Об устройстве SafeTouch

**Уважаемые клиенты!**

Благодарим Вас за то, что Вы выбрали услуги дистанционного банковского обслуживания РОСКОМСНАББАНК (ПАО). Наши сервисы обеспечат Вам удобный и безопасный доступ к Вашим финансам, простое и оперативное управление счетами.

Отличительной чертой электронных сервисов, представляемых РОСКОМСНАББАНК (ПАО), является высокий уровень защиты пользовательских данных. РОСКОМСНАББАНК (ПАО) считает приоритетным вопрос обеспечения информационной безопасности своих услуг, ввиду участившихся в последнее время случаев мошенничества в сети Интернет.

Анализ ситуации показывает, что в целях хищения денежных средств в основном используется атака, направленная на заражение компьютера клиента специальными вредоносными программами. Далее, в момент подписания клиентом платежного поручения такая программа незаметно для пользователя подменяет реквизиты документа, после чего средства перечисляются от лица легальных пользователей на счета мошенников.

**Почему это происходит?**

Основными причинами, при которых подобные действия злоумышленников могут нанести существенный ущерб пользователем систем дистанционного банковского обслуживания, являются:

- Слабая антивирусная защита рабочего места пользователя. Вредоносные программы (вирусы) могут инфицировать Ваш компьютер через электронную почту или при посещении Вами предварительно «зараженных» Интернет-сайтов.

- «Фишинговые» атаки с использованием методов социальной инженерии. Пользователи получают якобы официальные электронные письма от банка (обычные письма, телефонные звонки, сообщения SMS) с просьбой что-то подтвердить или с чем-либо ознакомиться на подложном сайте банка. При прочтении такого письма клиент перенаправляется на сайт, похожий на официальный сайт банка, где ему предлагается указать свои регистрационные данные и реквизиты своего счета. Даже если Вы не поддадитесь на уловки мошенников, то уже сам факт посещения такого сайта чреват риском заполучить на свой компьютер программу - «шпиона».

- Низкий уровень защиты доступа к компьютеру. Применение простых парольных комбинаций и отсутствие должного контроля за доступом к Вашему компьютеру, могут стать существенным подспорьем для проведения атаки злоумышленником с целью хищения денег со счета в системе Интернет-банкинга.

РОСКОМСНАББАНК (ПАО) непрерывно работает над обеспечением безопасности Ваших платежей: производит контроль доступа к системе дистанционного обслуживания, осуществляет проверку целостности и авторства электронных документов, отслеживает нетипичные операции,

назначения платежей, а также проводит анализ реквизитов получателей. В некоторых случаях банк может дополнительно обращаться к клиенту для подтверждения операций, вызывающих подозрение. Тем не менее, полностью исключить риск мошенничества с использованием сети Интернет без участия самого пользователя невозможно.

**Как снизить риски мошенничества?**

- Необходимо ограничить доступ к компьютеру, используемому для работы с системой дистанционного банковского обслуживания и запретить допуск посторонних лиц для совершения операций в системе от Вашего имени.

- Хранить Ваши секретные данные только на специализированных защищенных носителях (токенах или смарт-картах).

- Использовать средства дополнительной визуализации платежных поручений

Для исключения случаев мошенничества при удаленном доступе к Вашим счетам в РОСКОМСНАББАНК (ПАО) мы рекомендуем использовать средства визуализации подписываемых данных SafeTouch, позволяющие контролировать основные реквизиты платежных документов в доверенной среде.


**SafeTouch – считыватель смарт-карт и токенов, позволяющий визуально контролировать содержание передаваемых на подпись в смарт-карту данных, путем вывода их на дисплей.**

**Безопасность**

- SafeTouch не позволяет подписать документ до тех пор, пока не будет нажата кнопка подтверждения операции подписи на устройстве.

**Удобство**

- Быстрый просмотр подписываемых данных и подтверждение подписи одной кнопкой позволяет максимально быстро и удобно подтвердить верность подписываемых данных.

**Совместимость**

- SafeTouch не требует установки драйверов и дополнительного программного обеспечения в современных операционных системах.

**Часто задаваемые вопросы о SafeTouch**

**1. Неужели сейчас наша система настолько незащищенная, что нужна такая вещь?**

Ваша система защищена надежно, однако, если на компьютере клиента работает вредоносная программа (вирус), она выводит на монитор "поддельную" информацию о реквизитах проводимых документов. Соответственно, бухгалтер просто не видит, что он подписывает. Это атака на операционную систему компьютера, а не на систему Интернет-банкинга.

*Примечание: Мошенники часто заражают такими вирусами "целевые" сайты, например www.glavbukh.ru, www.banki.ru и т.д. Соответственно, каждый, кто зашел на зараженный сайт, очень сильно рискует всеми деньгами на своем счете. Антивирусные программы от таких вирусов практически не помогают.*

**2. Как, собственно, работать с SafeTouch?**

SafeTouch не вносит никаких изменений в работу бухгалтера с системой. Единственная операция, которая добавляется - проверка реквизитов на дисплее устройства и нажатие кнопки подтверждения операции.

**3. SafeTouch нужно присоединять к компьютеру?**

Да, SafeTouch подключается к компьютеру через USB-кабель (идет в комплекте).

**4. Как SafeTouch «присоединяется» к Интернет-Банку?**

SafeTouch стоит "между" системой Интернет-банкинга и смарт-картой/токеном, в которой подписывается документ после нажатия кнопки "подписать". Для самой системы Интернет-банкинга SafeTouch выглядит как обычная смарт-карта/токен.

**5. Как SafeTouch проверяет документы?**

SafeTouch выводит на экран основные реквизиты платежного (или иного) документа, который направляется из системы Интернет-банкинга на подпись в смарт-карту/токен. Логика того, какие реквизиты выводить, задается самой системой ДБО.

**6. SafeTouch работает только со Смарт-картой?**

Нет, по желанию клиента ему может быть выдана версия Safetouch с поддержкой токена.

**7. Что хранится на Смарт-карте/токене, какая информация?**

На смарт-карте/токене хранится ключ электронной подписи (ЭП) клиента. Этот ключ нельзя скопировать или извлечь из смарт-карты/токена. При нажатии кнопки "подписать", платежка направляется в смарт-карту/токен, там подписывается, а затем результат подписи передается обратно в систему.

*Примечание: Смарт-карта и токен, это одно и то же устройство, только в разных форм-факторах. Токен, это по сути маленький USB-считыватель смарт-карт и чип смарт-карты в одном корпусе.*

**8. Как использовать Смарт-карту/токен для входа в Интернет-банк?**

Для входа в систему Интернет-банк используется ключ ЭП, который находится на смарт-карте/токене. В таком случае SafeTouch может также подтверждать операцию входа в систему. Для пользователя это выглядит следующим образом:

- запустить систему Интернет-банк

- вставить смарт-карту/токен с ключом ЭП в SafeTouch

- ввести PIN-код для смарт-карты/токена

- на SafeTouch выводится сообщение о попытке входа в систему

- нажать кнопку подтверждения операции

*Примечание: Этот функционал очень полезен, так как пользователи часто оставляют подключенный токен (смарт-карту) и уходят, оставляя рабочее место без присмотра. В этот момент хакер легко может удаленно подключиться к компьютеру и провести свой платеж. В случае с SafeTouch, хакер не сможет даже войти в систему ДБО, так как для этого надо нажать кнопку на устройстве.*

**9. Где гарантия, что SafeTouch тоже не обманут/не взломают?**

Программное обеспечение SafeTouch нельзя изменить со стороны компьютера. Прошивка устройства осуществляется только на производстве. Украсть деньги могут только в том случае, если бухгалтер не проверяет реквизиты, которые выводятся на дисплей SafeTouch и подтверждает все документы подряд.

**10. SafeTouch в сравнении с уже существующей системой: что он дает дополнительно?**

Главное преимущество SafeTouch: он не меняет привычной схемы работы бухгалтера с системой Интернет-банк. При этом пользователь видит реальные реквизиты подписываемых документов, а не то, что ему "подсовывает" недоверенная операционная система.

**11. Клиенты могут сказать: «Мы и так не допускаем посторонних лиц к совершению операций и используем специализированный защищенный носитель – токен».**

Да, токен повышает безопасность использования системы Интернет-банк. Однако, хакеры могут удаленно подключиться к компьютеру клиента и провести свой документ незаметно для него, либо просто подменить реквизиты и сумму легальной платежки, которую пользователь отправил на подпись в токен. Основной тезис: "Без SafeTouch Вы не видите, что подписываете"

**12. Получается, что SafeTouch – это только средство «дополнительной визуализации платежных поручений»?**

Кроме визуализации платежных поручений, SafeTouch блокирует все попытки подписания документа удаленным пользователем, который не может физически нажать на кнопку подтверждения операции. В данном случае мы защищаемся от всех мошенников (хакеров), которые не имеют доступа в кабинет бухгалтера.