**Рекомендации**
**по снижению рисков осуществления (повторного осуществления)**
**перевода денежных средств без добровольного согласия клиента**

АО «АБ «РОССИЯ» (далее – Банк) в целях выполнения требований Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и Методических рекомендаций Банка России от 28.02.2024 № 3-МР по усилению информационной работы, направленной на повышение осмотрительности клиентов в отношении сохранности информации, используемой в целях осуществления банковских операций, в частности перевода денежных средств, заключения договоров на получение кредитных (заемных) денежных средств, в том числе с использованием систем дистанционного банковского обслуживания, доводит до своих клиентов информацию о рисках получения злоумышленниками несанкционированного доступа к защищаемой информации клиентов с целью хищения денежных средств клиентов и дает рекомендации по снижению рисков осуществления (повторного осуществления) перевода денежных средств без добровольного согласия клиента.

К операциям по переводу денежных средств, совершаемым без добровольного согласия клиента, могут относиться операции, совершенные без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, в том числе с использованием методов социальной инженерии.

Мошенники, используя ***методы социальной инженерии*** (представившись сотрудниками Банка, оператора связи, органов внутренних дел и пр.), 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 обратиться в Банк.

Несанкционированный перевод денежных средств может проводиться вследствие заражения электронного устройства (компьютера, планшета, смартфона, мобильного телефона и пр.) (далее – ЭУ) клиента ***вредоносным программным обеспечением*** (далее – ВПО) или ***посредством удаленного доступа*** к ЭУ 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 в сети Интернет. ВПО устанавливается на ЭУ клиента при переходе по таким ссылкам или с использованием вирусных программ, массово распространяемых в сети Интернет через взломанные сайты, социальные сети и другие сетевые сервисы.

ВПО может обладать различными возможностями, в том числе управлять вашим ЭУ удаленно, демонстрировать информацию с экрана вашего ЭУ (в том числе логин и пароль к системе ДБО), формировать и отправлять от имени клиента распоряжения на перевод денежных средств, перехватывать сообщения с кодами подтверждения, приходящие на ЭУ в целях подтверждения операции, скрывать от Вас 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 своевременно ее выявить и направить в Банк уведомление о факте перевода денежных средств без его согласия.

Если под воздействием мошенников Вы установили на свое ЭУ какое-либо приложение, вероятнее всего это программа удаленного доступа к вашему устройству (AnyDesk, AirDroid, AirMore, TeamViewer и пр.). Пока Вы не удалите вредоносную программу, мошенникам будет доступно управление вашим телефоном или компьютером (в том числе просмотр логина и пароля для входа в Интернет-Банк и мобильное приложение Банка).

*Клиентам следует руководствоваться следующими рекомендациями по снижению рисков осуществления / повторного осуществления перевода денежных средств без добровольного согласия:*

1. При совершении операций с использованием банковской карты / реквизитов банковской карты / в Системе «Интернет-банк» (в том числе в мобильном приложении Банка) (далее – система ДБО) обязательно соблюдайте меры безопасности, приведенные в «Правилах пользования картой» и «Правилах безопасности использования Системы «Интернет-Банк», являющихся неотъемлемой частью «Договора комплексного банковского обслуживания физических лиц в АО «АБ «РОССИЯ».
2. При общении с сотрудниками Банка пользуйтесь только теми телефонами, которые указаны на официальном сайте Банка https://abr.ru/ или на оборотной стороне Вашей банковской карты.
3. При совершении любой операции проводите контроль сумм и получателей до подтверждения операции. При совершении перевода СБП после ввода номера телефона получателя обращайте внимание на информацию о ФИО получателя. Если Вами выявлено расхождение с данными лица, которому Вы планировали отправить денежные средства, лучше отказаться от перевода и уточнить реквизиты у получателя (если у Вас есть основания ему доверять).
4. Регулярно проверяйте уведомления о совершенных операциях, контролируйте состояние своих счетов. В случае отсутствия регулярных проверок Вы можете не отследить несанкционированные операции в случае их совершения. Незамедлительно информируйте Банк обо всех подозрительных или несанкционированных операциях в соответствии с заключенным с Банком договором.
5. Никогда не сообщайте свою персональную информацию третьим лицам. При обращении от имени Банка или иной организации по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить или передать конфиденциальную информацию (ПИН-код карты, CVV/CVC-код, указанный на оборотной стороне карты, логин, пароль, код доступа в систему ДБО, SMS-коды, необходимые для подтверждения операций, и пр.) ни при каких обстоятельствах не сообщайте данную информацию. Банк никогда не запрашивает у клиентов конфиденциальные данные. При возникновении подозрения, что такие данные стали известны третьему лицу, незамедлительно сообщите об этом по телефонам, указанным на официальном сайте Банка https://abr.ru/ или на оборотной стороне Вашей банковской карты.
6. В случае изменения номера телефона, зарегистрированного в Банке, с использованием которого осуществляется доступ к сервисам Банка, обратитесь в Банк для изменения телефонного номера. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время.
7. 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 мошеннических действий, совершаемых в отношении Вас третьими лицами.
8. В случае утери мобильного телефона / планшета, с которого осуществляются переводы денежных средств, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи.
9. Используйте защищенные точки доступа Wi-Fi. Если Вы подключились к публичной Wi-Fi-сети, не пользуйтесь ДБО, не совершайте оплату на сайтах, ничего не скачивайте, не устанавливайте обновления.
10. Ограничьте доступ посторонних лиц к ЭУ, с которого осуществляются переводы денежных средств. Установите пароль на доступ к ЭУ. Не допускается использование в качестве пароля простых, легко угадываемых комбинаций букв и цифр, а также паролей, используемых для доступа в другие системы. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.).

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

12. Не передавайте ЭУ для использования третьим лицам, в том числе родственникам, так как третьими лицами может быть совершен ряд действий, направленных на получение доступа к персональным данным, системе ДБО, реквизитам банковских карт и иным данным.

13. Не переходите по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях из недостоверных источников, в том числе на известные сайты, не загружайте и не устанавливайте на ЭУ программное обеспечение из недостоверных источников.

14. Будьте внимательны при получении SMS-сообщений, направленных от имени Банка или иных организаций. Основные признаки того, что сообщение отправлено мошенниками:

- в сообщении требуют Вашего срочного ответа или принятия немедленного решения или действия;
- в сообщении требуется предоставить, обновить или подтвердить Ваш логин / пароль / код доступа к системе ДБО (в случае ее использования) / сообщить SMS-код;
- сообщение содержит информацию, что на Ваш счет поступили денежные средства, которых Вы не ожидали, или оформлен кредит.

15. Если Вы планируете использовать ЭУ, на который было установлено ВПО, для входа в систему ДБО, то необходимо осуществить поиск и удаление со своего устройства ВПО до момента восстановления доступа к системе ДБО. Для этого воспользуйтесь Инструкцией по удалению вредоносных программ с электронного устройства клиента, размещенной на сайте Банка https://abr.ru/face/d-service/.

16. При возникновении любых сомнений относительно сохранности средств на Вашем банковском счете ***самостоятельно позвоните в Банк*** по номерам телефонов, указанным на официальном сайте Банка https://abr.ru/ или на оборотной стороне Вашей банковской карты.