



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ (ПОДДЕЛЬНЫЙ) САЙТ

ЕСЛИ ПОД РАЗЛИЧНЫМИ ПРЕДЛОГАМИ ВАС ПРОСЯТ:

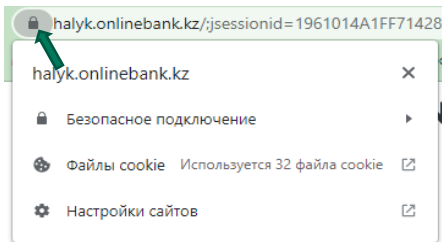
- ввести идентификационные данные, логин/пароль, одноразовый пароль с устройства eTOKEN PASS, а также подключить ключевой носитель с ключами ЭЦП - для входа на веб-сайт, после перехода по прямой URL или баннерной ссылке с различных интернет ресурсов, не относящихся к официальным веб-сайтам Банка;
- ввести идентификационные данные, логин/пароль, одноразовый пароль с устройства eTOKEN PASS, а также подключить ключевой носитель с ключами ЭЦП - для входа на веб-сайт, адрес которого размещен в форме (теле) письма, полученного от «Банка».

ПОМНИТЕ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ, БАНК:

- не осуществляет массовые email-рассылки писем с вложенными файлами, ссылками и формами в виде страниц для входа на сайт системы OnlineBank HALYK;
- не запрашивает посредством этих писем или каким-либо другим способом идентификационные данные/логин, пароль, одноразовый пароль с устройства eTOKEN PASS и другие, конфиденциальные и персональные данные.

НЕ ВВОДИТЕ СВОИ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ для входа в систему OnlineBank HALYK, если:

- открытый Вами веб-сайт системы OnlineBank HALYK работает в незащищенном режиме;
- иконки браузера, указывающие на работу в защищенном режиме, не активны, например, замочек не закрыт или имеет предупреждающую пиктограмму и цветовую раскраску;
- первые символы адреса веб-сайта системы OnlineBank HALYK http://, а не https:// и в окне браузера появляется сообщение о том, что начинается просмотр страницы через небезопасное соединение;
- при входе на веб-сайт Ваш браузер предупреждает, что сертификату безопасности сайта нельзя доверять;
- адрес не совпадает с официальным адресом веб-сайта системы OnlineBank HALYK <https://halyk.onlinebank.kz>.



ВНИМАНИЕ! Для защиты от атак, направленных на подмену адреса банковского веб-сервера и модификации контента во время передачи данных, Банк применяет протокол TLS (Transport Layer Security), который шифрует трафик между клиентом и сервером, а SSL-сертификат, выданный одним из авторитетных Интернет центров сертификации ключей (Certificate Authority) – компанией GeoTrust Inc, позволяет очень просто и быстро проверить перед началом работы с веб-сайтом его принадлежность Банку. Для проверки достаточно кликнуть курсором в область, указанную стрелкой и убедиться, что сайт принадлежит Банку (для получения более подробной информации по сертификату достаточно нажать кнопку Подробнее или кнопку Просмотр сертификатов, в зависимости от типа браузера).



Банк владеет всей необходимой информацией и **НИКОГДА**, ни при каких обстоятельствах **НЕ ОСУЩЕСТВЛЯЕТ** звонки по телефону, рассылку электронных писем, SMS-сообщений, с просьбой передать реквизиты платежной карты, ПИН-код к платежной карте, авторизационные данные, а также не распространяет по электронной почте программы и их обновления.



В случае компрометации данных или обнаружения несанкционированных транзакций, Вам необходимо обратиться в Контакт-центр Банка, по следующим телефонам:
9595 (бесплатно с мобильного), 8(727) 259-07-77 (для города Алматы).