What we do

- Our online banking system is designed to protect your information and privacy. Here are some of the security measures we have in place.

Strong Encryption

- Information exchanged between your computer and our web server is secured through encryption. Encryption converts the information into a form that is unreadable as it travels along the internet. You must have a browser that supports strong encryption to access the system (in technical terms, the browser must support 128-bit encryption).

Password Protection

- To protect your password, our system will periodically request that you change your password. When changing your password, you will be shown whether your password is considered weak, medium or strong. Strong passwords are harder for a fraudster to guess. Please do not reveal your password to anyone and please commit your password to memory rather than writing it down where others may find it.

Automatic Logout

- You should always log out of the online banking facility when you are done, but if you forget, our system will automatically log you out after a period of time.

Protecting your Privacy

- In order to protect your personal information, you may be asked to enter security credentials before gaining access to pages that contain your address, phone number, and login credentials. Providing these credentials will confirm your identity so that only you can see and modify your personal information.

Fraud Protection

- In order to protect you against fraudulent transactions, you may be asked to enter security credentials for any transaction that moves funds out of the bank (for example, a transfer to an external account or a bill payment).

What you can do

- Always keep your virus protection software up-to-date. This will help protect you against programs that attempt to install themselves onto your computer hoping to capture personal information. Anti-spyware protection is also recommended to prevent against malicious programs.
- Always keep your computer's operating system up-to-date. Check regularly for the availability of security-related patches.
- Always verify the bank's web site name in your browser. In Internet Explorer, look at the Address and in Netscape Navigator, look at the location in the Navigation Toolbar.
- Never send e-mail that contains your personal information. This may include your address, account numbers, credit card numbers, and login credentials. E-

mail is not encrypted and can be intercepted. To send us confidential information, log into your online banking account and use our Secure Message service.

- Never respond to an e-mail that asks you to click on a link to connect to the bank. These e-mails are scams (called "phishing" scams). We will never send you e-mail or call you asking you to provide us with personal information.
- Whenever in suspicion of a spoofed, phished or fraudulent email that bares the address of Bank of Beirut please do not hesitate to send the email to bobdirect@bankofbeirut.com.lb or contact our contact center on 80071982 (from Oman) and on +961 5 955262 from abroad.
- Avoid using software features that remember your password. These features provide convenience but can reveal your password to someone else using your machine.
- Avoid doing your banking from a public computer (for example, a library, cafe, or airline lounge).