Security recommendations when using Bank Client

1. Set a password to the operating system
2. Set a password to BIOS
3. Restrict physical access to the computer where Bank-Client system is installed; exclude uncontrolled access to the premise where it is installed.
4. Do not entrust maintenance of this computer to unauthorized persons, do not let unauthorized persons access it.
5. Generate your secret key for Bank-Client yourself; do not entrust anybody to do it.
6. Keep key media in a safe box excluding unauthorized access to them.
7. After completion of work, remove key medium from the computer immediately and put it in safe box. Never hand over your key medium to anybody, do not leave it unattended.
8. Ensure safety of the computer where the system "Bank-Client" is installed:
   - Use only licensed software, a copy of which is obtained from reliable sources.
   - Make sure that you have antivirus software installed and automatic update of the anti-virus database is on. Check your computer for viruses and malware on a weekly basis.
   - Do not allow installation of remote controlling software such as Remote Administrator, VNC, Team Viewer. Turn off the built-in remote access service on your operating system.
   - Minimize the number of users on this computer.
   - Do not work use computer accounts with administrative privileges. Administrative privileges can be used only for installation and maintenance of software.
   - Do not use Internet on this computer for purposes other than using Bank-client and updating the software and the anti-virus databases. Using computer for browsing in Internet significantly increases the risk of its infection with malicious software.
   - Do not use e-mail, instant messaging software, and social networking in this computer. The malefactors often use these services to send malicious attachments, links to the sites distributing malicious software or fishing sites.
   - Block the computer when leaving the workplace (even for a short period). Turn off your computer in case upon completion of a working day or absence for a long period of time.
9. If Bank-Client is installed in a notebook, ensure keeping the key media separately from it and do not leave notebook unattended.
10. Immediately notify the bank to block the keys and check payment documents received by the bank on behalf of you in the following cases:

- Loss of the key medium
- Obtaining access to keys or your computer by unauthorized persons
- Detection of malicious software in the computer where Bank-client is installed
- Any other situation when unauthorized persons might have received access to secret keys.

11. In case of Bank-Client's or the computer's sudden failure, immediately inform the Bank about it and control the payment documents received by the bank on behalf of you.
12. Monitor operations on your account online daily. In case of detection of movements on the account that you did not make, immediately call the Bank's 24x7 Call Center by this number +996 312 620 101.
13. Follow the security recommendations sent by the Bank via Bank-Client system.
14. Contact technical support unit should you have any questions on Bank-Client +996 312 621 123.

Remember, when working with your accounts in Bank-client you should be more attentive and vigilant than when handling cash in your wallet!