



СОВЕТЫ ПО БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ONLINEBANK HALYK (1/2)



Официальный сайт системы

<https://halyk.onlinebank.kz>

➤ Избегайте подключений к веб-сайту системы OnlineBank HALYK по баннерным ссылкам или по ссылкам, содержащимся в электронных письмах. Проверяйте, что установлено защищенное SSL-соединение с официальным сайтом системы OnlineBank HALYK, по адресу <https://halyk.onlinebank.kz>. Рекомендуем ввести адрес веб-сайта самостоятельно и добавить его в закладки браузера.

➤ Узнайте, [как распознать фишинговый \(поддельный\) веб-сайт](#).

➤ Ни при каких обстоятельствах НЕ РАЗГЛАШАЙТЕ свой логин и пароль, и ни при каких обстоятельствах НЕ ПЕРЕДАВАЙТЕ устройство eTOKEN PASS, ключевой носитель с ключами ЭЦП - НИКОМУ, включая сотрудников АО «Народный Банк Казахстана».

ПАРОЛЬ, устройство eTOKEN PASS, ключевой носитель с ключами ЭЦП для входа и работы с системой OnlineBank HALYK - это ваша личная КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ.

Ответственность за хранение личных конфиденциальных данных, устройств eTOKEN PASS, ключевого носителя с ключами ЭЦП и паролей возлагается на пользователя системы. Храните ключевые носители, устройства eTOKEN PASS, логин и пароль в местах, к которым ограничен доступ третьих лиц.

➤ Не используйте программное обеспечение, предоставляющее удаленный доступ и удаленное управление Вашим персональным компьютером/данными, а в случае обнаружения такого программного обеспечения, необходимо его деинсталлировать и принять меры по смене пароля и регенерации ключа ЭЦП.

➤ Никто кроме Вас не должен иметь доступ к содержимому ПИН-конверта, предназначенного для безопасной и конфиденциальной процедуры смены пароля. При получении ПИН-конверта в филиале АО «Народный Банк Казахстана» убедитесь, что ПИН-конверт, переданный Вам работником Банка, не содержит следов вскрытия и повреждений.

➤ Требования к использованию одноразовых паролей, генерируемых на устройстве eTOKEN PASS, аналогичны требованиям к использованию ПИН-конвертов: никто кроме Вас не должен иметь доступ к устройству eTOKEN PASS. В случае утери или кражи, а также обнаружения фактов несанкционированного доступа к устройству Вам следует НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЬСЯ В БАНК.

➤ НЕ СОХРАНЯЙТЕ Ваш ПАРОЛЬ В ИНТЕРНЕТ БРАУЗЕРЕ И ТЕКСТОВЫХ ФАЙЛАХ на компьютере, либо на других электронных носителях информации, так как это может привести к его краже и компрометации.

➤ Во время доступа в систему OnlineBank HALYK, не рекомендуется работать в операционной системе под учетной записью пользователя, который имеет расширенные права в операционной системе, например, «Администратор». Используйте политики безопасности операционной системы для ограничения прав доступа пользователю. Это поможет снизить риск реализации различных атак на рабочую станцию и причинения ущерба компании от возможных действий деструктивного характера злоумышленников.

➤ Максимально ограничьте доступ к компьютеру, на котором установлена система OnlineBank HALYK.



СОВЕТЫ ПО БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ONLINEBANK HALYK (2/2)

- Ежедневно анализируйте информацию о принятых и непринятых Банком электронных платежных документах, а также немедленно информируйте Банк о случаях несанкционированного зачисления (перечисления) или списания денег.
- При утере/краже мобильного телефона, на который Банк отправляет SMS-уведомления, или неожиданном прекращении работы SIM-карты, Вам следует, как можно быстрее, обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Банк.
- Всегда выходите из системы OnlineBank HALYK через ссылку «Выход», в этом случае Ваш сеанс будет прекращен немедленно и корректно.
- По завершению работы в системе OnlineBank HALYK отключите и извлеките ключевой носитель с ЭЦП из USB порта компьютера. Не оставляйте ключевой носитель с ключами ЭЦП постоянно подключенным к компьютеру. Подключайте его только при необходимости работы в системе OnlineBank HALYK.
- Блокируйте компьютер и обязательно извлекайте из USB порта персонального компьютера ключевой носитель с ключами ЭЦП, если требуется покинуть рабочее место.
- Избегайте публичных мест с общедоступными точками доступа в интернет (таких как интернет-кафе и игровые клубы) для использования системы OnlineBank HALYK, так как Вы не можете быть уверены, что на компьютерах, подключенных к данной сети, не стоят программы-шпионы, способные перехватить и скомпрометировать Ваши конфиденциальные идентификационные данные. Осуществляйте банковские операции со специально выделенного под эти цели персонального компьютера и в доверенной сети.
- Используйте для работы с системой OnlineBank HALYK только проверенные на отсутствие угроз безопасности и надежные компьютеры.
- Своевременно УСТАНОВЛИВАЙТЕ ОБНОВЛЕНИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ своего компьютера, рекомендуемые компанией-производителем.
- Используйте ЛИЦЕНЗИОННОЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ и следите за его регулярным обновлением.
- РЕГУЛЯРНО ВЫПОЛНЯЙТЕ АНТИВИРУСНУЮ ПРОВЕРКУ для своевременного обнаружения и блокирования вредоносных программ.
- Используйте дополнительное лицензионное программное обеспечение: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам-рассылок» и своевременно обновляйте их.
- Не запускайте программы, полученные не из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или скачанные из Интернета).
- ПОДКЛЮЧИТЕСЬ К УСЛУГЕ «SMS-УВЕДОМЛЕНИЕ» - сервису, который представляет собой отправку SMS-сообщения на мобильный телефон уполномоченного лица организации – пользователя системы обо всех инициированных платежах в тенге, превышающих установленный банком пороговый лимит. Подключение к услуге осуществляется Банком бесплатно.



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).