premium call rates.
- Check for updates to your device's operating system regularly.
- Be smart with Wi-Fi and Bluetooth – try to use an encrypted network that requires a password, and avoid online banking or financial transactions in busy public areas.
- If you recycle your device, make sure you delete all your personal information first.

g. Safety Tips for Alerts

- Check your monthly statement regularly to make sure that all charges are your own and correct, if not notify the Bank of any errors or unauthorized charges immediately.
- Keep your mobile number/Email id/Address updated with the Bank to get transaction alerts/account statement or any other communication from Bank
- If you receive any transaction alert through SMS/Email or observe any debit entry in your account statement which is not executed by you, immediately call Customer Care for details and/or to Hotlist/Block your card/internet banking.
- Immediately call customer care at numbers provided to Hotlist/Block your card, in case it is Lost/Stolen or is captured by any other bank ATM.

h. Safety Tips for Collection Practices

- Please check the identity card of the collection agent before making a payment to him.
- Please ask for a customer receipt copy from any collection agent for a payment done towards your credit card.
- Do not issue signed blank cheques towards your credit card payment to any person who claims to represent the Bank

2. Customer Knowledge Centre

- RBI's Financial Education Initiative (link- http://www.rbi.org.in/financialeducation/home.aspx)
- Visa Risk Initiatives (link http://www.visa.co.in/personal/security/riskinitiative.shtml)

3. Contact Us

- If you suspect fraudulent activity in your account call our IDBI Cards Customer Care on 1800 425 7600 (Toll Free) or 4042 6013 (Non-Toll Free) immediately. You can also report such incidents at idbicards@idbi.co.in
- To update your email id or mobile number, please contact our helpline.