ПАМЯТКА
О ВОЗМОЖНЫХ РИСКАХ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ООО «БАНК СТАНДАРТ-КРЕДИТ»

ООО «Банк Стандарт-Кредит» (далее – Банк) предлагает Вашему вниманию информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемые меры по снижению этих рисков.

Компрометация ключей ЭЦП – факт доступа постороннего лица к информации, содержащей (закрытый) ключ электронной цифровой подписи (далее – ЭЦП), а также подозрение на него.

Ключ может быть скомпрометирован в следующих ситуациях:

- физическая утеря носителя информации, на котором хранится файл ключа ЭЦП;
- передача файла ключа ЭЦП по открытым каналам связи (т.е. без использования шифрования);
- несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место (срабатывание сигнализации, повреждение устройств контроля несанкционированного доступа (слепков печатей), взлом учётной записи пользователя и т.п.);
- сознательная передача информации постороннему лицу;
- перехват информации вредоносным программным обеспечением (компьютерными вирусами, троянскими программами).

Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации при утрате или компрометации устройства, с использованием которого клиентом осуществлялся перевод денежных средств (компьютер, USB-flash, USB-токен и т.п.)

Рекомендуется выполнять следующие меры для снижения риска несанкционированного доступа к защищаемой информации:

- для работы с системой «Клиент-Банк» используйте отдельный компьютер, доступ к которому имеют только лица, осуществляющие платежи в системе «Клиент-Банк»;
- на компьютере, с которого осуществляется работа в системе «Клиент-Банк», используйте только лицензионное системное и прикладное программное обеспечение (далее – ПО), оперативно его обновляйте;
- не реже 1 раза в день осуществляйте проверку компьютера, на котором установлено ПО «Клиент-Банк» на наличие вредоносных программ при помощи установленных средств антивирусной защиты;
- в качестве хранилища ключей ЭЦП используйте USB-токен. Использование USB-токена позволяет существенно снизить вероятность хищения ключей ЭЦП злоумышленниками, т.к. ключи с USB-токена не возможно скопировать;
- при использовании двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи и ключ ЭЦП главного бухгалтера с правом второй подписи) осуществляйте работу с системой «Клиент-Банк» на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах;
- не передавайте ключ ЭЦП третьим лицам (т.к. электронные документы, заверенные ЭЦП юридически эквивалентны документам на бумажном носителе, заверенным подписями лиц из карточки с образцами подписей и оттиска печати);
- не храните на устройстве, с использованием которого клиентом осуществлялся перевод денежных средств, (компьютер, USB-flash и т.п.) пароль от входа в систему «Клиент-Банк»;
- в случае возникновении подозрения на наличие вредоносных программ выполняйте «Рекомендации клиентам по организации антивирусной защиты информации».

В случае компрометации или подозрения на компрометацию ключа ЭЦП необходимо незамедлительно связаться с сотрудником операционно-клиентского отдела Банка по телефону **+7 (87778) 5-18-50** или **+7 (495) 600-37-61 (филиал в г. Москва)** и сообщить о компрометации ключа ЭЦП и заблокировать его, указав блокировочное слово (задаётся при первичной регистрации Клиента в системе «Клиент-Банк»). При этом блокировка ключей ЭЦП производится сроком на один рабочий день и аннулируется в случае непредставления за это время письменного заявления Клиента, заверенного его подписью и печатью организации. Клиент в любое время может блокировать или полностью прекратить действие своего ключа (ключей) ЭЦП и зарегистрировать новый ключ ЭЦП. При этом во всех случаях блокировка или отмена каждого ключа ЭЦП производится на основании письменного заявления Клиента, заверенного его подписью и печатью организации.

Информация для клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации путем использования ложных ресурсов сети Интернет

При осуществлении переводов денежных средств в платежных сервисах существует риск получения несанкционированного доступа к защищаемой информации (персональные данные, контакты и т.п.) использования ложных ресурсов сети Интернет лицами, не обладающими правом распоряжения этими денежными средствами, т. е. злоумышленниками. В указанном случае злоумышленник может создавать сайт-копию сайта, например, с именем ibank2.stkbank.com, тогда как адрес подлинного сайта ibank2.stkbank.ru. При этом сайт-копия будет выглядеть как сайт платежного сервиса, но при вводе данных (персональных данных, контактов и т.п.), они будут отправляться

злоумышленнику. Попадание на такой сайт-копию возможно, например, с различных внешних ссылок, на которых установлена переадресация на сайт злоумышленника.

С целью снижению указанного риска, защиты от него, а также защиты от вредоносного кода рекомендуется выполнять следующие действия:

- переходите на сайт, набрав его название собственноручно в адресной строке;
- после перехода на сайт по ссылке (прежде чем ввести имя и пароль) проверяйте подлинность сайта по данным SSL-сертификата (в адресной строке около названия сайта будет отображен значок закрытого замочка зеленого цвета; чтобы увидеть детали SSL-сертификата, необходимо сделать двойной щелчок мыши по закрытому замочку);
- проверяйте информацию о предыдущем сеансе работы при каждом входе на сайт (дату последнего посещения сайта и т.п.);
- не переводите денежные средства по просьбам, озвученным по телефону, присланным в sms-сообщениях, в сообщениях из социальных сетей, а также людям, которые обещают различные подарки, выигрыши, компенсации и п.т.;
- не используйте функции автозаполнения в настройках специализированных программ для просмотра веб-страниц в сети Интернет – браузера. Использование данной функции приводит к сохранению конфиденциальной информации (пароля и имени пользователя и др.) в памяти браузера, что в свою очередь может привести к использованию данных злоумышленниками. Регулярно удаляйте случайно сохраненные в памяти браузера пароли и имена пользователя;
- храните пароль от входа в платежный сервис отдельно, в недоступном для посторонних лиц месте. Не храните пароль в компьютере. Записав пароль, не делайте комментариев к записи. Не используйте в качестве пароля имена и фамилии родственников и знакомых, элементы адреса местожительства и памятных дат, клички животных и другие простые и известные окружающим слова и словосочетания. Используйте пароль не короче 6 символов, включающий бессмысленное сочетание букв и цифр. Меняйте пароль не реже 1 раза в месяц.

Рекомендации клиентам по организации антивирусной защиты информации

Соблюдайте ограничение по физическому доступу к данному компьютеру. Любой компьютер, с которого осуществляется выход в сеть Интернета, подвержен риску заражения вирусом (вредоносный код, способный нарушить целостность используемой информации, что приведет к сбоям компьютера из-за ошибок, к краже персональной информации и т.п.), поэтому рекомендуется придерживаться следующих правил безопасной работы в сети Интернет:

- не работайте со съёмными носителями других систем и компьютеров, которые ранее были заражены вирусом;
- не посещайте непроверенные и небезопасные сайты (возможна непреднамеренная загрузка на свой компьютер вирусов и шпионских программ);
- не скачивайте информацию из сети Интернета на диск своего компьютера;
- не нажимайте на всплывающие окна, содержащие рекламу;
- не открывайте вложения и не переходите по ссылкам при получении электронного сообщения с неизвестным вложением или со ссылкой на неизвестный ресурс сети Интернет;
- не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных, ни при каких обстоятельствах не сообщайте свой пароль никому, включая людей, представляющихся сотрудниками Банка;
- максимально ограничьте использование Интернет-пейджеров (ICQ, Skype и т.п.) на данном компьютере;
- будьте внимательны к странным и непонятным сообщениям и поведению системы (нетипичная работа ПО, появление графических и звуковых эффектов, искажение данных, исчезновение файлов, частое появление сообщений об ошибках, замедление работы компьютера и сети и т.п.);
- не используйте непроверенное и неизвестное ПО (такое ПО может быть мошенническим и провоцировать на выполнение действий, нужных мошенникам: устанавливать вредоносное ПО для кражи персональных данных; отображать всплывающие окна с ложными уведомлениями об угрозах; снижать производительность компьютера, повреждать файлы; отключать обновления операционной системы или антивирусных программ; блокировать посещение веб-сайтов разработчиков антивирусных программ и др.).

Рекомендуется осуществлять проверку компьютера на наличие вредоносных программ при помощи лицензионных антивирусных программ (программы, которые способны находить, лечить, а также полностью удалять вирусы из системы, а также моментально предупреждать о том, что на той или иной странице Интернета есть вирус и система может быть им заражена): Антивирус Касперского, Dr. Web и др. Используйте и оперативно обновляйте антивирусное ПО.

Не рекомендуется использовать программы «scareware», которые являются ложными антивирусами (программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции).

Разработчики ложных антивирусов создают специальные рекламные окна, которые выглядят так, как будто они рекламируют лицензионное ПО для обеспечения безопасности или его обновления. Их можно увидеть при посещении различных веб-ресурсов. В «сообщениях» таких окон предлагается выполнить некоторое действие, например, установить программу, загрузить рекомендуемые обновления и т.д. Если щелкнуть по такому объявлению, на компьютер будет загружен и установлен ложный антивирус. Защитой от ложных антивирусов является использование лицензионного антивирусного ПО, и его регулярное обновление.