Dubai Islamic Bank بنك دبي الإسلامي

DIBPL CYBER SECURITY SAFETY TIPS

INTRODUCTION

We understand that Online/Mobile banking is a very convenient facility for our valued customers.

To ensure your data is protected, we have deployed all the necessary controls to provide secure and safe transactions.

We also understand that connivance matters and to place excessive protection would only cause inconvenience to our most important asset, meaning you! In light of this, we request that you must protect your password and other login details to prevent criminals from accessing your account(s). Because of the sums of money and frequent transactions involved, online/mobile banking has become a favorite target for fraudsters and criminals.

To help you avoid being a target of such notorious individual, we request you to follow the underline guideline issued for your protection and convenience.
Let us emphasize that following these common security practices will protect you from cyber criminals and help you use our services without any delay.

MOBILE DEVICES PROTECTION

Consider opting for automatic updates for your device's operating system and "apps" (applications) when they become available to help reduce your vulnerability to software problems.

Never leave your mobile device unattended and use a password or other security feature to restrict access in case your device is lost or stolen. Make sure you enable the "time-out" or "auto-lock" feature that secures your mobile device when it is left unused for a certain period of time. Only download official "DIBPAK Mobile" application from App Store/ Play Store

PROTECT YOUR COMPUTER

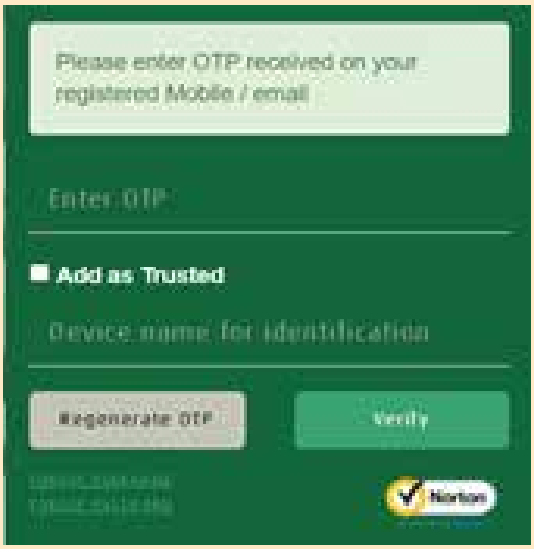
Install software that protects against malware, or malicious software, which can access a computer system without your consent to steal passwords or account numbers. Also, use a firewall program to prevent unauthorized access to your PC. While protection options vary, make sure the settings allow for automatic updates

STRONGEST AUTHENTICATION

Use the strongest authentication offered, especially for high-risk transactions.
Use passwords that are difficult to guess and keep them secret. Create a "strong" user ID and passwords for your computers, mobile devices, and online accounts by using combinations of upper- and lower-case letters, numbers, and symbols that are hard to guess and then change them regularly. Although using the same password or PIN

for several accounts can be tempting, doing so means a criminal who obtains one password or PIN can log in to other accounts.
However, for your own protection we have already configured our online banking with two factor authentication (2FA) sometime known as OTP.
We request you to ensure that your email and mobile number are always updated with the bank.

This can either be through call our call center on 111-786 -342 or visit one off our branches



PHISHING EMAILS

It's easy for cyber criminals to copy the logo of Dubai Islamic Bank into a phishing email. When responding to a simple request, you may be installing malware. Your safest strategy is to ignore unsolicited requests, no matter how legitimate or enticing they appear.

HOTSPOTS PROTECTION

Only access the Internet for banking or for other activities that involve personal information using your own laptop or mobile device through a known, trusted, and secure connection. A public computer, such as at a hotel business center or public library, and free Wi-Fi Networks are not necessarily secure. It can be relatively easy for cyber criminals to intercept the Internet traffic in these locations.

SOCIAL MEDIA

Cyber criminals use social networking sites to gather details about individuals, such as their place or date of birth, a pet's name, their mother's maiden name, and other information that can help them figure out passwords - or how to reset them. Don't share your 'page' or access to your information with anyone you don't know and trust. Cyber criminals may pretend to be your 'friend' to convince you to send money or divulge personal information.

SECURE ONLINE CONNECTIONS

You can have greater confidence that a website is authentic and that it encrypts (scrambles) your information during transmission if the web-address starts with "https://." Also, ensure that you are logged out of financial accounts when you complete your transactions or walk away from the computer.

Dubai Islamic Bank بنك دبي الإسلامي

LASTLY ... ALWAYS SECURE YOUR PASSWORD

- Never share your Passwords; they act like a key to your Internet/Mobile 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

We will never ask you for your authentication (like Passwords, TPIN's) details via Email / SMS or through telephone banking.
We will never send out Email / SMS message containing links with URL. Always type the DIBPL URL in the browser yourself

DIBPL Internet Banking never communicates with customers via such emails and asks such kind of confidential information

Phone Assistance:
111-786-DIB (342

Website:
www.dibpak.com

Address:
Head Office, Hassan Chambers, DC-7, Block- 7, Kehkashan
Clifton, Karachi. Pakistan.