MTI Bank

SAFETY RULES

Dear Clients!

We remind you about the basic security measures when working with the Bank-Client remote banking system (hereinafter referred to as the Bank's System):

1. **It is necessary to use the computer only for the purposes of making electronic payments in the Bank's System. You should not use your computer to visit websites on the Internet, or to receive emails from unknown email addresses, as this may lead to viruses infecting your computer. Install and configure a personal firewall on a computer with the pre-installed Bank's System. Allow access from the computer only to the IP addresses necessary for operation (the server of the Bank's System, the servers for updating the operating system and antivirus).**
2. Make sure that your computer is not infected with viruses. Install and periodically check the correctness of the antivirus software. Update your antivirus databases daily. Please note that viruses can be used to store and transmit information about your passwords and electronic signature keys to third parties.
3. Use licensed software obtained from trusted and reliable sources. To eliminate existing vulnerabilities, promptly install the latest Service Packs and up-to-date security patches for the operating system and application software. Remove software that is not related to the preparation and execution of electronic payments in the Bank's System from your computer.
4. It is necessary to restrict access to the computer from which the connection to the Bank's System is made. To do this, install the computer in a place inaccessible to unauthorised persons. It is desirable that this room be locked with a key. Sometimes a single restriction of physical access removes many security issues.
5. You need to set a password to access your computer. It is highly advisable to install a "screen saver" on the desktop with a start time of no more than 5 minutes (i.e. if the responsible employee does not work at the computer for more than 5 minutes, the computer turns on the "screen saver"), which can be unlocked only after entering the password. It is better to choose a password length of at least 8 characters. It is advisable that this password cannot be guessed, i.e. your phone numbers, names of loved ones, pet names and other facts known about you should not be used in the password. Storing the password in electronic form is unacceptable!
6. When connecting eToken for the first time, you need to change the PIN code and keep it secret. However, the password must not match the password for accessing your computer.
7. Be extremely careful about the key carrier, do not leave it unattended and do not pass it on to third parties. Remove key carriers from your computer if they are not used for work. The key must be stored separately from the computer in the safe of the company's director or a responsible employee and must not be accessible to unauthorised persons (including company employees who are not involved in electronic payments).
8. Do not leave eToken unattended while the specialists are working with your computer. When sending computer equipment for repair, make sure that no confidential information remains on the computer's hard drive.
9. Be careful when entering the server address of the Bank's System. Do not follow external links through fake websites to the server of the Bank' System. The Bank will never ask you to send your username and password by e-mail or by any other way.
10. **If there is the slightest suspicion of compromising the electronic signature keys, as well as the loss of a computer with the Bank-Client System installed, the Bank must be immediately informed in order to take urgent measures to block the electronic signature keys in order to prevent their unauthorised use**.

The Bank applies a wide range of measures to ensure the security of operations in the "Bank-Client" System. But remember that ensuring the security of financial transactions is our common cause!

Sincerely, MTI Bank