Our Commitment to Information Security

Bank of Beirut is working towards providing greater access to information and more electronic banking services to customers. As these capabilities increase, information security becomes an even more important issue.
The staff and management at Bank of Beirut have pledged to take all necessary precautions to safeguard your confidential information, and to give you guidance on how you can protect yourself against ID theft, electronic fraud, and other common threats encountered by today's banking customers, **however your awareness and assistance are key in helping us secure your information**. This pamphlet provides general guidelines on protecting your information and assets.

Protecting Your Identity

- The bank will never ask you to provide the below by email or SMS:
  - Passwords
  - Account Numbers
  - Card Numbers
  - User Names
  - Secret answers
  - Any other confidential customer information
- Fraudulent emails may be designed to appear as though they originated by Bank of Beirut, therefore:
  - Do not respond to any email communications which request any type of personal or confidential information,
  - Do not click on any links listed on such emails unless you are sure you are accessing Bank of Beirut official site.
  - Never give out any information that the Bank already has to a caller, text messenger, or email sender. We will never contact you and ask for your debit card number or account details we already have them.
- If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves.
- We work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible.
- We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.
- Report lost or stolen checks or credit cards immediately.
- Never give out any personal information to anyone whose identity you can't verify, if at all.
- Shred any documents you don't need any more that contain personal information, like bank statements, unused checks, deposit slips, credit card statements, and invoices.
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.

- Please report any suspicious calls, e-mails, or messages to the Bank of Beirut Contact Center, by calling 1262, or by e-mailing bobdirect@bankofbeirut.com.lb

Best Practices for Online Protection

- Maintain active & up-to-date anti-virus software
- Maintain spy-ware protection
- Set up automatic Windows (or other Operating System) updates
- Maintain firewall installed on the network or PC
- Internet cafes and public computer systems are discouraged especially when doing money transfers online or while communicating with the bank through web chat channel
- If you use a wireless network, it is suggested that you use password protection and encryption
- If your email is hacked or your phone is stolen directly change your online banking passwords.
- Block cookies on your Web browser. When you surf, hundreds of data points are being collected by blocking cookies, you'll prevent some of the data collection about you.
- Use multiple usernames and passwords. Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate.
- If you believe your Internet Banking User Name or Password or other means of access have been lost or stolen, or that someone has used them without your authorization, call us immediately at 1262, or by e-mail us at bobdirect@bankofbeirut.com.lb.

Secure Passwords

Since your password acts as a personal key, it provides access to your computer systems, emails and applications. It also gives each user certain permissions and capabilities. Therefore, you should select passwords to at least meet the following guidelines:

- Use strong passwords that contain a minimum of 9 alphanumeric characters (a mix of upper and lower case) including at least one special character.
- Changes passwords regularly least every 60 days with no repetition.
- Initial passwords provided to you by Bank of Beirut should be changed immediately upon receipt, this feature is already set by default for our online banking systems.
- Passwords should not be written down or recorded on-line in any form,
- Never share your passwords with anybody especially online banking passwords or user accounts.
- Don't use numbers that are tied to your personal information within the password such as date of birth, address, phone number, etc.
- Avoid using same password for all online services
- If you suspect that your password has been compromised, change it immediately

Debit & Credit Card Fraud

Debit cards and credit cards have become the most convenient form for purchasing our everyday needs. They have replaced the actual need to carry cash and should be treated like cash. With the ever-increasing volume of debit cards and credit cards so has fraud. Follow these steps to protect your cards:

- You should never lend your cards to anyone.
- Carry only the cards you use frequently.
- Never leave your wallet or purse in your vehicle.
- Safeguard your ATM access cards and PIN as you would checks and cash. Memorize your PIN – Don't write it on your card or in your checkbook.
- Tear up receipts, bank statements, and unused credit card offers before throwing them away
- Be aware of your surroundings when using an ATM, especially at night. Consider having someone accompany you to the ATM when you make transactions after dark.
- Consider using another machine or coming back later if you notice anything suspicious or feel uneasy.
- When using an ATM, stand squarely in front of the machine to keep your transaction as private as possible. Shield your PIN entry with your hand for greater privacy. When waiting to use an ATM, please respect the privacy of those using the machine.
- Consider canceling your transactions, pocketing your card and leaving if you notice anything suspicious while using an ATM.
- Protect the sensitive magnetic stripe on the back of your card. Keep it from direct sunlight. Avoid leaving your card on or near electrical appliances, such as a TV or stereo. Do not carry your card next to another card's stripe as they may demagnetize each other.
- Always take your receipt with you at the conclusion of every transaction to assure your financial privacy. Keep your receipts and use them to check your monthly statement.

Email Guidelines

- You should not e-mail confidential or other sensitive information. It is your responsibility to determine the confidentiality of each e-mail message you send. Assume that any message or information sent using the Internet is available to the public.
- You should not open e-mail that is of a questionable nature, such as an unusual attachment, a message from an unusual sender, or unexpected e-mail.
- Beware of Phishing emails always check the links sent in an email.
- Be careful while opening attachments and macros should be disabled if a dialog box appears.
- It is best to turn off Outlook's Auto Preview and Preview Pane features should be turned off.

- Never put anything in an e-mail message that you would not want to be seen by others.
- Be selective when using Reply and Reply to all.
- When mailing to multiple recipients, consider adding recipients to BCC instead of the To field.
- Be careful when addressing e-mail – know whom you are sending to.