

HOW TO RECOGNIZE FISHING (FAKE) WEBSITE

IF UNDER VARIOUS PRETEXTS YOU ARE REQUESTED:

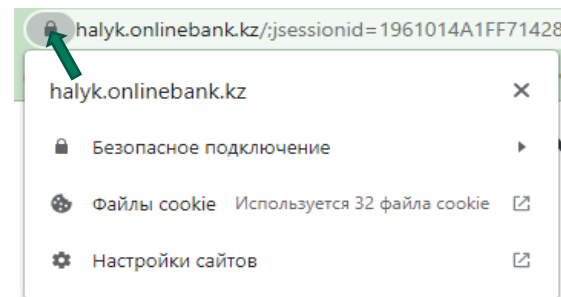
- to enter credentials, login/password, one-time password from eTOKEN PASS device, as well as to connect key carrier with EDS keys - for logging in the website after following a direct URL or banner link from various Internet resources, which are not official websites of the Bank;
- to enter credentials, login/password, one-time password from eTOKEN PASS device, as well as to connect key carrier with EDS keys - for logging in to the website, the address of which is placed in the form (body) of the letter received from the "Bank".

REMEMBER, UNDER NO CIRCUMSTANCES, THE BANK:

- does a bulk distribution of e-mails with attached files, links and forms as pages for logging in to the website of OnlineBank HALYK system;
- requests credentials/login, password, one-time password from eTOKEN PASS device and other confidential and personal information via these emails or in any other way.

DO NOT ENTER YOUR CONFIDENTIAL INFORMATION to logon the OnlineBank HALYK system, if:

- the website of OnlineBank HALYK system opened by you runs unsecured.
- browser icons indicating secure operation are inactive, for example, the lock is not closed or has a warning pictogram and coloring.
- the first characters of the website address of the OnlineBank HALYK system are http://, not https:// and browser window displays a message that browsing of the page starts via an insecure connection.
- at the entrance to the website your browser warns that the website's security certificate cannot be trusted.
- address does not match with the official website address of the OnlineBank HALYK system <https://halyk.onlinebank.kz>.



REMEMBER! To protect against attacks aimed at substitution of the address of the bank web-server and modification of content during data transmission, the Bank uses the TLS (Transport Layer Security) protocol, which encrypts traffic between the customer and the server, and the SSL certificate issued by one of the authoritative Internet key certification centers (Certificate Authority) - GeoTrust Inc, allows very simply and quickly check before using the website if it belongs to the Bank. To check it, just click the area indicated by the arrow and make sure that the site belongs to the Bank (for more details on the certificate just click More or View Certificates, depending on the type of browser).



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).