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

Телефон Банка: 8 800 707-39-39

Соблюдение данных рекомендаций позволит обеспечить максимальную сохранность Ваших денежных средств, а также снизит возможные риски при осуществлении платежей в пользу поставщиков услуг (мобильные операторы, интернет- провайдеры и т.д.), при переводах денежных средств как внутри Банка, так и в другие кредитные организации.

1. При утере мобильного устройства, используемого для осуществления платежей и переводов, незамедлительно обратитесь к своему оператору сотовой связи для блокировки SIM-карты, заблокируйте доступ в мобильное приложение при помощи специалистов Банка, а также обратитесь в Банк для выявления возможных несанкционированных операций.
2. Незамедлительно сообщайте в Банк:

- об утрате платежной карты и (или) мобильного устройства, используемого для осуществления платежей и переводов;
- о смене номера Вашего телефона;
- о несанкционированных операциях по Вашему счету;
- в случае, если Ваши персональные или банковские данные стали доступны постороннему человеку.

3. 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.
4. 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.
5. Регулярно контролируйте состояние Ваших счетов, незамедлительно сообщайте работникам Банка о несанкционированных операциях.
6. На устройство, используемое для управления счетом, своевременно устанавливайте обновления безопасности операционной системы, а также обновления безопасности прикладного программного обеспечения (желательно в автоматическом режиме).
7. Не устанавливайте на устройство программное обеспечение из не доверенных источников.

8. Установите на устройстве, используемом для получения банковских услуг, автоматическую блокировку экрана на период бездействия (с паролем).

9. Не передавайте устройство, используемое для получения банковских услуг, третьим лицам (детям, знакомым, коллегам) для проведения игр, чтения сообщений в социальных сетях и пр.

10. Не используйте функцию автосохранения паролей в браузере устройства, используемого для получения банковских услуг.

11. Не переходите по подозрительным ссылкам, полученным по электронной почте, в SMS-сообщениях, в мессенджерах или в социальных сетях.

12. Не осуществляйте вход в дистанционное банковское обслуживание в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, Интернет-кафе или общественный транспорт.

13. При передаче устройства в ремонт предварительно удалите информацию и приложения, связанные с доступом к банковским счетам.

14. Не передавайте третьим лицам (в том числе - родственникам, знакомым) конфиденциальные сведения: номер карты, ПИН-код, CVC/CVV код (данные на обратной стороне карты), подтверждающий код, направляемый на Ваш номер телефона для подключения к Интернет-банку/мобильному банку.

15. Строго соблюдайте требования по использованию, хранению, уничтожению криптографических ключей электронной подписи, средств криптографической защиты информации (СКЗИ), логинов, паролей/ПИН-кодов при использование дистанционного банковского обслуживания юридических лиц.

16. Обязательно проверяйте написание адреса сайта, на который Вы хотите войти, в командной строке. Не вводите свои данные, если видите предупреждение «Сертификат не является достоверным»/«Ваше подключение не защищено».

17. 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.

18. Сообщите своим родным и близким, а также коллегам рекомендации о противодействии мошенничеству.