Приложение 2
к Правилам предоставления услуг
Финансового портала Homebank
для физических лиц
в АО «Народный Банк Казахстана»

Советы по безопасности при работе на Финансовом портале Homebank и использовании мобильного приложения Homebank

- НИКОМУ НЕЛЬЗЯ СООБЩАТЬ/ПЕРЕДАВАТЬ КОД ИЗ SMS-СООБЩЕНИЯ, В ТОМ ЧИСЛЕ РАБОТНИКУ БАНКА!
- НЕЛЬЗЯ ПОДКЛЮЧАТЬ В БАНКОМАТЕ ЧУЖОЙ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА!
- НИКОМУ НЕ СООБЩАЙТЕ/НЕ ПЕРЕДАВАЙТЕ, В ТОМ ЧИСЛЕ РАБОТНИКУ БАНКА - НОМЕР КАРТЫ, СРОК ЕЕ ДЕЙСТВИЯ (ЛИЦЕВАЯ СТОРОНА КАРТЫ) И 3-Х ЗНАЧНЫЙ КОД CVV/CVC (ОБРАТНАЯ СТОРОНА КАРТЫ)!
- Избегайте подключений к веб-сайту системы Homebank по баннерным ссылкам или по ссылкам, содержащимся в электронной почте. Проверяйте, что соединение с официальным сайтом системы Homebank защищено шифрованием (наличие префикса https), а также доменное имя сайта (обязательно очень внимательно, имя мошеннического сайта может отличаться всего на один символ) – https://homebank.kz. Рекомендуем ввести этот адрес веб-сайта самостоятельно и добавить его в закладки браузера.
- Ни при каких обстоятельствах НЕ РАЗГЛАШАЙТЕ свой логин и пароль никому, включая работников Банка. ПАРОЛЬ ДЛЯ ВХОДА в Homebank – это Ваша личная КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ. Ответственность за хранение личных конфиденциальных данных и паролей возлагается на пользователя.
- **НЕ СОХРАНЯЙТЕ** Ваш **ПАРОЛЬ В ИНТЕРНЕТ-БРАУЗЕРЕ И ТЕКСТОВЫХ ФАЙЛАХ** на компьютере либо на других электронных носителях информации, потому что это может привести к его краже и компрометации.
- Не указывайте при регистрации в системе Homebank и при изменении настроек номера телефонов, не принадлежащие Вам.
- Не осуществляйте авторизацию в приложении Homebank с установкой ПИН-кода или входа по отпечатку пальца на чужом мобильном устройстве.
- Во время доступа в Homebank не рекомендуется работать в системе под учетной записью с расширенными правами в операционной системе, например, «Администратор».
- Ежедневно анализируйте все сообщения о принятых и непринятых Банком транзакциях, а также немедленно информируйте Банк о случаях несанкционированного зачисления (перечисления) денег.
- В случае утери/кражи мобильного телефона, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, или неожиданного прекращения работы SIM-карты Вам следует как можно быстрее обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Банк.
- **ПОВЫШАЙТЕ УРОВЕНЬ БЕЗОПАСНОСТИ** – пользуйтесь дополнительными услугами Банка, такими как «SMS-банкинг» и установление лимитов на карточные операции в сети интернет и пр.
- Всегда выходите из системы Homebank через ссылку «Выход», в этом случае Ваш сеанс будет прекращен немедленно и корректно.
- Избегайте мест с публичными точками доступа в интернет (таких как интернет-кафе и игровые клубы) для использования системы Homebank, так как Вы не можете быть уверены, что на компьютерах данных заведений не стоят программы-шпионы, способные сохранить ваши конфиденциальные идентификационные и персональные данные.
- Используйте для работы с системой Homebank только проверенные и надежные компьютеры.

- Своевременно **УСТАНАВЛИВАЙТЕ 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 вредоносных программ.
- Банк владеет всей необходимой информацией и никогда, ни при каких обстоятельствах **НЕ ОСУЩЕСТВЛЯЕТ РАССЫЛКУ ЭЛЕКТРОННЫХ ПИСЕМ, SMS-сообщений**, звонков по телефону с просьбой передать реквизиты платежной карточки, авторизационные данные, ПИН-код к платежной карточке, а также не распространяет по электронной почте программы и их обновления.
- В случае компрометации данных или обнаружения фактов несанкционированного доступа и проведения с банковских счетов несанкционированных транзакций посредством системы Homebank Вам необходимо незамедлительно обратиться в Контакт-центр по телефонам, размещенным в нижней части страницы web-сайта, а также по короткому номеру с мобильного телефона или звонка в Skype.

Как распознать фишинговый (поддельный) веб-сайт?

Зеленый замочек и наименование Банка перед адресом официального сайта системы Homebank означает, что этот веб-сайт использует сертификат расширенной проверки подлинности (EV).

ЕСЛИ под различными предлогами Вам предлагается:

- ввести идентификационные данные, логин/пароль, номер мобильного телефона, номер платежной карточки, CVV, Ф.И.О. – для входа на веб-сайт системы Homebank, после перехода по прямой URL или баннерной ссылке с различных интернет-ресурсов, не относящихся к официальным веб-сайтам Банка;
- ввести идентификационные данные, логин/пароль, номер мобильного телефона, номер платежной карточки, CVV, Ф.И.О. – для входа на веб-сайт системы Homebank 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 для входа на сайт системы Homebank;
- не запрашивает посредством этих писем или каким-либо другим способом логины, пароли, одноразовые пароли и другие конфиденциальные идентификационные и персональные данные.

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

- открытый Вами веб-сайт системы Homebank работает в незащищенном режиме – иконки браузера, указывающие на работу в защищенном режиме, неактивны, например, замочек не закрыт или имеет предупреждающую цветовую раскраску;
- первые символы адреса веб-сайта системы Homebank 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 Homebank https://homebank.kz;
- в случае компрометации данных или обнаружения фактов несанкционированного доступа и проведения с банковских счетов несанкционированных транзакций посредством системы Homebank Вам необходимо незамедлительно обратиться в Контакт-центр по телефонам, размещенным в нижней части страницы web-сайта, а также по короткому номеру с мобильного телефона или звонка в Skype.