

Dubai Islamic Bank Pakistan Limited – Guidelines for Customer Using Internet Banking

Passwords

- Never share your Passwords; they act like a key to your Internet Banking account, where its sharing means that offenders can also access your online account.
- Make your Password as impersonal as possible; it should be unique to you. Do not use your Date of Birth, Phone Number or your Identity Card Number as your password. Offenders can access this information or decide to try it out as observing your behavior towards password-keeping.
- Do not store password in Text-File, or write it down on any piece of paper.

Encryption



- Encryption is the process of protecting your private information from unauthorized access.
- DIBPL use encrypted channel while conducting internet banking services, most internet browsers display a small icon on your screen that looks like a “lock” or a “key” when you conduct secure online transactions.
- Make sure that your registered email address also has the same encryption practices.
- Do not keep Internet Banking correspondences in your Registered Email Inbox for longer period.
- In case you doubt that your Registered Email has been hacked or used by someone else, act promptly to secure your Internet Banking User ID and contact 24/7 Phone Banking.

Beware of Spam Email

- Offenders may send you email asking for your personal information such as a User ID, Password or TPIN.
- DIBPL Internet Banking never communicates with customers via such emails and asks such kind of confidential information.
- The email message contain links with URL written as of dibpak.com, however when you click on these links they take you to their own websites link.
- With the passage of time, the bad guys are getting smarter and smarter. They Designed fake DIBPL logos and use them when sending you an email and create exact replica of DIBPL website, where you may be easily lured to give personal information.
- These emails are easily detectible because their emails usually direct you to questionable internet sites, they do not address you as you are used to being called by DIBPL. The emails may also contain poor grammar.

Keep an Eye on potential Malware and Spywares

- Various Companies track your web browsing habits to understand your interests and then to market particular services or promotions. To track such information Malwares and Spywares are installed by accessing these sites or clicking on promotional links.
- Make sure that you do not use DIBPL Internet Banking while accessing other sites at a time.
- When using Internet Banking, close all browser windows other than it. Perform necessary transaction and close the Internet Banking. DIBPL Internet Banking asks to close the browser window, always click 'OK' on it.
- Clear internet cache, before and after accessing DIBPL Internet Banking. For details on how to do it, look into your Internet Browser Help.



General Security & Use Anti-Virus Protection Softwares

- You should get the best quality anti-virus protection installed on PC or handheld device, where you intend to use DIBPL Internet Banking.
- They protect your personal information in your PC or handheld from being lost due to a virus. Search for the services of a computer expert to enable you to get the top rated services available.

Avoid using Public Computers or Wi-Fi Hotspots

- Do not access DIBPL Internet Banking at Shared or a Public facility computer, like we have at Airports, Hotels, and Shopping Malls etc.
- Similarly, never use Public Wi-Fi Hotspots for Internet Banking, until and unless you could trust the service provider. They are mostly unsecured and offer free connectivity to conduct malicious activities.

Report our 24/7 Phone Banking

If you encounter difficulty accessing your account after you have entered your credentials or see unfamiliar banking email messages such as "Security verification Required" or " Customer Support Team", contact us immediately via our 24/7 Phone Assistance at 111-786-342.

Disclaimer

Dubai Islamic Bank Pakistan Limited is not responsible if customers do not comply with above security guidelines