Please note the following points which would help you transact over the internet in a more secure environment.

Never respond to emails that request personal information.
At IDBI Bank Ltd., we would never ask for updation / activation of your personal details through an email. Nor would we ask for your password through any means, online or offline. If any of our bank personnel asks you for your password, do not disclose it and report him or her immediately to us.

Keep your password top secret and change them often.
Changing passwords often helps in protecting your account even if inadvertently you may have disclosed it to someone.

Never use cyber cafes to access your online accounts.
PCs at cyber cafes may be infested with viruses and Trojans that can capture and transmit your personal data to fraudsters. Beware of typing passwords on unknown PCs. If you do, ensure to change your password at the earliest using your own PC at your workplace or at home

Use the Virtual KeyPad.
Please remember to always use the facility of the Virtual KeyPad, provided on the login page while logging on to your account from an unknown PC or from a cyber café.

Keep your computer secure.
Please ensure that anti-virus software is installed on your PC and regularly updated. It is also prudent to install a firewall on your PC to prevent any unauthorised control and access to data on your PC while surfing the internet.

Check the website you are visiting is secure.
Before submitting your bank details or other sensitive information the following checks will help ensure that the site uses encryption to protect your personal data: If the address bar is visible, the URL should start with 'https://' ('s' stands for secured) rather that the usual 'http://'. Please note that the fact that website is using encryption doesn't necessarily mean that the same is legitimate. It only tells you that data is being sent in encrypted form.

Following the above steps would help you transact over the net in the most secure environment. We reiterate the following simple precautionary measures:

- **Never let anyone know your PINs or passwords, do not write them down.**

- **Do not use the same password for all your online accounts.**

- **Avoid opening or replying to spam emails,even if purportedly sent by the**

Bank.

- **In case of suspicion, report the matter immediately to us on our toll free 24 hour customer care numbers or email us at**

- **Look for the padlock symbol on the bottom bar of the browser to ensure that the site is running in secure mode.**

- **Disable the "Auto Complete" function on your browser to prevent your browser from remembering Passwords.**

- **Always logout to terminate your session, instead of closing the browser directly.**

- **Always type the address of the bank website in the address bar of your browser or access it from your stored list of favourites. Do not access the bank website through a link in an email or through another website.**

- **Using special characters like # $ @ etc. in your password is highly recommended.**

Caution :

If you receive an e-mail claiming to be from IDBI Bank Ltd. regarding updating sensitive account information or asking for verifying your identity or login to your account for instant activation etc. by clicking on a link provided within the email, DO NOT act on the mail and delete such mails from your mailbox. Please also let us know by forwarding the e-mail to customercare@idbi.co.in or call on our toll free Phone Banking numbers.