البنك العربي
ARAB BANK

1. Be Cautious When Using the Internet

- Browsing to unknown sites can increase the risk of becoming infected with viruses and other malicious code.
- Download files and install programs only when there is a real need and only from trusted sources.
- Never share personal or confidential information if you are uncertain of the recipient's identity or if you are uncertain that they need the information in question.
- Even when you are certain with whom you are dealing, never share sensitive information (like PINs, passwords) with anyone. In case you have a wireless internet connection, NEVER accept connections from neighboring unknown wireless networks

2. Be Aware of Phishing

- Phishing is a type of deception designed to obtain and use your personal data (such as credit card numbers, passwords, account data, etc.) for fraudulent purposes.
- Con artists might send thousands of fraudulent e-mail messages (or even SMS messages) that appear to come from Websites or sources you trust, like your bank or credit card Company, and request that you provide personal information via e-mail or on illegitimate Website created by them for this purpose.
- If you receive a suspicious e-mail or SMS message that appears to be from your bank please do the following:
  -Do not respond to the message, or click on any of the links, or change the e-mail in any way.
  -Contact us immediately.
- Only enter credit card and personal information when it involves a transaction you initiate and on Websites you trust.
- Regularly monitor your account activity to detect fraudulent transactions. If you want us to alert you whenever a transaction takes place on your account / Credit Card, you can register for our SMS Banking Service.
- Do not access your on-line Banking Services in open, public areas like Internet Cafes.
- If using cable modems or DSL for Internet access, do not keep the connection active when not in use; also consider installing personal firewall software.

3. Maintain Your Computer Security

- Review your computer's security periodically and apply appropriate repairs, upgrades, and replacements.
- Maintaining your computer is an important component in your security. One of the most effective ways of protecting your computer is to use an up-to-date anti-virus and anti-spyware products.

4. Know How to Respond to an Incident

- Learn how to recognize incidents and know what to do if things go wrong.
- Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately.
- If you don't know how to report an incident, call our Customer Contact Center or your closest branch directly.

5. Remember that Information Security is Everyone's Responsibility

- By protecting yourself and the systems you use, using them properly and with caution: You are protecting your money, your privacy, and your own data.

6. What is Social Engineering?

- The term «social engineering» refers to the art of manipulating people so as to circumvent security systems and conduct fraud.
- This technique involves obtaining information by telephone, email, fax, traditional mail or direct contact.
- As a countermeasure, use common sense and not release information that could be used to compromise your information.
- Regardless of the type of information requested, you are advised to:

[1] Find out about the other person's identity by asking him for precise information (last name, first name, department, telephone number, etc)

[2] Verify the information provided

[3] Ask yourself how critical the requested information is

7. E-Mail Spoofing

- Email "spoofing" is when an email message appears to have originated from one source when it actually was sent from another source.
- Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).
- Examples include email claiming to be from the Bank requesting customers to follow a link and enter their credit cards numbers or internet passwords or PINS.
- Note that while the Bank may request that you change your PINs / Passwords frequently, it will not specify what you should change it to or send you an email with a link requesting to change it.
- Also, legitimate financial institutions will never ask you to send them any critical information via email, phone, fax, postal mail, or any other means.

8. Understand Passwords and Authentication

- Passwords and other authentication methods like tokens are ways systems verify that you are who you claim to be.
- If someone else uses your login and password for example, the system will think it's you. That person can do anything you can do (such as initiating transactions).
- Don't share your passwords and access codes, don't store them in unencrypted files, and don't write them down unless you then place them in a locked, secured location.
- Passwords need to be strong and complex so they are not easily guessed or quickly cracked.
- Use complex passwords that are at least six characters long and have numbers, letters, and special characters in them.

9. Messaging Security - E-mail and Instant Messaging (IM) - Phishing Once Again

- E-mail and instant messaging are wonderful tools but they can be used or misused in a variety of ways.
- As a general rule, do not send confidential or sensitive information, like PIN numbers, account numbers, or secret information through unencrypted e-mail or IM.
- Do not open a message that is of a questionable nature, such as when it has an unusual attachment or it is from an unknown sender.
- Remember that e-mail is subject to forgery and spoofing so apply common sense before assuming a message is valid.
- Phishing is a special type of attack where the Phisher sends out a fake notice for example "The Bank is currently going through a scheduled data upgrade and customers are advised to login to their account and update their Account Preferences where failure to do such will result to the deactivation of Account". It will direct the customer to a false website to collect his\her account or credit cards information.