Электронная почта

ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)
Волго-Вятское
главное управление
Отделение по Саратовской области
410029, г. Саратов, ул. Советская, 2
Тел. (845-2) 23-72-10, факс (845-2) 74-20-08
www.cbr.ru

от 22.04.2015 № 6-36/14690

на № от

Руководителю кредитной организации
Саратовской области

О направленнии информации о несанкционированных операциях

Уважаемые руководители!

Направляем Вам информацию, подготовленную Пресс-службой Банка России, о существующих рисках и о порядке использования устройств мобильной связи при осуществлении переводов денежных средств.

В рамках реализации пункта 2.12.3 Положения Банка России от 09.06.2014 № 382-П просим довести данную информацию до своих клиентов. При использовании материала ссылка на Пресс-службу Банка России обязательна.

Приложение на 3 листах.

Управляющий Отделением Е.А. Бирюкова

Батраев С.Р.
74-21-52

В.В. ГОЖАНСКИЙ
20.04.2015

Приложение к письму
Отделения Саратов
от 22 04.2015 № 6-36/14690

Пресс-центр
Центральный банк Российской Федерации (Банк России)
Пресс-служба
107016, Москва, ул. Неглинная, 12
www.cbr.ru

Информация
О несанкционированных операциях, совершенных с использованием устройств мобильной связи

Банк России отмечает участившиеся случаи осуществления переводов денежных средств с использованием устройств мобильной связи (смартфоны, телефоны, планшеты) без согласия их владельцев (далее — несанкционированные операции).

В частности, к таким несанкционированным операциям относятся:

операции по оплате товаров и услуг при осуществлении доступа к сети Интернет через устройство мобильной связи, в том числе по реквизитам платежных карт;

операции по переводу денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;

операции, осуществляемые с использованием приложений дистанционного банковского обслуживания (ДБО), предоставляемых кредитной организацией («Клиент-Банк») и установленных клиентом на устройстве мобильной связи;

операции по оплате товаров и услуг с использованием иных приложений, установленных на устройстве мобильной связи.

Несанкционированные операции проводятся вследствие заражения устройств мобильной связи вредоносными программами (в том числе вирусами), через спам-рассылку сообщений (sms-сообщений, сообщений электронной почты), содержащих ссылки на внешние ресурсы, или при переходе пользователя устройства мобильной связи по ссылкам на ресурсы сети Интернет. При переходе пользователя по таким ссылкам вирус устанавливается на устройство мобильной связи.

Вредоносные программы могут обладать различными возможностями, в том числе:

формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств, в том числе в виде смс-сообщений на «короткие номера»;

формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств с использованием приложений ДБО и иных приложений, предназначенных для оплаты товаров и услуг;

перехватывают одноразовые коды подтверждения, приходящие на мобильное устройство в целях дополнительного подтверждения операции.

Наибольший риск таких операций связан с тем, что в ряде случаев вредоносная программа скрывает от клиента приходящие от кредитной организации уведомления о списании денежных средств. Таким образом, пользователь мобильного устройства, не зная о несанкционированном списании с его банковского счета, не может направить в кредитную организацию в определенные законодательством сроки уведомление о переводе денежных средств без его согласия.

Дополнительно сообщаем, что распространенным случаем осуществления несанкционированных операций также является использование методов социальной инженерии, когда злоумышленники обманными действиями вынуждают клиента сообщить данные, необходимые для проведения операции, в том числе пароли, коды аутентификации и др.

Банк России рекомендует лицам, осуществляющим переводы денежных средств с использованием устройств мобильной связи, предпринимать следующие меры для минимизации рисков хищения денежных средств:

установить на устройство мобильной связи антивирусное программное обеспечение с регулярно обновляемыми базами;

не переходить по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты;

своевременно уведомлять кредитную организацию о смене номера телефона мобильной связи, который клиент предоставил кредитной организации для получения услуги «мобильный банкинг», в том числе, на который происходит информирование об операциях по счету клиента;

не скачивать на устройство мобильной связи приложения из непроверенных источников;

не передавать устройство мобильной связи и платежную карту для использования третьим лицам, в том числе родственникам;

не сообщать третьим лицам, в том числе сотрудникам кредитной организации, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платежной карте (CVV/CVC-код[1]), пароли от «Клиент-банка», одноразовые коды подтверждения; при наличии подозрения, что такие данные стали известны третьему лицу, необходимо

сообщить об этом кредитной организации по контактным данным, указанным на ее официальном сайте.

В случае обнаружения списания денежных средств необходимо в сроки, установленные законодательством РФ, обратиться в кредитную организацию или к оператору связи (если произошло списание денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»).

Банк России в рамках реализации пункта 2.12.3 Положения Банка России от 09.06.2014 № 382-П рекомендует кредитным организациям довести до своих клиентов информацию о существующих рисках и о порядке использования устройств мобильной связи при осуществлении переводов денежных средств.

[1] Трехзначные коды проверки подлинности банковской карты платежных систем Visa и MasterCard, наносимые на полосе для подписи держателя карты.

15 апреля 2015 года

При использовании материала ссылка на Пресс-службу Банка России обязательна.