Important Security Notice

Use Internet Banking To Minimize The Risk of Fraud. MBBL Stands for Mahalaxmi Bikash Bank Limited.

1. Utilize paperless options. Restrict receipt of paper statements by subscribing to e-mailed bank account statements.
2. Monitor your account activity regularly by checking your balances and statements online through www.yetibank.com.This helps you to detect fraudulent transactions, if any, quickly. The earlier a fraud is detected, the lesser will be its financial impact.
3. Link and manage all your YDBL Bank relationships online at yetibank.com
4. YDBL does not ask you for any personal information other than your user ID and password when you log in www.mahalaxmibank.com
5. YDBL 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 and forward the e-mail to it@mahalaxmi.com.np
6. Be cautious about any unsolicited offers or opportunities offering you the chance to make some easy money. These adverts will normally state that they are an overseas company seeking "representatives" or "agents" to act on their behalf for a period of time, sometimes to avoid high charges for making payments, or local taxes

Tips For Use When Banking Through The Internet

1. Check the webpage's URL. When browsing the web, the URLs (web page addresses) begin with the letters "http". However, over a secure connection, the address displayed should begin with "https" - note the "s" at the end. For example: Our home page address is www.mahalaxmibank.com. Here the URL begins with "http" meaning this page is not secure and there is no account or personal information stored or asked. Click the tab under "Login". The URL now begins with "https", meaning the user name and password typed in will be encrypted before being sent to our server.
2. Avoid accessing your Internet Banking account from a cyber cafe or a shared computer. However, if you happen to do so change your passwords from your own computer.
3. Every time you complete your online banking session, log off from yetibank.com. Do not just close your browser.
4. To access YDBL Bank's Internet Banking, always type in the correct URL (www.mahalaxmibank.com) into your browser window. Never click a link that offers to take you to our website.
5. If your log-in IDs or passwords appear automatically on the sign-in page of a secure website, you should disable the "Auto Complete" function to increase the security of your information.
   To disable the "Auto Complete" function:
   1. Open Internet Explorer and click "Tools" > "Internet Options" > "Content".
   2. Under "Personal Information", click "Auto Complete".
   3. Uncheck "User names and passwords on forms" and click "Clear Passwords".
   4. Click "OK".
6. Change your Internet Banking passwords (both log-in password and transaction password) after your first log-in, and thereafter regularly (at least once in a month).
7. Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !,@, #,$, %, ^, &,* (,)] in your passwords.
8. For additional security to financial transactions through Internet Banking, create and maintain different passwords for log-in and for transactions.

9. If you have more than one Account, you need not to register a different user and password for each of the Accounts. You may also view all your accounts with Yeti Bank under a single user ID by linking your various accounts to your preferred Internet Banking user ID.
10. Never share your Internet Banking passwords with others, even family members. Do not reveal them to anybody, not even to Yeti Development Bank's employee.

Contact Us

1. If you forget your password
2. If you are unable to log in to your Internet Banking account.
3. If you notice any suspicious activity on your account.