ПАМЯТКА

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

при работе с системой Интернет-банкинг
АО «Жилстройсбербанк Казахстана»

ЖИЛ СТРОЙ СБЕР БАНК

УВАЖАЕМЫЕ КЛИЕНТЫ АО " ЖИЛСТРОЙСБЕРБАНК КАЗАХСТАНА"!

Для минимизации рисков при работе в системе Интернет-банкинг просим Вас:

- не передавать свои пароли или другие атрибуты доступа работникам Банка и третьим лицам (логины, ключи, токены, смарт-карты и т.п.);
- в целях недопущения несанкционированного доступа третьими лицами в систему Интернет-банкинг осуществлять смену пароля в установленные сроки или по мере необходимости;
- обязательно сменить пароль в систему Интернет-банкинг при первом входе, или после сброса пароля администратором системы;
- не хранить пароль на вход в систему Интернет-банкинг в открытом виде, том числе непосредственно в браузере или в системе автоматизированного входа;
- не распространять пароли по открытым каналам (устно, письменно или по электронной связи и т.д.);

- пользоваться одним компьютером, не допускать смены паролей и проведение платежей с малознакомых компьютеров, к которым имеет доступ множество пользователей. При работе на чужом компьютере, ни в коем случае не сохранять свои данные (ключ электронноцифровой подписи, учетные записи, пароли и др.);
- подключить СМС-информирование о всех операциях по счетам;
- в случае выявления (подозрения) несанкционированного доступа к системе Интернет-банкинг (личному кабинету) или несанкционированной операции, заблокировать номер телефона через оператора сотовой связи и незамедлительно любыми способами информировать Банк;
- осуществлять информационное взаимодействие с Банком только с использованием средств связи, реквизиты которых оговорены в документах, полученных непосредственно от Банка или иных официальных информационных источниках (особенно при использовании электронной почты);
- в случае утери, кражи и иных случаях утраты SIM-карты, а также смены SIM-карты или ее передачи третьим лицам по любым основаниям, немедленно обратиться в Банк, с заявлением на изменение данных клиента по форме установленной внутренними документами Банка в целях смены номера телефона;

- использовать современные средства обеспечения информационной безопасности при работе в сети Интернет (антивирусное программное обеспечение, персональные межсетевые экраны и т.п.). Используйте лицензионное программное обеспечение, а также своевременно обновляйте антивирусные средства защиты на Вашем компьютере/мобильном устройстве. Регулярное обновление антивирусных баз и поддержка антивирусных средств защиты в актуальном состоянии обезопасит Ваш компьютер от вредоносного программного обеспечения;

- не доверяйте непроверенным Wi-Fi соединениям, которые не запрашивают пароль. Не заходите в Интернет-банкинг через открытые Wi-Fi сети в кафе или на улице, воспользуйтесь мобильным интернетом. Выключайте Wi-Fi, когда им не пользуетесь.

- для корректного закрытия сессии следует совершать выход из системы Интернет-банкинг с помощью кнопки «Выход». Настоятельно рекомендуется завершать работу с системой Интернет-банкинг с использованием данной кнопки;

- сотрудничать с Банком в принятии последним мер, направленных на минимизацию рисков при дистанционном банковском обслуживании, в том числе выполнять рекомендации банка, касающиеся обеспечения безопасности работы в системе Интернет-банкинг.

Следует помнить и учитывать, что большинство случаев хищения логина и пароля осуществляются:

- лицами, имевшими доступ к Вашему компьютеру, с которого осуществлялась работа в системе дистанционного банковского обслуживания;
- злоумышленниками путем заражения через сеть Интернет компьютеров клиентов вредоносными программами с последующим хищением учетных данных и паролей клиентов – рекомендуем установить программное обеспечение, предназначенное для безопасной работы в сети Интернет, на постоянной основе осуществлять контроль функционирования, в том числе своевременное обновление операционной системы, антивирусных баз и модулей программного обеспечения, реализующего функции информационной безопасности.

Помните:

Банк никогда не рассылает писем с просьбой перейти по ссылке, изменить свой пароль, ввести номер телефона и секретный код подтверждения или сообщить другие личные данные!

- Со своей стороны Банк полностью осознает необходимость принятия адекватных мер по обеспечению безопасности работы клиентов с системой Интернет-банкинг и делает всё возможное для вашей безопасности, уверенности и спокойствия.

ПАМЯТКА
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Скачайте наше мобильное приложение

https://play.google.com/store/apps/details?id=kz.sdk.hcsbk

https://apps.apple.com/us/app/zssb-24/id1148478653

ЖССБ 24 https://online.hcsbk.kz

ЖИЛСТРОЙСБЕРБАНК