

## ABK-Egypt Online Banking - Security Advisory

### A. Steps we have taken to safeguard your access

ABK-Egypt realizes the importance of security in electronic transactions 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.

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

- **Client Identification through Security Access codes (User ID & password)**

After registration, you must use your User ID and password every time you login to Online Banking.

- *Retail Users* create their own User ID and password online, as per specific guidelines
- *Corporate Users* receive their initial access codes from the Bank, and during their first login to Online Banking must change the initial password to one of their choice, as per specific guidelines

By default, your password will expire every six months. However, you can change your password before that term if you wish so, and we recommend that you do so frequently, so that it will be impossible for any third party to guess it.

Furthermore, in case you do not intend to use the ABK 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 ABK-Egypt branch.

- **Privacy of Data Transfer through Encryption**

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

- **Session Time-out**

If Online Banking remains idle for ten minutes, then the session is automatically terminated and you are logged off. You must login 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 login, the system will lock your security codes and deny access to Online Banking. You can unlock your access via our Call Center (Retail & Corporate Users). Keep in mind that the Call Center representatives, or any ABK-Egypt Bank employee for that matter, are not aware of your password and they cannot retrieve it for you. In

case you do not remember it, you can reset your password online (Retail Users only) or request a new one from nearest ABK-Egypt branch (Corporate Users).

- **Security Code for additional authentication**

This is a one-time-password (OTP) that enables you to use the features requiring additional authentication. In general, the OTP may be generated either through a token or sent as an SMS message to your mobile phone.

## **B. 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 always up-to-date so that it can guard your PC 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, PINs, 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, frequently checking for and downloading new versions/security enhancements from the vendor's website
- Password-protect your PC so that no unauthorized person can gain access
- Disable the "auto complete" and the "save/remember password" functions of your web browser so that the next person using the same PC cannot access your accounts

- **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: ABK-Egypt will never initiate a contact with you to ask for your e-banking password, debit or credit card PIN, 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 in to 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 Online Banking through the official ABK-Egypt website [www.eahli.com](http://www.eahli.com)
  - Never attempt to access Online Banking 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 ABK-Egypt
  - When accessing Online Banking, look for the website identification info which confirms that connection to the server is encrypted over the Secure Sockets Layer (SSL) Data Encryption technology
  - Ignore and delete immediately suspicious fraudulent (phishing, spoof, hoax) e-mails that appear to be from ABK - Egypt, 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
  - Never use Online Banking from public shared PCs (as in internet cafés, libraries, etc.) to avoid the risk of having your sensitive, private information copied and abused
- **Stay alert**
  - Login to Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)
  - Read your banking statements and review your account transactions for any sign of irregular/fraudulent activity
  - Keep track of your last log-on date and time, displayed at the top left side of the ABK Online Banking Home page
  - Once logged into ABK 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** (from Egypt) or **(+202) 3535 2790/91** (from abroad), if you think someone knows your security access codes or in case of loss or theft
  - Forward any suspicious e-mails to ABK-Egypt at [infosec@abkegypt.com](mailto:infosec@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

Follow these simple instructions and make your online banking experience a safe and positive one. If you feel that the security of your account has been tampered with, contact the Bank immediately.