ATM Safety Measures

Confidentiality of PIN is utmost necessity. Neither write your PIN anywhere nor disclose to anybody howsoever close he may be to you. Always memorize the PIN.

Change your ATM PIN frequently.

Stand close to the ATM machine while using ATM so that no one can peep at your PIN as you enter it.

Taking help from strangers for using the ATM should be avoided.

Press the 'Cancel' key and take your card back before moving away from the ATM.

Transaction slip should be destroyed if of no future use.

Try avoiding using ATM which are situated in isolated location.

On loss of ATM card, report immediately to branch as well as toll free phone number for blocking the same. The toll free phone number (1800220096) is available to each ATM site.

In case ATM card get stuck in the ATM, contact the bank immediately.

Be wary of anything about the ATM machine that looks out of the ordinary, such as odd looking equipments or wire attached to the device mainly near ATM card slot.

One should check their Bank A/c regularly to make sure that there is no unusual/ unauthorized transaction.

If you see anything unusual or suspicious around an ATM or if you find unauthorized ATM transaction on your Bank account, immediately contact your home branch/ local law enforcement agency.

Update your current mobile phone number and E-Mail address with your Branch for getting SMS alert on Credit/Debit to your account and E-Mail alert for other communications.

Internet Banking Safety Measures

Every Internet Banking user has been provided with User ID and Login Password. These three items enable a user to login to Internet Banking. So, these should be very confidential to the customer/user and should never be disclosed to anybody even a person claiming from The Mahanagar co-op. Bank ltd.

It is customer/user responsibility not to disclose User ID & Login Password . So, it is always better to keep password complex, a mix of alphanumeric & special character, so that it is difficult to guess by others.

Always maintain different login and passwords so that compromise of password becomes difficult.

Change your Internet Banking passwords regularly so that there is less chances of guessing of the same by others.

Never click a hyperlink in your email or any link on any website which directs you to login to Mahanagar Bank Internet Banking website. Most of these links are fictitious which leads to fake website and aims to get User ID and Password of the customer so that unauthorised access is made to Internet Banking for siphoning-off money.

Always type the address of the website in the address bar of the browser or access it from stored list of favourites.

Do not access any website such as bank website through a link in an email or through

another website.
Always ensure before entering user ID and password that you have accessed https://www.mahanagarbank.co.in for Internet Banking service. The website can also be accessed through Internet Banking link in Mahangar Bank websites www.mahanagarbank.com Beware from phishing websites wherein pages looks same as in the bank's original website but website addresses are different.
Avoid accessing your Internet Banking account from a cyber cafe or a public computer as there is risk that some hidden applications (Spyware like Keyloggers) installed on such computer may be capturing your user ID and passwords. Preferably use virtual keypad for entering password.

). Every time you login to Internet Banking, check the date and time of last login to ensure that it is you who logged-in that time. In case of any doubt of somebody else having access your account, first change the login passwords and verify your transactions. In case of any discrepancies, inform the branch.

. The past login details and navigation within the menu can be checked through history option.

. Every time you complete your online banking transaction, logoff through logout option rather than just closing your web browser, because in such instance, session remains valid even after closing the web browser.

. Always track your account activity by checking your balances and statements online for any unauthorized transaction.

. Clear all browsing history (temporary files, cookies, etc) before leaving the system. Also close the browser after proper logout.

. Always update your correct and current mobile number with the branch to get SMS alert for your online transactions. If you are not getting SMS alerts about your transactions in the account, contact your home branch for updation of your mobile number in the bank's system to receive the SMS.

. Always access Internet Banking through latest version of browsers like Internet Explorer 7.0 & above, Firefox 3.6.3 & above, etc as URL turns green to indicate that you are accessing safe Mahanagar Bank Internet Banking site.

. Disable the "Auto Complete" function in browser to increase the security of your information.

. Before entering User-ID and Password check whether the url in the browser starts with "https://" and a padlock icon at the right bottom corner of the browser.

). You can also verify the genuineness of internet banking website by entering CIF number and Date of Birth in the option "Is this a Valid site?" and therefore, a phishing website can easily be detected if you do not get correct personal details.

). In case of any problem you may write to support@mahangarbank.com and contact your home branch without delay.

Mobile Banking Safety Measures

1. Always keep Application password, MPIN, TPIN and User ID confidential to yourself. Do not save these in mobile phone or write on paper.
2. Regularly change Application password, MPIN and TPIN so that it becomes difficult to compromise.

3. Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone.
4. Do not allow any unknown person to have access to your handset/mobile phone or leave the same unattended while using Mobile Banking Services.
5. If the mobile phone or SIM is lost, then immediately take action to de-register from mobile banking from home branch i.e. from where Mobile Banking facility has been availed.
6. You should de-register for Mobile Banking application if you do not want not to avail the facility any more.
7. Ensure that you receive SMS alerts for all debit/credit to your account. In case of not receiving the SMS alerts, please contact home branch.
8. If the mobile handset is given for repair, ensure that no confidential data pertaining to mobile banking is left in the phone.
9. Note the IMEI (International Mobile Equipment Identity) code of your cell phone and keep it in a safe place. This helps the owner to get stolen mobile blocked for further use through mobile operator.
10. Chain and junk messages should be deleted regularly.
11. In case of any problem you may write to itsupport@mahangarbank.com

Phishing

Phishing is a criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit/debit card details by masking as a trustworthy entity in an electronic communication. It is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy source. Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims.

TIPS TO PREVENT PHISHING ATTACK

1. Never respond to emails that request personal information like user ID, password, etc.
2. Keep your password top secret and change them often.
3. Avoid using cyber cafes to access online accounts. If access is required, preferably use virtual keypad for entering password.
4. Keep your computer secure by ensuring that an latest and updated antivirus software is installed.
5. It is preferable to install/ enable the personal firewall on the PC from which online account is being accessed to prevent any unauthorized access to data while surfing internet.
6. Ensure that you are visiting secure website before submitting any sensitive information.
7. Please note that Allahabad Bank never asks for any kind of your credentials.
8. Do not use the same password for all online accounts
9. Avoid opening or replying to spam emails.

10. If the browser is of latest version (Internet Explorer 7.0 & above, Firefox 3.6.3 & above, etc), observe that the address bar turns green after entering bank's Internet Banking website address in the address bar, which indicates that the site is authenticate & trustworthy and online transaction can be done in good faith.
11. Look for the padlock symbol on the bottom bar of the browser to ensure that the site is running in secure mode.
12. Disable the "Auto Complete" function on the browser to prevent browser from remembering details entered.
13. Always logout to terminate the session, instead of closing the browser directly.
14. Always type the address of the website in the address bar of the browser or access it from stored list in favorites.
15. Do not access Bank's website through a link in an email or through another website.
16. Using special character like # $ @ etc in the password is highly recommended.

Mobile Banking Safety Measures

- Always keep Application password, MPIN, TPIN and User ID confidential to yourself. Do not save these in mobile phone or write on paper.

- Regularly change Application password, MPIN and TPIN so that it becomes difficult to compromise.

- Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone.

- Do not allow any unknown person to have access to your handset/mobile phone or leave the same unattended while using Mobile Banking Services.

- If the mobile phone or SIM is lost, then immediately take action to de-register from mobile banking from home branch i.e. from where Mobile Banking facility has been availed.

- You should de-register for Mobile Banking application if you do not want not to avail the facility any more.

- Ensure that you receive SMS alerts for all debit/credit to your account. In case of not receiving the SMS alerts, please contact home branch.

- If the mobile handset is given for repair, ensure that no confidential data pertaining to mobile banking is left in the phone.

- Note the IMEI (International Mobile Equipment Identity) code of your cell phone and keep it in a safe place. This helps the owner to get stolen mobile blocked for further use through mobile operator.

- Chain and junk messages should be deleted regularly.

- In case of any problem you may write to customercare@allahabadbank.in.

- Customers may visit mobile banking portal for

a. application download
b. view transaction history
c. change pin
d. Information about mobile banking.