БАНК КУЗНЕЦКИЙ
440000, г. Пенза, ул. Красная, 104, тел./факс (8412) 23-22-23 / 23-18-40
e-mail: info@kuzbank.ru, www.kuzbank.ru

Приложение №3

Рекомендации Банка по снижению рисков осуществления перевода денежных средств без согласия клиента при работе юридических лиц в системе дистанционного банковского обслуживания (далее ДБО)

Уважаемые клиенты!

Официальный номер контактного центра ПАО Банк «Кузнецкий»: 8-800-100-64-10.

В целях выполнения требований Федерального закона от 27.06.2011г. №161-ФЗ «О национальной платежной системе» ПАО Банк «Кузнецкий» (далее-Банк) доводит до клиентов информацию о существующих рисках получения злоумышленниками несанкционированного доступа к защищаемой информации клиентов с целью хищения денежных средств клиентов, а также дает рекомендации по снижению данных рисков.

Соблюдение данных рекомендаций позволит обеспечить максимальную сохранность Ваших денежных средств, а также снизит возможные риски при осуществлении платежей в пользу поставщиков услуг, при переводах денежных средств как внутри Банка, так и в другие кредитные организации.

Использование системы ДБО потенциально несет в себе риски неблагоприятных последствий, связанных с хищением денежных средств.

Основным риском при использовании системы ДБО является риск получения злоумышленником несанкционированного доступа к управлению счетом клиента и к документам клиента, передаваемым в Банк через систему ДБО.

Последствиями несанкционированного доступа могут быть списание денежных средств со счета клиента без его добровольного согласия или утечка конфиденциальной информации о совершаемых клиентом операциях.

Под Переводом без добровольного согласия клиента понимаются операции перевода денежных средств, осуществляемые без согласия Плательщика или с согласия Плательщика, полученного под влиянием обмана или при злоупотреблении доверием, с учетом установленных Банком России признаков осуществления перевода денежных средств без согласия клиента (к которым в том числе относятся Переводы, осуществляемые в адрес Получателя, сведения о котором (или об ЭСП которого) совпадают с информацией, содержащейся в базе данных Банка России о случаях и попытках осуществления Перевода без добровольного согласия клиента) (далее по тексту – Перевод(ы) без добровольного согласия клиента).

Основными способами несанкционированного доступа к системе ДБО являются:

- перехват злоумышленником управления компьютером, мобильным устройством Клиента;
- кража логина и пароля Клиента для входа в систему ДБО;
- перехват данных, передаваемых Клиентом в Банк и получаемых Клиентом из Банка.

Получение несанкционированного доступа может быть осуществлено:

- злоумышленниками, получившими доступ к компьютеру, мобильному устройству Клиента через сеть Интернет или иные каналы связи;
- третьими лицами, имеющими физический доступ к компьютеру, мобильному устройству Клиента.

Признаки несанкционированного использования рабочего места Клиента, предназначенного для работы в системе ДБО:

- в истории Распоряжение на перевод денежных средств в системе ДБО указаны Распоряжения, которые Вы не совершали;
- подозрительная активность на компьютере, с которого осуществляется работа (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.);

- осуществление запроса на ввод разового пароля для подтверждения выполнения действий, не связанных с входом в систему ДБО или совершением операций (подтверждение ознакомления с какими-либо правилами, инструкциями, или для подтверждения входа в какой-либо раздел системы);
- входящий звонок от лиц, представляющихся работниками ПАО Банк «Кузнецкий» уведомляющих Вас о регламентных/восстановительных работах в системе ДБО или Банке;
- получение сообщения о блокировке/разблокировке доступа в систему ДБО;
- изменение адреса в адресной строке браузера при работе с системой ДБО;
- обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время);
- невозможность получения доступа к системе ДБО по причине несовпадения пароля при введении заведомо верного пароля;
- "зависание" системы ДБО при одновременной нормальной работе других интернет-ресурсов.

Данный перечень признаков несанкционированного использования системы ДБО не является исчерпывающим. В зависимости от новых видов атак список может дополняться или корректироваться.

В целях минимизации рисков при использовании системы ДБО Банк просит клиентов для обеспечения безопасности их денежных средств соблюдать следующие рекомендации:

- для входа в систему ДБО вам требуется вводить только ваш логин и пароль;
- никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в систему ДБО или для подтверждения платежей, даже работникам банка;
- обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS-сообщении указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему Счету платеж, ни в коем случае не вводите его в системе ДБО и не называйте его, в том числе сотрудникам Банка;
- в случае утери мобильного телефона, на который приходят SMS-сообщения с разовым паролем, немедленно заблокируйте (замените) SIM-карту;
- запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете системы ДБО вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону;
- используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным ПО и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры;
- при вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке системы ДБО должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя, так как они будут переданы в отрытом (незашифрованном) виде и могут быть перехвачены;
- используйте виртуальную клавиатуру для ввода пароля;
- будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!;
- при работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора;
- не давайте разрешения неизвестным программам выходить в Интернет;
- при работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от непроверенных издателей;

- должно быть исключено подключение переносного компьютера(ноутбука), мобильного устройства к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.);
- включенный компьютер мобильное устройство не должны оставаться без контроля. Не отлучаться от компьютера, мобильного устройства пока происходит сеанс связи с Банком. Время до автоматической блокировки экрана во время бездействия пользователя должно составлять не более 3 минут. Разблокировка экрана должна происходить по паролю;
- на компьютере, мобильном устройстве должна быть установлена парольная защита на вход в систему ДБО;
- при выборе пароля необходимо соблюдать следующие требования:
  - длина пароля должна быть не менее 8 символов;
  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
  - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, девичью фамилию матери наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- пароль доступа необходимо менять каждые 3 месяца;
- строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам;
- для хранения ключей ЭП следует использовать отчуждаемые носители eToken, ruToken, jaCarta. Не использовать для хранения ключей ЭП флэш-накопители или жесткий диск компьютера;
- следует отключать, извлекать носители с ключами ЭП, если они не используются для работы;
- носители ключевой информации вне сеансов связи рекомендуется хранить в сейфе или другом, недоступном для посторонних лиц месте, хранить в тайне логин, пароль для входа в Систему ДБО и пароль от ключевого носителя;
- хранить ключевой носитель необходимо в защищаемой комнате, в сейфе, исключающим доступ неуполномоченных лиц и повреждение материального носителя. Вся ответственность за конфиденциальность секретных ключей Клиента лежит на Клиенте, как на единственном владельце секретных ключей ЭЦП/ЭП;
- сменный носитель с ключевой информацией должен использоваться только владельцем сертификата ключа либо лицом, уполномоченным на использование такого сменного носителя;
- не допускается:
  - снимать несанкционированные копии с носителей ключевой информации;
  - передавать носители ключевой информации лицам, к ним не допущенным;
  - записывать на носители ключевой информации постороннюю информацию.
- Необходимо обеспечить регулярное получение, доведение до уполномоченных лиц и исполнение рекомендаций и требований по вопросам безопасности, включая изучение рассылки Банка по вопросам защиты информации, от воздействия вредоносного кода, о возможных рисках и мерах по их снижению, в том числе информации о:
  - рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств;
  - рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;
  - появлении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения

БАНК КУЗНЕЦКИЙ
440000, г. Пенза, ул. Красная, 104, тел./факс (8412) 23-22-23 / 23-18-40
e-mail: info@kuzbank.ru, www.kuzbank.ru

- отправление переводов денежных средств следует производить только с использованием идентификационной информации, используемой для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств, которой в зависимости от технической возможности является IP-адрес и (или) иной идентификатор устройства.
- не допускать при использовании носителей секретных ключей их несанкционированного копирования.
- соблюдать требования информационной безопасности при работе в Системе дистанционного банковского обслуживания и рекомендации Банка.
- при увольнении ответственного работника или работника технической поддержки, имевшего доступ к ключам электронной подписи необходимо позвонить в Банк с уведомлением о приостановлении использования ключей электронной подписи, а также последующем перевыпуске ключей электронной подписи на новых работников; убедиться в отсутствии вредоносных программ на АРМах, задействованных в работе сервиса ДБО Банка;
- при возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно заблокировать ключи ЭП;

При возникновении подозрений в осуществлении несанкционированных операций в системе ДБО, несанкционированного доступа к компьютеру, мобильному устройству, либо при компрометации пароля, разового пароля на вход в систему ДБО следует:

- выйти из системы ДБО;
- заблокировать устройства, используемые для работы в системе ДБО (в том числе, выключить/перевести компьютер в режим сна;
- обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в системе ДБО;
- в письменном заявлении описать обстоятельства компрометации пароля, разовых паролей, несанкционированного доступа, либо другую информацию по фактам, вызвавшим подозрения;
- возобновление доступа в систему ДБО производится в офисе Банка при личном обращении Клиента.

Пожалуйста, будьте бдительны и внимательны.
Всегда помните: за все свои действия несете ответственность только Вы!