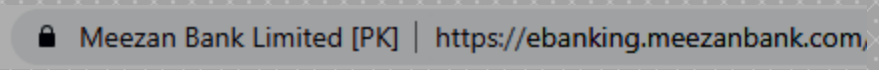
SECURITY USER GUIDE

- ***Remember you can access MBL internet banking by typing https://ebanking.meezanbank.com/.***

- ***Always look for GREEN BAR in your browser which ensures that the website you are accessing is genuine and secure.***



- ***Please beware of fraudulent emails and websites that attempt to obtain your banking information.***

Example of email scam - Important Information for Employers - Employer Bulletin Issue 45

From: HMRC Employer Alerts & Registrations [mailto:employers@alerts.hmrc.gov.uk]
Sent:
To:
Subject: Important Information for Employers

Employer Bulletin Issue 45 out now

The latest version of the Employer Bulletin issue 45 has just been published.
This edition contains the latest information about filing your PAYE information in real time.

To find out more open the attached document(s)

Your next employer email alert is scheduled for February 2014

**** Please do not respond to this email*

If you have any concerns regarding the validity of this or any emails received from HMRC go to our Online Security pages

➢*Always choose a strong password and change it regularly.*
Never share your password with anyone.

➢*Keep your browser up to date to ensure your browser security.*

➢*Check your account statement and balance regularly. In case of fraudulent transactions contact Phone Banking immediately for support.*
In case of any suspicious activity, change your password instantly.

Security Guide

As use of the Internet continues to expand, more banks and thrifts are using the Web to offer products and services or otherwise enhance communications with consumers.

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct banking business, any day, any time. However, safe banking online involves making good choices - decisions that will help you avoid costly surprises or even scams.

This guide offers information and tips to help you if you are thinking about or already using Meezan Internet banking service.

You must read the guidelines in provided in this document and take the necessary precautions while using Meezan Bank Internet Banking Service.

Security Overview

- ***Meezan Bank uses a very high level of encryption to protect your transactions and Accounts from unauthorized access. This includes security in terms of hardware and software at our end such as Firewalls, SSL certificates and other security software. Meezan Bank also uses 3D secure service to mitigate frauds.***

- ***Make sure that "LOCK" occurs in the browser bar without any warning on the login page***

- ***User ID and Password Security***

- ***Access to Meezan Bank Internet Banking Service is based on a User ID, password and a security image. This User ID, password and security image is chosen by you at the time of registration. You must keep them secure and take steps to prevent unauthorized use of them. You must not tell or disclose them to another person or allow them to be seen by another person (including family or friends). You must not keep a record of them in a way which they can be determined by another person. You must not record them together. You must not select a Password, which represents your birth date or a recognizable part of your name.***

MEEZAN BANK may from time to time provide guidelines for ensuring the security of a Password or User ID. The guidelines will provide examples only of security measures and will not determine your liability for any unauthorized Instruction on your Account. Make sure that you are typing your UserID, password and security image on the correct Meezan Internet Banking login page provided for this service. Customers are advised to change the Password frequently

PIN Based Security
All financials transactions are secured by a 4-digit One Time PIN. You have to enter this PIN whenever you will try to transfer funds or pay bills. You can always change your PIN from with-in the Meezan Bank Internet Banking website.

Security Tips

Login Information

Do not disclose your User ID, password and security image to any one including your friends, relatives or Meezan Bank Employees.

Try to keep changing your password regularly and frequently.

Change your password immediately when you think somebody has guessed or seen it and report the incident to our Phone Banking on (+92 21 111 331 331, +92 21 111 331 332).

Inform us in case there is an incident.

Do not share the email address used in Meezan Bank Internet Banking service, as it is used to reset the PIN or password for your account.

Web Browser

Make sure that you are typing your User Id/CNIC and password on the correct Meezan Bank Internet Banking login page provided for this service.

Never store your login information on the browser.

Always use the "LOGOUT" option to safely exit from Meezan Bank Internet Banking.

Computer & Software
Always update to recent version of the operating system.

Install the latest version on Antivirus

Do not use Meezan Bank Internet Banking from a shared PC such as Net-Cafe's etc.

Fraudulent Websites and Emails

Protect yourself from fraudulent websites and emails. For example, watch out for copycat Web sites that deliberately use our or Web address very similar to, but not the same as meezanbank.com. The intent is to lure you into clicking onto their Web site and giving your personal information, such as your User ID/CNIC and password.

Always check to see that you have typed the correct Web site address before conducting a transaction.

People are usually misled by fraudulent emails, which give an impression that email was sent out from us thus causing compromise on your security information.