



MOBILE APP SAFETY TIPS



- Do not register phone numbers that do not belong to you as trusted numbers in the HOMEBANK mobile app;
- Do not save the password/PIN for access to the mobile app on the mobile device;
- Download the app to work with banking services only from official sources:
 - Bank's website- <http://www.halykbank.kz>;
 - app store for mobile platform iOS - [App Store](#);
 - app store for mobile platform Android - [Google Play](#).

Make sure that the author of the application is JSC Halyk Bank.
- Install the antivirus software on the mobile phone or mobile device that is available on:
 - app store for mobile platform iOS - [App Store](#);
 - app store for mobile platform Android - [Google Play](#), and make sure to update it regularly.
- Timely install official operating system updates of the mobile device, especially if it is related to security;
- When you install new application on the mobile device, always pay attention to authorization that it requires for its operation, especially on the ability to have access to the SMS messages. If authorization is suspicious or obviously does not correspond to the functionality of the program, it is better to abandon its use;
- If your mobile phone, to which the Bank sends you SMS messages with confirmation one-time password, is lost/stolen, or the SIM-card stops functioning unexpectedly, you should contact your mobile operator as soon as possible and block the SIM-card, as well as call the Bank's Contact Center to inform about it;
- Upgrade security level - use additional services of the Bank, such as the "SMS Notifications" package and setting limits on the card transactions made on the Internet, etc.;
- You must call the Bank's Contact Center, if you lose/change the mobile phone number;
- When you replace the mobile phone or mobile device, be sure to remove the HOMEBANK mobile app and its settings from the old device;
- Do not remove the limitations set by the mobile device manufacturer by [rooting](#) or [jailbreak](#) operations. This greatly reduces the effectiveness of the security options incorporated by the manufacturer, whereby your phone becomes vulnerable to infection with virus software;
- Set the password protection for access to the mobile device. This option is available for any modern models;
- Shut down the mobile application through the completion of the session ("Log out" button).



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).