Рекомендации по защите информации при использовании системы HandyBank.

*УБЕДИТЕСЬ, что название сайт **https://aktivbank.handybank.ru/** и в наличии символа **замка** справа/слева от адресной строки или в правом нижнем углу страницы. Этот символ указывает на то, что сайт работает в защищенном режиме.

*ЗАПОМНИТЕ, что для входа в HandyBank требуется вводить только ваши Handy-номер и Handy-пароль. НЕ НУЖНО вводить номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации!

*НИКОГДА и ни при каких обстоятельствах не сообщайте никому свой Handy-пароль.

*В СЛУЧАЕ УТЕРИ мобильного телефона, на который приходят SMS-сообщения с Handy-кодом, немедленно заблокируйте SIM-карту (тел. МТС 8 800 250 0890, Мегафон - 8 800 550 0500, Билайн -8 800 700 0611).

*БУДЬТЕ БДИТЕЛЬНЫ: в случае возникновения подозрения на мошенничество необходимо максимально быстро сообщить об этом в банк с целью оперативной блокировки доступа!

Подробнее о мерах безопасности

Уважаемые клиенты!

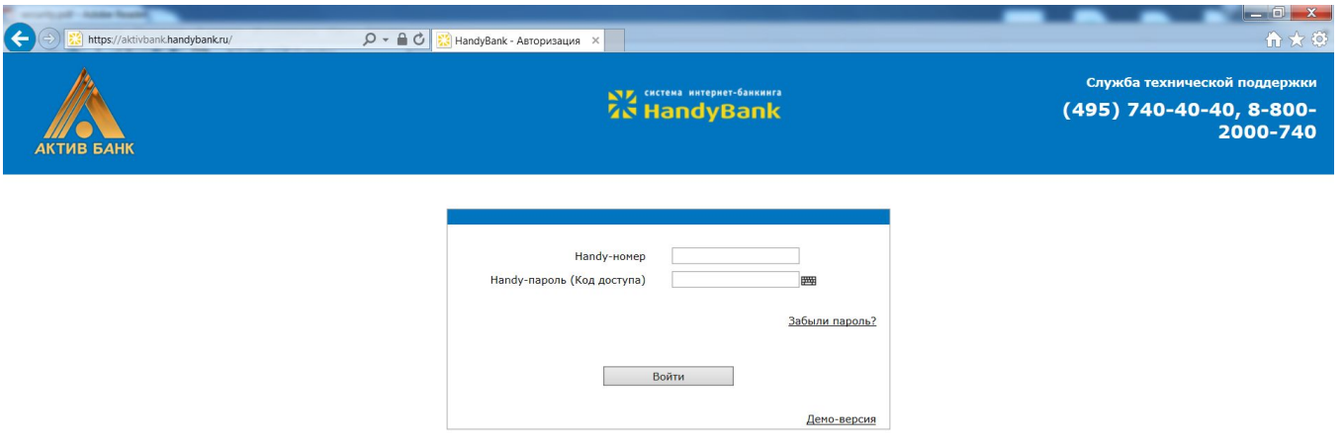
Для того, чтобы работа в системе интернет-банкинга HandyBank была не только удобной, но и более защищенной, просим вас до начала работы ознакомиться с рекомендациями по безопасности.

Распечатайте для себя эти рекомендации, чтобы в любой момент иметь их под рукой.

Для обеспечения безопасности проводимых операций в HandyBank используются следующие средства защиты:

Защищенное соединение (SSL-шифрование)

Соединение и работа с HandyBank осуществляется через интернет, поэтому для защиты канала, по которому компьютер клиента соединяется с сервером, используется защищенный режим SSL. Признаком установки защищенного соединения является то, что адрес **https://aktivbank.handybank.ru/** начинается с **https://** (обязательно символ **s**), а в браузере появляется изображение замка (справа или слева от адресной строки, либо справа вверху/внизу браузера).



Кликнув по замку, можно убедиться в подлинности сертификата.

Handy-коды для проведения операций.

Handy-код используется для подтверждения операций в HandyBank. Для получения Handy-кода необходим мобильный телефон, номер которого был указан вами при подключении услуги HandyBank. После ввода всех необходимых платежных реквизитов, система предложит ввести Handy-код для подтверждения операции. Для

получения Handy-кода нужно нажать на кнопку «Handy-код» в пункте «Подписать». Handy-код будет доставлен в SMS-сообщении на ваш мобильный телефон, и будет содержать также краткую информацию о реквизитах подготовленного документа.

Как Вы можете позаботиться о безопасности:

Обновляйте операционную систему и другие программы на вашем компьютере.

Используйте лицензионную операционную систему. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые компанией-производителем. Устанавливайте обновления только с официальных сайтов (репозиториев) компаний-производителей.

Используйте дополнительные средства безопасности.

Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты вашего компьютера - персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.

Установите и обновляйте антивирус на вашем компьютере.

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Используйте современное, лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

Если у вас есть подозрение, что ваши Handy-номер и Handy-пароль украдены, как можно быстрее смените ваш Handy-пароль в HandyBank, либо заблокируйте доступ в HandyBank по телефону Банка: **+7 (8342) 77-77-81** (в рабочее время банка: пн.-пт. с 8.30 до 17.30), либо заблокируйте банковскую карту по телефону процессинга: **+7 (495) 723-77-21.**

Помните, что для входа в HandyBank нужны только Handy-номер и Handy-пароль.

На странице входа не должно быть никаких дополнительных полей для ввода такой информации как Handy-код, номер вашей карты и другие реквизиты (CVV/CVC код, срок действия карты, имя владельца). Если появились такие поля - сообщите об этом по телефонам системы HandyBank: **+7 (495) 740-40-40 и 8-800 2000-740,** либо по телефону Банка **+7 (8342) 77-77-81** (в рабочее время банка: пн.-пт. с 8.30 до 17.30).

Никому не сообщайте ваши Handy-пароль и Handy-код.

Handy-пароль и Handy-код - это ваша личная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте никому свои пароли, включая сотрудников Банка. Сотрудники Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию.

Не сохраняйте ваш Handy-пароль на компьютере либо на других электронных носителях информации, потому что это может привести к его краже и компрометации.

При каждом входе в систему проверяйте адрес сайта HandyBank.

Система HandyBank доступна только по адресу: **https://aktivbank.handybank.ru/** Вас могут пытаться обмануть, предлагая оставить ваши Handy-пароль и Handy-номер на поддельном сайте (например, http://aktivbank.handybank.com.org). Если вы обнаружите такой сайт, обязательно сообщите об этом по телефонам, указанным выше!

Не используйте публичные сети доступа в интернет (интернет-кафе, открытые Wi-Fi сети в супермаркетах и т.п.) для работы в системе.

Подобный доступ в систему увеличивает риск хищения и дальнейшего неправомерного использования средств идентификации и/или подтверждения.

Помните, что Handy-код, присланный вам по SMS, действует только на подтверждение операции.

Никто никогда не попросит у вас ввести Handy-код для отмены операции.

Внимательно проверяйте сумму и реквизиты операции в SMS-сообщении, содержащем Handy-код.

Информация в нем должна совпадать с вашей операцией в HandyBank, которую вы хотите подтвердить. Если эта информация не совпадает, не вводите Handy-код и сообщите об этом в Банк!

Используйте для звонков в Банк номера телефонов, указанные на вашей карте, либо в данной памятке.

Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, который будет пытаться вас обмануть. В случае подозрения на мошенничество сообщите об этом в Банк только по номерам, указанным выше или на вашей карте!

Проверяйте, используется ли защищенное соединение - https://aktivbank.handybank.ru/

Проверяйте, действительно ли соединение происходит в защищенном режиме SSL - справа или слева от адресной строки, либо справа вверху/внизу браузера должен быть изображен значок **закрытого замка.**

Корректно завершайте работу в HandyBank.

Завершение работы с системой выполняйте путем выбора соответствующего пункта меню «ЗАКРЫТЬ СЕАНС» - это удалит из браузера информацию о параметрах работы в HandyBank. После окончания работы в системе или при временном перерыве завершайте работу в системе, не оставляйте её открытой.

Защитите свой мобильный телефон.

Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения с Handy-кодом, приложения, полученные от неизвестных вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email - сообщения.

При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с Handy-кодом, Вам следует как можно оперативнее обратиться к своему оператору сотовой связи и заблокировать телефонную SIM-карту, либо заблокировать доступ в систему HandyBank, либо заблокировать карту.

Не заходите в интерфейс HandyBank с того же мобильного телефона, устройства, на который приходят SMS-сообщения с Handy-кодом.

Что делать, если вам пришло SMS на подтверждение операции, которую вы не совершали:

Вам следует как можно оперативнее обратиться по телефонам, указанным в памятке для блокирования вашей банковской карты и учетной записи в системе HandyBank. Не используйте этот Handy-код, даже если вам позвонил сотрудник Банка и попросил сделать это.

Установите или обновите антивирус.

Выполните полную проверку компьютера на вирусы.

Проверьте SSL-сертификат при доступе к интерфейсу HandyBank (сделать это можно нажав на иконку замка в вашем браузере). Сертификат должен быть действительным для ***.handybank.ru** (поле «Кому выдан).

Заходите в интерфейс HandyBank с этого компьютера только после того, как вы выполнили все рекомендации, перечисленные выше.

О факте такого SMS обязательно сообщите по телефонам: +7 (495) 740-40-40 и 8-800-2000-740 Что делать, если есть подозрение на мошенничество:

Если вы получили подозрительное письмо или sms-сообщение, необходимо обратиться в службу поддержки по телефонам **+7 (495) 740-40-40 и 8-800-2000-740.**

Если есть подозрения, что ваши Handy-номер и Handy-пароль стали известны кому-либо, обязательно смените Handy-пароль самостоятельно на незараженном компьютере или получите новый Handy-пароль в Банке.

О несанкционированных операциях, совершенных с использованием устройств мобильной связи

Участились случаи осуществления переводов денежных средств с использованием устройств мобильной связи (смартфоны, телефоны, планшеты) без согласия их владельцев (далее — несанкционированные операции).

В частности, к таким несанкционированным операциям относятся:

операции по оплате товаров и услуг при осуществлении доступа к сети Интернет через устройство мобильной связи, в том числе по реквизитам платежных карт;

операции по переводу денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;

операции, осуществляемые с использованием приложений дистанционного банковского обслуживания (ДБО), предоставляемых банком («Клиент-Банк») и установленных клиентом на устройстве мобильной связи;

операции по оплате товаров и услуг с использованием иных приложений, установленных на устройстве мобильной связи.

Несанкционированные операции проводятся вследствие заражения устройств мобильной связи вредоносными программами (в том числе вирусами), через спам-рассылку сообщений (sms-сообщений, сообщений электронной почты), содержащих ссылки на внешние ресурсы, или при переходе пользователя устройства мобильной связи по ссылкам на ресурсы сети Интернет. При переходе пользователя по таким ссылкам вирус устанавливается на устройство мобильной связи.

Вредоносные программы могут обладать различными возможностями, в том числе:

формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств, в том числе в виде смс-сообщений на «короткие номера»;

формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств с использованием приложений ДБО и иных приложений, предназначенных для оплаты товаров и услуг;

перехватывают одноразовые коды подтверждения, приходящие на мобильное устройство в целях дополнительного подтверждения операции.

Наибольший риск таких операций связан с тем, что в ряде случаев вредоносная программа скрывает от клиента приходящие от банка уведомления о списании денежных средств. Таким образом, пользователь мобильного устройства, не зная о несанкционированном списании с его банковского счета, не может направить в банк в определенные законодательством сроки уведомление о переводе денежных средств без его согласия.

Дополнительно сообщаем, что распространенным случаем осуществления несанкционированных операций также является использование методов социальной инженерии, когда злоумышленники обманными действиями вынуждают клиента сообщить данные, необходимые для проведения операции, в том числе пароли, коды аутентификации и др.

Рекомендуется лицам, осуществляющим переводы денежных средств с использованием устройств мобильной связи, предпринимать следующие меры для минимизации рисков хищения денежных средств:

установить на устройство мобильной связи антивирусное программное обеспечение с регулярно обновляемыми базами;

не переходить по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты;

своевременно уведомлять банк о смене номера телефона мобильной связи, который клиент предоставил банку для получения услуги «мобильный банкинг», в том числе, на который происходит информирование об операциях по счету клиента;

не скачивать на устройство мобильной связи приложения из непроверенных источников;

не передавать устройство мобильной связи и платежную карту для использования третьим лицам, в том числе родственникам;

не сообщать третьим лицам, в том числе сотрудникам банка, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платежной карте (CVV/CVC код - трехзначные коды проверки подлинности банковской карты платежных систем Visa и MasterCard, наносимые на полосе для подписи держателя карты), пароли от «Клиент-банка», одноразовые коды подтверждения; при наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом в банк.

В случае обнаружения списания денежных средств необходимо в сроки, установленные законодательством РФ, обратиться в банк или к оператору связи (если произошло списание денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»).

Для получения дополнительной информации по Вы можете ежедневно по рабочим дням с 8-30 до 17-30 обратиться: Отдел пластиковых карт: (8342) 77-77-81