



Official website of the system

<https://halyk.onlinebank.kz>

➤ Avoid connections to the website of the OnlineBank HALYK System on banner links or links contained in emails. Check secure SSL-connection with official website of OnlineBank HALYK at <https://halyk.onlinebank.kz>. We recommend to enter the web address by yourself and add it to your browser bookmarks.

➤ Learn [how to recognize fishing \(fake\) website.](#) *

➤ Under NO circumstances DISCLOSE your login and password, and under NO circumstances TRANSFER your device eTOKEN PASS, key carrier with EDS keys to ANYONE, including employees of JSC Halyk Bank. The PASSWORD, device eTOKEN PASS, key carrier with EDS keys to enter and work in the OnlineBank HALYK system are your personal CONFIDENTIAL INFORMATION.

The system user is responsible for storage of personal confidential information, device eTOKEN PASS, key carrier with EDS keys and passwords. Keep the key carriers, eTOKEN PASS devices, login and password in places, where access is restricted to third parties.

➤ Do not use software that provides remote access and remote control of your personal computer/data, and in case of detection of such software, you must uninstall it and take measures to change the password and regenerate the EDS key.

➤ Nobody, but you must have access to the contents of the PIN envelope intended for safe and confidential password change procedure. When you receive the PIN envelope in JSC Halyk Bank's branch, make sure that the PIN envelope handed to you by an employee of the Bank does not contain any traces of opening or damage.

➤ Requirements for the use of one-time passwords generated by the eTOKEN PASS device, are similar to the requirements for the use of PIN envelopes: no one but you must have access to the eTOKEN PASS device. In case of loss or theft, as well as detection of unauthorized access to the device, you should IMMEDIATELY CONTACT THE BANK.

➤ DO NOT SAVE your PASSWORD IN THE INTERNET BROWSER AND TEXT FILES on the computer, or on other electronic media, as this may lead to its theft and compromise.

➤ When you access to the OnlineBank HALYK System, it is not recommended to work in the operating system under user account that has extended rights in the operating system, for example, "Administrator." Use the Operating System Security Policies to restrict access rights of the user. This will help reduce the risk of various attacks on the workstation and damage to the company from possible destructive actions of intruders.

➤ Minimize the access to the computer on which the OnlineBank HALYK System is installed.



- Monitor daily the information on electronic payment documents accepted and rejected by the Bank, as well as immediately inform the Bank about the unauthorized money crediting (transfer) and debiting.
- If your mobile phone, to which the Bank sends SMS notifications, is lost/stolen, or the SIM-card stops functioning unexpectedly, you should contact your mobile operator as soon as possible to block the SIM-card and inform the Bank about it.
- Always log out from the OnlineBank HALYK System through the "Log out" link, in this case your session will be terminated immediately and correctly.
- Upon completion of operation in the OnlineBank HALYK System, disconnect and remove the key carrier with EDS from the computer's USB port. Do not leave the key carrier with EDS keys constantly connected to the computer. Connect it only when you need to operate in OnlineBank HALYK system.
- Block your computer and be sure to remove key carrier with EDS keys from the USB port of the PC, if you want to leave the workplace.
- Avoid public places with shared Internet Access Points (such as Internet cafes and game clubs) to use the OnlineBank HALYK System, since you cannot be sure that computers connected to this network are free of spywares that can intercept and compromise your confidential credentials and personal data. Make banking transactions from personal computer that is specially assigned for these purposes and on a trusted network.
- Use only computers that have been checked for security risks and reliability to operate OnlineBank HALYK system.
- Timely INSTALL OPERATING SYSTEM UPDATES of your computer that are recommended by the manufacturing company.
- Use LICENSED ANTIVIRUS SOFTWARE and make sure to update it regularly.
- Perform REGULAR ANTIVIRUS SCANNING for the early detection and blocking of any malware.
- Use additional licensed software: personal firewalls, spyware program search, spam mailout protection programs and update them in timely manner.
- Do not run programs that are received from untrusted source (particular danger may be the program received by e-mail or downloaded from the Internet).
- CONNECT TO THE SMS NOTIFICATION SERVICE – the service represents sending of SMS messages to the mobile phone of the authorized person of the company - system user, about all initiated payments in tenge, exceeding the threshold limit set by the bank. Connection to the service is carried out by the Bank free of charge.



The Bank has all the necessary information and NEVER, under NO circumstances calls, sends emails, SMS messages, requesting to provide card details, PIN code of the card, and credentials, as well as emails programs and their updates.



In case of compromise of information or detection of unauthorized transactions, you should immediately call the Contact Center: 9595 (toll free), 8(727) 259-07-77 (for Almaty).