بنـــك أبـوظبــي الأول
FAB
First Abu Dhabi Bank

Security

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).

Secure Login

Our online banking system allows you to login with your credentials with the authentication of your RSA token.

Password Protection

To protect your password, our system will periodically request that you change your password. Strong passwords are harder for a fraudster to guess. Please do not reveal your password to anyone and 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 corporate information, you will be able to view only your address, phone number, and login credentials, but will not be able to edit the same. In order to update the same, you are requested to submit an official letter with the relevant update details at your Account Holding Branch or to your Relationship Manager.

Fraud Protection

In order to protect you against fraudulent transactions, you will be asked to enter security credentials for any transaction that moves funds inside or out of the bank.

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's address bar or window-header where the website name of the bank will be properly given without any other details appended to the same. Never send e-mails that contain your personal information. This includes your address, account numbers, credit card numbers as well as your login credentials since most e-mails are not encrypted and can be intercepted.

To send us confidential information, loginto your iBanking access and use our Contact Relationship Manager service under the Other Services tab.

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. Please contact us immediately at the following number if you receive such an e-mail or phone call.

Telephone number : 80076076 (Inside Oman) or +968 24761076 (Outside Oman)

Or Email : ibanking@bankfab.com

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).