



HOME BANK SYSTEM AND MOBILE APP SAFETY TIPS

Official website of the system

<https://homebank.kz>



- Avoid connections to the website of the HOME BANK System on banner links or links contained in emails. Check secure SSL-connection with official website of the HOME BANK System - <https://homebank.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 to anyone, including employees of JSC Halyk Bank. HOME BANK login password is your personal CONFIDENTIAL INFORMATION. Remember, it is the user's responsibility to keep personal confidential data and passwords!
- The requirements to storage of one-time passwords printed on the ATM receipt are similar to the requirements for storage of bank card's PIN codes: no one except you must have access to the check with one-time passwords. IF THEY ARE LOST or stolen, you must IMMEDIATELY CONTACT THE BANK, or request new list of passwords via ATM.
- DO NOT SAVE your PASSWORD IN THE INTERNET BROWSER AND TEXT FILES on the computer or on other electronic media, because it can entail theft and compromise of the password.
- Do not indicate the mobile phone numbers, which are not registered in your name, when you register in the HOME BANK system and modify the settings.
- When you work in the HOME BANK system, it is not recommended using the account with expanded rights in the operating system, for example "Administrator".
- Analyze all messages about transactions accepted and unaccepted by the Bank on a daily basis, and immediately inform the Bank about cases of unauthorized crediting (transfer) or withdrawal of money.
- In case of loss/theft of the mobile phone, to which the Bank sends SMS messages with a confirmation one-time password, or if the SIM-card unexpectedly stops functioning, you should contact your mobile operator as soon as possible and block the SIM-card and inform the Bank accordingly.
- UPGRADE SECURITY LEVEL OF YOUR PAYMENTS - use the additional services of the Bank in the HOME BANK Mobile App, such as the "SMS Notifications" package, and set limits on the card transactions made on the Internet, etc.
- Always log out from the HOME BANK system via the link "Log out". In this case, your session will be terminated immediately and correctly.
- To use the HOME BANK system avoid public places with public Internet Access Points (such as Internet cafes and game clubs), since you cannot be sure that computers connected to these networks are not running spyware that can intercept and store your confidential credentials and personal data.
- Use only security-tested and reliable computers to work in HOME BANK 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 virus scanning to timely detect and block any malware.
- Use additional licensed software: personal firewalls, spyware program search, spam mailout protection programs, etc.
- Do not run programs that are received from untrusted sources (particular danger may be the programs received by e-mail or downloaded from the Internet).



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: 7111 (toll free), 8(727) 259-07-77 (for Almaty).