Рекомендации по обеспечению безопасной работы
в системе HandyBank

Уважаемые клиенты, до начала работы в системе HandyBank просим Вас ознакомиться с нижеуказанными 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 HandyBank 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.

Минимальные меры безопасности, которые необходимо соблюдать при работе в системе:

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 в целях защиты от вредоносного кода

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 или обратитесь в офис Банка для блокировки доступа в систему.

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 – срочно сообщите об этом в Банк.

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 системы HandyBank

Система HandyBank доступна только по адресам: https://metcombank.handybank.ru/ или https://secure.handybank.ru/. Вас могут пытаться обмануть, предлагая оставить Ваши Handy-пароль и Handy-номер на поддельном сайте (например, http://metcombank.handybank.com.org). Если Вы обнаружите такой сайт, обязательно сообщите об этом в Банк!

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 только номера телефонов, указанные на официальном сайте Банка http://www.metcombank.ru

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 на официальном сайте Банка!

Проверяйте, используется ли защищенное соединение – https://metcombank.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.

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.

При наличии возможности, не заходите в интерфейс HandyBank с того же мобильного телефона, 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 в Банк для блокировки учетной записи в системе HandyBank. Не используйте этот Handy-код, даже если Вам позвонил человек, представившийся сотрудником 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 в Банк.

Что делать, если есть подозрение на мошенничество:

Если Вы получили подозрительное письмо или sms-сообщение, необходимо обратиться в Банк и сообщить о данном факте.

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.