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 №1**

**Рекомендации Банка по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия**

**Уважаемые клиенты!**

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.

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).

Несанкционированный перевод денежных средств может проводиться вследствие заражения электронного устройства (далее -ЭУ) клиента вредоносным программным обеспечением (далее – ВПО) или посредством удалённого доступа к устройствам клиента.

Заражение ЭУ клиента осуществляется через спам-рассылку SMS или MMS-сообщений, сообщений электронной почты, содержащие ссылки на внешние ресурсы, или при переходе по ссылкам на ресурсы сети Интернет. При переходе по таким ссылкам ВПО устанавливается на ЭУ клиента. Также внедрение ВПО на устройства клиентов производится с использованием вирусных программ, массово распространяемых в сети Интернет через взломанные сайты, социальные сети и другие сетевые сервисы, свободно распространяемое ВПО и пр. Через сайты российских и международных социальных сетей и через рекламно-баннерные сети, распространяется наибольшее количество вредоносных программ.

ВПО может обладать различными возможностями, в том числе:

- формировать и отправлять от имени клиента распоряжения на перевод денежных средств, в том числе в виде SMS-сообщений на «короткие номера»;
- формировать и отправлять от имени клиента распоряжения на перевод денежных средств с использованием приложений, предназначенных для оплаты товаров и услуг;
- перехватывать сообщения с кодами подтверждения, приходящие на ЭУ в целях подтверждения операции.

Наибольший риск таких операций связан с тем, что в ряде случаев ВПО скрывает от клиента приходящие от Банка или оператора связи уведомления о списании денежных средств. Таким образом, клиент, не зная о несанкционированной операции с его денежными средствами, не может направить в Банк в определённые законодательством сроки уведомление о факте перевода денежных средств без его согласия.

Обращаем Ваше внимание на следующие случаи повышенного риска при переводе денежных средств:

- использование для перевода денежных средств устройств, предназначенных для доступа через сеть Интернет в вирусно-опасные ресурсы, такие как социальные сети, другие сетевые сервисы, включая электронную почту;
- наличие на устройстве, предназначенном для перевода денежных средств, вредоносного программного ПО, программ удаленного доступа к ресурсам устройства либо свободно распространяемого ВПО;

- отсутствие на устройстве, предназначенном для перевода денежных средств антивирусных баз, либо их нерегулярное обновление;
- хищение носителей информации и/или объектов, используемых при переводе денежных средств или несанкционированное копирование данных;
- нерегулярная проверка входящих документов.

Также злоумышленники, используя методы социальной инженерии (представившись сотрудниками Банка, оператором связи), могут обманом вынудить клиента сообщить данные для проведения операции – коды доступа, коды SMS-подтверждения и осуществить с использованием таких сведений несанкционированные операции.

В случае обнаружения списания денежных средств необходимо незамедлительно, но не позднее дня, следующего за днем получения от Банка уведомления о совершении операции, обратиться в Банк.

**Следует учитывать следующие рекомендации для снижения риска хищения денежных средств:**

- не следует сообщать посторонним лицам свою персональную информацию (ФИО, реквизиты ЭСП, логин, пароль, номер карты, счета, паспорта и т.д.). Сотрудник Банка имеет право уточнять у клиента подобную информацию только в случае, если клиент самостоятельно обратился в Банк;
- не забывайте актуализировать номер телефона и другие данные. Если у сотрудников банка будут устаревшие данные, они не смогут оперативно связаться с вами для уточнения информации, также необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время;
- не оставляйте ЭУ без присмотра при работе в системе по осуществлению переводов денежных средств. Ограничьте доступ посторонних лиц к компьютеру, с которого осуществляется переводы денежных средств. Установите пароль на доступ к ЭУ и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к ЭУ в случае его утраты;
- извлекайте носители ключевой и парольной информации с ключами электронной подписи, при завершении работы с сервисом ДБО Банка;
- исключите использование сервиса ДБО Банка на гостевых автоматизированных рабочих местах (далее - АРМ), а также исключите посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения;
- на АРМах, задействованных в работе сервиса ДБО Банка, используйте исключительно лицензионное программное обеспечение или свободно распространяемое программное обеспечение, загруженное с официальных сайтов, а также обеспечьте их своевременное обновление;
- используйте лицензионные средства антивирусной защиты, регулярно обновляйте антивирусные базы. Вирусы: открывают удаленный доступ к вашему устройству, крадут логины и пароли от онлайн- и мобильного банка, перехватывают секретные коды из сообщений. Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов;
- исключите обслуживание ЭУ случайными работниками технической поддержки, а также обеспечьте контроль за их действиями;
- не рекомендуется записывать код доступа там, где доступ к нему могут получить посторонние лица (включая незаблокированное ЭУ);
- пароль доступа меняйте не реже одного раза в квартал. Помните, что в случае раскрытия пароля доступа существует риск совершения неправомерных действий с Вашими денежными средствами со стороны третьих лиц.

При создании паролей придерживайтесь следующих правил:

Не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы. Пароль должен 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, год рождения, номер телефона и т.п.);

- 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;

- не проводите действия по указанию или по рекомендациям третьих лиц, не сообщайте им результаты своих действий в Интернет-банке/Мобильном банке и банкоматах Банка (не сообщайте любую цифровую или буквенную информацию) третьим лицам, в том числе представляющимся сотрудниками правоохранительных органов, операторами сотовой связи, работниками банков;
- в некоторых случаях мошенниками используются технологии подмены отображаемого на экране номера телефона при входящем звонке. Если Вы сомневаетесь, что входящий звонок осуществляется работником Банка, завершите разговор и самостоятельно перезвоните в Банк по номеру телефона, указанному на официальном сайте Банка или на обратной стороне платежной карты;
- регулярно контролируйте состояние Ваших счетов, незамедлительно сообщайте работникам Банка о несанкционированных операциях;
- при возникновении вопросов о безопасном использовании банковских услуг обратитесь за разъяснением в любое отделение Банка или по номеру телефона, указанному на официальном сайте Банка/на обратной стороне платежной карты;
- сообщите своим коллегам, а также родным и близким рекомендации о противодействии мошенничеству;
- в случае если имеются предположения о раскрытии пароля доступа, Ваших персональных данных, позволяющих совершить неправомерные действия с использованием системы, необходимо немедленно обратиться в Банк и следовать указаниям сотрудника Банка.

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

**Пожалуйста, будьте бдительны и внимательны -безопасность Вашей финансовой информации в Ваших руках!**

**Риски и последствия вовлечения в дропперство.**

Существуют схемы вывода денежных средств при сотрудничестве с мошенниками и становлении дроппером.

Дропперами становятся люди, которые верят, что могут быстро и легко заработать, они остро нуждаются в деньгах, поэтому соглашаются на любую работу. Мошенники часто звонят тем, кто ранее уже «попадался на их уловки». В группе риска находятся студенты, жители небольших населенных пунктов, приехавшие в крупные города, люди, находящиеся в трудном финансовом положении, иммигранты, уязвимые слои населения (многодетные семьи, пенсионеры, безработные).

Мошенники звонят человеку под видом:

- органов государственной безопасности с предложением официально устроится на работу по поиску преступников и обещают ежемесячный доход. Если человек соглашается, то мошенники переводят на его банковскую карту похищенные деньги и затем требуют снять эти деньги в банкомате;
- сотрудников банка с предложением вывести деньги с «замороженного счета» на «безопасный»;
- работодателя с рекламой предложения о работе, связанной с переводом и обналичиванием денежных средств;
- человека, который ошибся. Мошенники «случайно» переводят денежные средства, потом просят их вернуть наличными или переводом на карту.

Схема вывода денежных средств:

Дроп – заливщик получает деньги от злоумышленника, вносит их на свой счет и затем переводит другим дропам ➲

Дроп – обнальщик обналичивает поступившие ему деньги, при этом оставляя часть себе как «вознаграждение», а оставшуюся часть передает третьему лицу ➲

Дроп – транзитник перечисляет денежные средства на карту или электронный кошелек и оставляет часть себе как «вознаграждение».

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

Мошенники часто используют в своих схемах безналичные переводы. Они предлагают Вам регулярно получать на свою карту деньги, а потом переводить их иным лицам. По такой схеме через Ваш банковский счет (карту) будут идти «транзитные» переводы. ЭТО ОПАСНО!

Злоумышленники часто используют интерес к криптовалюте с целью сделать Вас дроппером.

БУДЬТЕ БДИТЕЛЬНЫ!

Преступники могут выслать QR-коды для «спасения» Ваших денег. НЕ ПЕРЕВОДИТЕ ДЕНЬГИ ПО СОМНИТЕЛЬНЫ QR-КОДАМ!

Таким образом, при сотрудничестве с мошенниками и становлении дроппером человек несет наказание по уголовным статьям Российской Федерации за мошенничество и легализацию (отмывание) денежных средств. Если есть подозрение, что Вас используют в дропперстве, уведомите полицию, Банк России и ПАО Банк «Кузнецкий».

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

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