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

1. Никогда не сообщайте свои персональные данные (фамилию, имя, отчество, паспортные данные, СНИЛС, ИНН), а также логины, пароли, коды доступа, присылаемые по SMS одноразовые пароли, реквизиты банковских карт, ПИН-коды, цифры с обратной стороны карты (CVV/CVC-код) посторонним людям во время телефонного разговора, или иным способом, даже если они представляются сотрудниками правоохранительных органов, операторами сотовой связи, работниками служб безопасности банков, работниками Банка России или портала Госуслуг и т.д.)
2. Не совершайте никаких действий по указаниям или по рекомендациям посторонних лиц, не сообщайте им о результатах своих действий в системах дистанционного банковского обслуживания (ДБО), на портале Госуслуг, в личных кабинетах на сайтах операторов мобильной связи и т.д.
3. Если Вам звонят по телефону и говорят, что Ваши сбережения находятся в опасности, и их немедленно необходимо перевести на безопасный счет, или просят сообщить Ваши персональные данные, незамедлительно прекратите общение и сами перезвоните в нужную организацию по официальному номеру телефона, представленному на официальном сайте этой организации.
4. Не используйте бесплатные (публичные) беспроводные сети Wi-Fi для выполнения операций по переводу денежных средств в общественных местах: метро, интернет-кафе, парки, выставки и т.д.). Такие сети трудно контролировать, из-за чего у злоумышленников появляется больше возможностей для обхода механизмов защиты, используемых приложениями.
5. При использовании паролей доступа придерживайтесь следующих правил:
   - для каждой системы используйте отдельный пароль;
   - длина пароля должен быть не меньше 8 символов;
   - не используйте простые, легко угадываемые комбинации букв и цифр, символов или личных данных (123, qwerty, дата рождения, логин от почты и т.п.);
   - в составе пароля должны быть буквы в верхнем (прописные) и нижнем (строчные) регистре, цифры и специальные символы (@, #, $, &, *, % и т.п.);
   - для создания надёжного пароля используйте сложные парольные фразы – это позволит Вам легче запомнить Ваш пароль и создаст сложности для киберпреступников в попытках вычислить Ваш пароль. Сложная парольная фраза – это набор из несвязанных логически между собой слов, которые Вы берете, как буквенную часть в ваш пароль, а затем добавляете к паролю цифры и специальные символы.
6. Храните все коды и пароли в тайне, примите все необходимые меры для предотвращения утечки и несанкционированного использования данной информации:
   - не записывайте пароли и коды доступа на бумажных или электронных носителях информации, доступ, к которым могут получить посторонние лица;
   - не используйте функцию автосохранения паролей в браузере устройства, используемого для получения банковских услуг (смартфон, персональный компьютер, ноутбук, планшет и т.д.).

7. Соблюдайте правила безопасного выполнения операций по переводу денежных средств с использованием электронных устройств:
   - своевременно обновляйте программное обеспечение Ваших устройств;
   - используйте только версии программного обеспечения, для которых действует техническая поддержка производителя и выпускаются обновления безопасности;
   - обязательно используйте на устройствах, используемых для получения банковских услуг, лицензированные средства антивирусной защиты, с автоматическим обновлением баз;
   - регулярно проверяйте устройства, используемые для получения банковских услуг, на наличие вредоносного программного обеспечения;
   - в случае обнаружения вирусной угрозы, прекратите использование устройства для перевода денежных средств и незамедлительно примите меры по устранению заражения и анализу последствий;
   - для выполнения операций по переводу денежных средств используйте приложения, получаемые только из проверенных источников, обращайте внимание на сайт поставщика, при установке и настройке внимательно читаете информацию, которая появляется на экране устройства, контролируйте предоставляемые приложениям разрешения;
   - не устанавливайте программное обеспечение по просьбе незнакомых лиц;
   - установите надежный пароль, как для входа на электронное устройство, так и для авторизации в приложениях;
   - настройте автоматическую блокировку экрана по прошествии определённого периода бездействия;
   - извлекайте носители ключей электронной подписи (Рутокен ЭЦП и т.п.) из Вашего устройства, если в данный момент не используете их в работе;
   - используйте двухфакторную аутентификацию везде, где это возможно;
   - строго соблюдайте требования по использованию средств криптографической защиты информации (СКЗИ), хранению, уничтожению ключей электронной подписи, политике использования кодов доступа при использовании систем ДБО;
   - не оставляйте электронные устройства без присмотра и не передавайте их другим людям;
   - не передавайте электронные устройства в недоверенные (неавторизованные) сервисы, оказывающие услуги по технической поддержке. В случае необходимости передать устройства в ремонт, предварительно удалите из него всю информацию, используемую Вами для доступа к банковским счетам;
   - не устанавливайте программы для удаленного подключения к устройству, используемому для перевода денежных средств.
8. В случае утраты мобильного устройства (смартфона, телефона) номер, которого используется Вами для доступа к сервисам Банка, незамедлительно обратитесь к оператору сотовой связи для блокировки SIM-карты, уведомите Банк о факте утраты мобильного устройства и заблокируйте доступ в мобильное приложение Банка.
9. Если Вы изменили номер телефона, используемый Вами для совершения операций по переводу денежных средств, обратитесь в офис Банк для изменения телефонного номера, по которому осуществляется доступ к сервисам Банка.

10. Не забывайте, что Ваш старый номер телефона, который длительное время был неактивен, может быть передан оператором другому абоненту. В последующем этот номер может быть использован для попыток получения несанкционированного доступа к Вашему личному кабинету на портале Госуслуг и к сервисам Банка.
11. Если по неизвестной причине Ваша SIM-карта перестала работать, срочно обратитесь к оператору сотовой связи, для выяснения причины, так как это может быть одним из признаков, говорящих о попытках совершения в отношении Вас мошеннических действий.
12. Не переходите по ссылкам, полученным Вами по электронной почте, содержащимся в текстах SMS-сообщений, полученным в мессенджерах или в социальных сетях. Даже если отправитель Вам известен, не исключена возможность того, что аккаунт отправителя сообщения могли взломать.
13. При пользовании системами дистанционного банковского обслуживания, убедитесь в корректности написания адреса: проверьте, верно ли написано доменное имя.
14. Соблюдайте осторожность при заказе и оплате товаров в интернет-магазинах и на торговых площадках, убедитесь в том, что сайт не создан мошенниками.
    Основными признаками того, что сайт создан мошенниками, могут являться следующие:
    - в адресе сайта отсутствует буква «s» после «http»;
    - сайт работает по «https», но к используемому сайтом сертификату нет доверия;
    - адрес сайта не содержит названия используемого сервиса, либо наименование сервиса искажено или имеет ошибки;
    - в содержимом сайта много орфографических ошибок или опечаток;
    - для регистрации или входа на сайте просят ввести данные банковской карты, логин и пароль от почты и т.д.;
    - на сайте нет пользовательского соглашения или в его содержимом указаны сторонние компании, которые не имеют отношения к сайту;
    - указаны неверные контактные данные или реквизиты организации, которой принадлежит сайт.