ABK – Egypt Online Banking Security

ABK - Egypt realizes the importance of security in electronic services and has taken all necessary measures to ensure the maximum security possible, using the most advanced and modern methods. Rest assured that all information relating to your accounts is secured and classified.

Security Advisory

Dear Valued Customers,

Our Bank will never ask you for your login credentials or financial information over e-mail, even if it appears that the email was sent from our Bank.

1. Steps we have taken to safeguard your account

2. Steps you should take for your own security

1. Steps we have taken to safeguard your account

We realize the importance of security in electronic transactions and we have taken all necessary measures to ensure the maximum security possible, using the most advanced and modern methods. Rest assured that all information relating to your accounts is secured and classified.

The security of our Online Banking is achieved through the following methods:

•Client Identification through Security Access codes (User ID & password):

After signing your contract, you will receive your two security access codes, the User ID and password, to be used every time you log-in to our Online Banking.

During your first log-on, the system will ask you, for security reasons, to change the initial User ID and password you received from the Bank. You must change your password every two months (default option) or every time you request to issue a new password. In general, you can change your security access codes as often as you wish and we recommend that you do so frequently so as to reduce the chance that someone can obtain your codes and possibly access to your account.

Furthermore, in case you do not intend to use the Online Banking internet service for a long period in the immediate future, you can choose to deactivate your access codes. Whenever you will be ready to start using the e-banking services again, you can request to reactivate your access codes at your nearest Piraeus Bank branch.

• Privacy of Data Transfer through Encryption:

In order to ensure that all data is safely transferred, we use the SSL-128bit encryption protocol. This system has been implemented in conjunction with VeriSign, a company specializing in the security of transactions.

From the beginning of your connection to our Online Banking internet until the end (online session), all your data and personal information are encrypted with the SSL 128-bit encryption protocol. Encryption is actually a way to encode the information until it reaches a specific recipient, who will be able to decode this piece of information by means of an appropriate key. Every time that you are connecting to Online Banking, all the communication between your PC and the Bank's systems is encrypted through the use of a 128 bits key: every time you are sending information to the system, your browser first encrypts it through the 128-bits key and then sends them to the Bank's system. The Bank's system in its turn first decodes the information it receives by using the same key (as defined at the beginning of your on-line session) and then process it. The Bank's systems follow the same encryption process in order to send information to you.

•Firewalls:

Access to the Bank's servers is controlled by special firewalls, which allow to visiting customers access to particular services, while at the same time deny access to systems and databases with classified Bank data and information.

•Security of Personal Information (Bank Secrecy):

The very same policies regarding Bank Secrecy that apply in the traditional banking activities and transactions are also in place for the use of Online Banking, so as to guarantee the confidentiality and privacy of your data and transactions. All information sent by you to the Bank is highly confidential and we have taken all necessary measures to use this information only to the extent needed to provide e-banking services and execute the requested transactions. For your own safety, you should also treat all information communicated to you through our Online Banking as private and confidential and never disclose it to third parties.

•Session Time-out:

If the Online Banking internet remains idle for ten minutes, then the session is automatically terminated and you are logged off. You must log-in again if you want to resume using the service. In any case, we strongly advise you not to leave your computer unattended during your online session.

•Security Code Lock:

After a specific number of incorrect attempts to log-in, for your own safety the system locks your security codes and denies you access to the Online Banking. To unlock them, you must contact our Call Center at 19322 (in Egypt) or (+202) 3535 2790/91 (if calling from abroad) and

have your personal information authenticated. Keep in mind that the Call Center representatives, or any Bank employee for that matter, are not aware of your PIN and they cannot retrieve it for you. In case you do not remember it, you have to apply for a new PIN at your nearest branch.

•extraPIN code:

This is an optional one-time security password that enables you to use all advanced features requiring additional security. The extraPIN may be generated either through the extraPIN generator or sent as an SMS message to your mobile phone number upon your request.

2. Steps you should take for your own security

Here-below you can find some measures, by all means not exhaustive, but for sure a good start towards ensuring enhanced protection for your PC, for your private sensitive information and for your money.

•Protect your PC:

◦Install anti-virus software and keep it updated on a regular basis to guard against new viruses

◦Install anti-spyware security software against those programs that monitor, record and extract the personal information you type in your PC (passwords, card numbers, ID numbers, etc.)

◦Install personal firewalls to protect your PC against unauthorized access by hackers

◦Keep your operating system and internet browser up to date, checking for and downloading new versions/security enhancements from the vendor's web site

• Protect your personal information:

◦Create hard-to-guess security access codes (User ID & password) for Online Banking and make them unique (e.g. they should not be the same as those you use to access your e-mail account)

◦ Change your security access codes periodically

◦ Memorize your security access codes, avoid writing them down and keep them strictly personal and confidential

◦ Do not disclose to ANYONE your security access codes: The Bank will never initiate a contact with you to ask for your e-banking or ATM PINs, card or account numbers, personal identification information, neither over the phone nor in any electronic or written message

◦ Never leave your PC unattended when logged into the Online Banking

◦ Always remember to log off from your online session using the “Log-off” button when finished using the e-banking services

•Use the Internet cautiously:

◦Always access our Online Banking internet through our official website www.eahli.com

Never attempt to access the Online Banking internet through an external link of unknown or suspicious origin appearing on other websites, search engines or e-mails

◦Before logging in, check for the Bank's Security Certificate details and the various signs (e.g. green address line and padlock for those using browser Internet Explorer) that confirm you are visiting the secure pages of our Bank

◦ Ignore and delete immediately suspicious fraudulent (phishing, spoof, hoax) e-mails that appear to be from the Bank, asking you to urgently click a link to a fraudulent (spoof) website that tries to mimic the Bank’s site and to lure you into giving out your sensitive personal information (PIN, account or card numbers, personal identification information et al.)

◦Never click on a link contained in suspicious e-mails

◦Avoid using the Online Banking from public shared PCs (as in internet cafes, libraries, etc.) to avoid the risk of having your sensitive private information copied and abused

• Stay alert:

◦Sign-on to our Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)

◦ Keep track of your last log-on date and time, displayed at the top left side of the Online Banking Home page

◦Once logged into the Online Banking, you can also monitor the actions performed online through the Services menu >> Actions Log

•Respond promptly to incidents:

◦Contact our Call Center immediately at 19322 (in Egypt) or (+202) 3535 2790/91 (if calling from abroad), if you think someone knows your security access codes or in case of their loss or theft

◦Forward any suspicious e-mails to at phishing@abkegypt.com

Contact our Call Center immediately in the unfortunate event that you did provide your security access codes and other sensitive personal information to spoof websites or to phishing e-mails

◦Your prompt action is crucial to prevent any (further) damage