НАРОДНЫЙ ДОВЕРИТЕЛЬНЫЙ БАНК

Рекомендации для клиентов по снижению рисков осуществления перевода денежных средств без согласия клиента

В целях выполнения требований Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Методических рекомендаций Банка России от 19.02.2021г. № 3-МР «По усилению кредитными организациями информационной работы с клиентами в целях противодействия несанкционированным операциям», а также Письма Центрального Банка Российской Федерации от 15 апреля 2022 г. № 01-56-5/3143 «О реализации кредитными организациями мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента» АО «НДБанк» (далее - Банк) доводит до своих 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.

К операциям по переводу денежных средств, совершаемым без согласия клиента, могут относиться (включая, но не ограничиваясь):

- операции по оплате товаров и услуг через сеть Интернет с использованием электронного устройства клиента (компьютер, электронный планшет, смартфон, мобильный телефон, далее – ЭУ) в том числе по реквизитам электронного средства платежа (ЭСП) клиента;
- операции по переводу денежных средств, предоставленных клиентом оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;
- операции, осуществляемые с использованием системы дистанционного банковского обслуживания, предоставляемой Банком/партнёром Банка (на основании заключённого договора) и установленной клиентом на ЭУ;
- операции по оплате товаров и услуг с использованием иных приложений, установленных на ЭУ клиента.

Несанкционированный перевод денежных средств может проводиться вследствие заражения 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, содержащих 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 устройств, предназначенных для перевода денежных средств, для доступа через сеть Интернет в вирусо-опасные ресурсы, такие как социальные сети, другие сетевые сервисы, включая почтовые клиенты;
- наличие на устройстве, предназначенном для перевода денежных средств, вредоносного ПО, программ удаленного доступа к ресурсам устройства либо свободно распространяемого ВПО;
- отсутствие на устройстве, предназначенном для перевода денежных средств, либо нерегулярное обновление антивирусных баз;
- использование неактуальных версий систем, используемых для перевода денежных средств;
- хищение носителей информации и/или объектов, используемых при переводе денежных средств или несанкционированное копирование данных;
- отсутствие контроля физического доступа к объектам, используемым при переводе денежных средств;
- нерегулярная проверка входящих электронных документов.

Также злоумышленники, используя методы социальной инженерии (представившись сотрудниками Банка, оператора 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 или от оператора связи уведомления о совершении операции, обратиться в Банк или к оператору связи (если произошло списание денежных средств, предоставленных оператору связи в оплату услуг связи, в том числе перечисление денежных средств на «короткие номера»).

Клиентам следует учитывать следующие рекомендации для снижения риска хищения денежных средств:

1. 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.
2. В случае утери ЭУ необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи.
3. В случае изменения номера телефона нужно обратиться в Банк для изменения телефонного номера, по которому осуществляется доступ к сервисам Банка. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время.
4. Если у Вас неожиданно перестала работать SIM-карта – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как это может быть одним из признаков, совершаемых в отношении Вас третьими лицами мошеннических действий.
5. Для перевода денежных средств используйте защищенные ЭУ – не пытайтесь обходить установленные производителем ЭУ программные средства защиты. Не перепрошивайте свое ЭУ программным обеспечением сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению ВПО.
6. Не допускается работать на ЭУ и осуществлять переводы денежных средств через публичные беспроводные сети (free Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через оператора мобильной связи (3G, 4G) или через доверенную защищенную беспроводную сеть.
7. 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.).

8. Необходимо хранить код доступа в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать код доступа там, где доступ к нему могут получить посторонние лица (включая незаблокированное ЭУ).

9. Не сообщать код доступа, SMS-коды, необходимые для проведения операций, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карты (CVV/CVC-код) посторонним лицам, сотрудникам Банка, банка-эмитента карты по телефону, электронной почте или иным способом. При возникновении подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Банка.

10. Не оставляйте ЭУ без присмотра. 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.

11. Необходимо применять на ЭУ лицензионные средства антивирусной защиты, работающие в автоматическом режиме, и регулярно в рекомендуемые разработчиками сроки проводить их обновление.

12. Отключение или несвоевременное обновление антивирусных средств, установленных на ЭУ не допускается. В случае обнаружения на ЭУ нештатного отключения антивирусных средств – не допускается работа на ЭУ и осуществление перевода денежных средств до устранения причины нештатного отключения.

13. Необходимо осуществлять проверку ЭУ на наличие ВПО перед началом работы, а также после доступа к Вашему ЭУ сотрудников технической поддержки различных организаций или любых других частных мастеров, выполнивших работу по установке, обновлению и поддержке различных программ.

14. Необходимо на постоянной основе регулярно, например, ежемесячно, проводить полную проверку ЭУ, на котором производиться переводы денежных средств, на наличие ВПО.

15. Не рекомендуется передавать ЭУ для использования третьим лицам, в том числе родственникам, т.к. на оставленном без присмотра ЭУ может быть совершён ряд действий, направленных на получение доступа к персональным данным, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карты (CVV/CVC-код) и иные данные. Например, злоумышленник может установить ВПО, настроить переадресацию SMS-сообщений на другое устройство и т.п.

16. Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях из недостоверных источников, в том числе на известные сайты, а также загружать и устанавливать на ЭУ программное обеспечение из недостоверных источников.

17. Будьте внимательны при получении писем или смс-сообщений якобы от имени Банка. Основные признаки, того, что сообщение отправлено мошенниками:

- ссылка, указанная в сообщении, не содержит названия Банка, либо содержит его в искаженном виде;
- запрашиваемые в сообщении действия требуют Вашего срочного ответа или принятия немедленного действия (ваш счет будет заблокирован);
- в сообщении требуется предоставить, обновить или подтвердить Ваш логин и пароль к системам дистанционного банковского обслуживания (в случае использования их Клиентами);
- содержит информацию, что на Ваш счет поступили денежные средства, которых Вы не ожидали.

18. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах не сообщать данную информацию. Банк никогда не запрашивает у клиентов персональные данные.

19. При общении с сотрудниками Банка пользуйтесь только теми телефонами, которые указаны на сайте банка, либо получены Вами от сотрудников банка лично.

20. Следует регулярно проверять входящие электронные документы в электронной системе. В случае отсутствия регулярных проверок Вы можете не прочитать уведомление о совершенных переводах денежных средств и не отследить несанкционированные операции в случае их совершения.

21. Необходимо проводить контроль сумм и получателей платежных документов в информационном окне электронной системы при выходе на связь с Банком, а также контролировать количество и сумму отправленных документов по полученным от Банка квитанциям.

22. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать Банк обо всех подозрительных или несанкционированных операциях в соответствии с Договором. При установке порядка регулярного контроля рекомендуем принимать в расчёт, что переводы денежных средств, в отношение которых наступила безотзывность перевода денежных средств, не могут быть приостановлены.

23. В случае неожиданного выхода из строя устройства, либо пропадания на нём программного обеспечения, необходимо прекратить на устройстве работу, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно связаться с Банком для блокировки, запросить выписку по счету непосредственно в Банке. При обнаружении несанкционированных платежных операций написать заявление в Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. Работоспособность поврежденного устройства не восстанавливать до проведения технической экспертизы.

24. Появление на экране устройства во время отсутствия соединения с банком сообщений, провоцирующих на становление такого соединения, свидетельствует о наличии вредоносного ПО. В данной ситуации установление соединения с банком может привести к отправке фальшивого документа. При появлении подобного сообщения необходимо провести контроль платежных документов, находящихся в статусе - «Выгружен».

25. В случае если имеются предположения о раскрытии пароля доступа, Ваших персональных данных, позволяющих совершить неправомерные действия с их использованием, необходимо немедленно обратиться в Банк и следовать указаниям сотрудника Банка.

26. В случае если в процессе работы на ЭУ обнаружены какие-то не имевшие ранее места события (нештатные информационные окна, платежи, Вами не проводившиеся или не санкционированные, сообщения об ошибках, сообщения о неверном ключе доступа или пароле, и т.п.) зафиксируйте суть события, прекратите работу, выключить компьютер и незамедлительно уведомите о событии сотрудников Банка

Предупреждение:

При получении от Банка России в порядке, установленном Указанием Банка России от 08.10.2018 № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента» (далее - Указание № 4926-У), информации из базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента (далее - база данных), в том числе специального кода номера документа, удостоверяющего личность получателя средств по переводам денежных средств без согласия клиента, рекомендуется оценивать риск нарушения клиентами порядка использования электронного средства платежа (далее - ЭСП), в том числе риск передачи ЭСП третьим лицам. Оценка риска проводится Банком в отношении ЭСП, принадлежащих лицам, информация о специальном коде номера документа, удостоверяющего личность клиента - физического лица, которых включена в базу данных.

В случае выявления такого риска Банк имеет право с учетом требований части 9 статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» приостанавливать использование ЭСП указанными клиентами - физическими лицами с незамедлительным направлением клиенту уведомления.