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

1). Не сообщайте свои личные данные, такие как ФИО, паспортные данные, логины, пароли, коды доступа, SMS-коды, одноразовые пароли, реквизиты банковских карт, ПИН-код, цифры с обратной стороны карты (CVV/CVC-код), посторонним людям во время телефонного разговора, по электронной почте или другим способом, в том числе если они представляются сотрудниками правоохранительных органов, операторами сотовой связи, работниками банков, работниками Центрального банка, Госуслуг и т.д.

Не проводите никакие действия по указанию или по рекомендациям посторонних лиц, не сообщайте им результаты своих действий в ДБО/Мобильном банке/на Госуслугах и т.д.

Если Вам говорят, что сбережения в опасности и их немедленно необходимо перевести на безопасный счет или просят передать личные данные, **незамедлительно прекращайте общение**.

В случае сомнений, положите трубку и перезвоните в нужную организацию по официальному номеру телефона сами. При необходимости, обратитесь в отделение Банка, либо позвоните по номеру на обратной стороне карты и убедитесь, что с вашими деньгами все в порядке.

2). Никогда не используйте публичные беспроводные сети (Free Wi-Fi) или незащищенные беспроводные сети для выполнения операций по переводу денежных средств (сети в интернет-кафе, общественных местах и т.д.).

Это связано с тем, что такие сети трудно контролировать, из-за чего у злоумышленников появляется больше возможностей для обхода механизмов защиты, используемых приложениями. Именно по этой причине для осуществления денежных переводов необходимо использовать сеть оператора сотовой связи или доверенную защищенную беспроводную сеть.

3). При создании паролей придерживайтесь следующих правил:

- Пароли от разных систем должны отличаться между собой
- Пароль должен быть не меньше 8 символов;
- Не используйте простые, легко угадываемые комбинации букв и цифр, символов или личных данных (123, qwerty, дата рождения, девичья фамилия, логин от почты и т.д.).
- В пароле должны быть буквы в верхнем (прописные) и нижнем (строчные) регистре;
- Обязательно используете специальные символы при создании пароля (@, #, $, &, *, % и т.п.);
- Используйте сложные парольные фразы, так будет проще запомнить вам и сложнее вычислить киберпреступникам. Сложная парольная фраза – это набор из несвязанных

логически между собой слов, которые вы берете, как буквенную часть в ваш пароль. Дополнительно к нему добавляете цифры и специальные символы.

Парольную фразу из четырех или более произвольных слов с комбинацией из дополнительных символов взламывать будут несколько веков, а «qwerty123» - миллисекунду.

4). Вместе с тем, когда вы обеспечили достаточную сложность пароля, у мошенников остаются иные пути узнать ваши пароли. Для исключения такой возможности, храните все коды и пароли в тайне, примите все необходимые меры для предотвращения утечки и несанкционированного использования данной информации.

- Не записывайте пароли и коды на бумажных или электронных носителях информации, доступ к которым могут получить другие лица.
- Не используйте функцию автосохранения паролей в браузере устройства, используемого для получения банковских услуг.

5). При работе на электронных устройствах, с которых осуществляете операции по переводу денежных средств (смартфон, персональный компьютер, ноутбук, планшет и т.д.):

- Своевременно обновляйте программное обеспечение ваших устройств.

Используйте те версии программного обеспечения, для которых действует поддержка производителя и выпускаются обновления безопасности;

- Обязательно используйте на устройствах лицензированные средства антивирусной защиты, с автоматическим обновлением баз. Регулярно проверяйте электронные устройства на наличие вредоносного программного обеспечения.

При обнаружении угрозы незамедлительно принимайте меры устранению заражения и анализу последствий.

- Загружайте программное обеспечение только из проверенных источников, обращайте внимание на сайт поставщика, при установке и настройке внимательно читаете информацию, которая появляется на экране, и контролируйте предоставляемые приложениям разрешения.

Не устанавливайте программное обеспечение по просьбе незнакомых лиц.

- Устанавливайте надежный пароль не только для входа на устройство, но и для авторизации в приложениях.
- Обязательно блокируйте устройство и выходите из всех приложений, если вам необходимо отлучиться.
- Установите автоматическую блокировку экрана с паролем на период бездействия.
- Обязательно извлекайте носители (Rutoken и иные модели) с ключами электронной подписи из вашего устройства, если в данный момент не используете их в работе. Не оставляйте носители в устройстве;
- По возможности используйте двухфакторную аутентификацию;

- Строго соблюдайте требования по использованию средств криптографической защиты информации (СКЗИ), хранению, уничтожению ключей электронной подписи, политике PIN-кодов, при использовании ДБО;
- Не оставляйте электронные устройства без присмотра и не передавайте их другим людям;
- Исключите обслуживание электронных устройств случайными работниками технической поддержки. Не устанавливайте программы для бесконтрольного удаленного подключения. В случае подозрения на удаленное управление, немедленно прекратите любые действия с устройством, обесточьте их (принудительно), и отключите от информационных сетей;

6). При утрате мобильного устройства с номером, который необходим для доступа к сервисам Банка, необходимо незамедлительно обратиться в салон оператора 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.

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

8). Если был сменен номер телефона, обратитесь в офис Банк для изменения телефонного номера, по которому осуществляется доступ к сервисам Банка.

9). Помните, что старый номер, который длительное время был неактивен, оператор может передать другому абоненту.

10). Если по какой-то причине у Вас перестала работать SIM-карта, срочно обратитесь к оператору сотовой связи, для выяснения причины, так как это может быть одним из признаков, говорящих о совершении мошеннических действий в отношении Вас.

11). Не переходите по сомнительным ссылкам, полученным в почтовых и SMS-сообщениях, в мессенджерах или в социальных сетях. Даже если отправитель не является неизвестным, не исключайте возможность того, что его аккаунт могли взломать.

12). При использовании ДБО/интернет-банка убедитесь в легитимности данного ресурса, обязательно проверяйте правильность доменного имени.

13). Будьте крайне внимательны при покупке товаров через интернет. Прежде чем вводить реквизиты банковской карты для оплаты товара, убедитесь в том, что сайт не создан мошенниками. Основные признаки, того что сайт создан мошенниками:

- у сайта отсутствует SSL-сертификат, отсутствует буква «s» после http, или же сайт работает по https, но к 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.

14). Если в отношении вас были совершены мошеннические действия, обратитесь лично в правоохранительные органы.

15). Сообщите своим родным, близким, пожилым родственникам, а также коллегами о существующих мерах противодействия мошенничеству.