Security

How does National Bank of Abu Dhabi protect my information?

National Bank of Abu Dhabi PJSC is committed to doing everything possible to secure customer information. Several measures have been taken to secure customer information over the Internet, one of which is the User Name and Password used to authenticate (login) to Internet Banking. We also use SSL technology to secure your personal information. More information on SSL technology can be found at:
http://wp.netscape.com/eng/ssl3/ssl-toc.html
Does National Bank of Abu Dhabi PJSC use pop-ups to solicit information?
As an added security measure, National Bank of Abu Dhabi PJSC will never use pop-ups to solicit personal information. If you encounter a pop-up from National Bank of Abu Dhabi PJSC asking for personal information, immediately contact National Bank of Abu Dhabi PJSC at 600 525500 or +97126818887.

What is email fraud?

There are many types of email fraud. An increasingly common type involves the use of phony emails that ask you to provide sensitive personal information that can be used for identity theft.

It is difficult to detect a fraudulent email because the address of the sender appears to be genuine (such as support@fgb.com), as do the graphics and page designs. These emails will often request personal information by luring you into providing it on the spot (e.g., by replying to the email) or by including links to a site that tries to get you to disclose personal data.

The people trying to extract this information may use it to access your accounts and withdraw money, or attempt to open new accounts using your information.

How do I know if I am using National Bank of Abu Dhabi PJSC site?

It is important not to rely on links provided in email messages to get to a Web site. Open a new browser window and type in the full address for the site you are trying to visit. For example, www.fgb.ae.

You can also tell that you're dealing with National Bank of Abu Dhabi PJSC because:

National Bank of Abu Dhabi PJSC will never send you an email asking for your passwords, credit card numbers, or other sensitive information.

How do I report a suspicious email?

If you believe you responded to or received a fraudulent email, immediately contact National Bank of Abu Dhabi PJSC at 600 525500 or +97126818887.

What can I do to protect my accounts and personal information?

National Bank of Abu Dhabi PJSC takes every precaution to keep your accounts and personal information secure. You can also take steps to maintain the security of your banking information.

- Remember that creating phony Web sites and sending bogus emails is easy to do. Be

cautious about the emails you reply to!

- Never click on a link in an email message that asks you to provide sensitive personal, financial or account information.
- If you are asked to update or verify personal or account information, call National Bank of Abu Dhabi PJSC directly.
- If asked for personal or account information in an email message, go directly to the National Bank of Abu Dhabi PJSC Web site. Open a new browser window, type in the Web Address (e.g. www.fgb.ae) and check to see if you must actually perform the task the email may be asking you to do. This may include things like changing your password or opting for electronic statements.
- Never give out your account information or passwords to anyone.
- If you are concerned that you responded to a fraudulent email or Web site, report the fraud to National Bank of Abu Dhabi PJSC immediately and change your passwords.
- Frequently monitor your account activity.
- Always sign off Web sites or secure areas of Web sites (for example, Internet Banking) for which you use an ID and password to enter.

When your computer is not in use, shut it down or disconnect it from the Internet.

What is SSL Protocol?

Secure Sockets Layer (SSL) is the leading security protocol on the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites including www.fgb.ae, use the protocol to obtain confidential user information. By convention, URLs that require an SSL connection start with https: instead of http:.

What is 128 bit encryption?

Encryption is a sophisticated scrambling method that is designed to prevent unauthorized eavesdropping on electronic data. Encryption works by taking a piece of information and processing it with a mathematical formula (called an "algorithm") that converts the information into a meaningless string of letters and numbers.

128-bit encryption refers to the size of the key used to encrypt the message. A longer key means the encryption is more random. Each extra bit in a key doubles the complexity of the key.