Рекомендации для клиентов ООО Банк Оранжевый по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники в целях противодействия осуществлению переводов денежных средств без согласия клиента.

В соответствии с требованиями Положения Банка России от 17.04.2019 № 683-П (ред. от 18.02.2022) «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» ООО Банк Оранжевый (далее – Банк) настоящим доводит до своих клиентов:

- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления, и мерах по их снижению;
- меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом совершались действия в целях осуществления банковской операции;
- меры по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления банковской операции, и своевременному обнаружению воздействия вредоносного кода.

Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления.

1. Доступ к защищаемой информации со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера, в том числе, сведений о банковских операциях, состоянии счетов, получаемых банковских услугах, персональных данных и иной значимой информации.
2. Получение доступа к защищаемой информации третьими лицами может повлечь за собой совершение банковских операций, не обладающими правом их осуществления, а также совершение ими иных юридически значимых действий, в частности, подключение и отключение услуг, внесение изменений в регистрационные данные клиента, использование счетов для совершения незаконных операций и др.
3. Использование третьими лицами доступа к защищаемой информации может повлечь за собой негативное воздействие на программное обеспечение клиента, носители информации и их содержимое, блокирование работы компьютера либо иного устройства, используемого клиентом что, в свою очередь может привести к невозможности использования клиентами услуг Банка, потерям и убыткам, как для клиентов, так и для Банка.

Меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом совершались действия в целях осуществления банковской операции.

1. Не сообщать посторонним лицам, в том числе в сети Интернет, персональные данные или информацию о банковских операциях, о банковских картах (счетах), логины и пароли доступов, историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к защищаемой информации.
2. Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются банковские операции, не использовать функцию запоминания логина и пароля, не использовать одинаковые логин и пароль для доступа к различным системам.
3. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат. Регулярно производить смену паролей.
4. По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации. При передаче информации с использованием чужих компьютеров или иных средств доступа, не сохранять на них персональные данные и другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.
5. Не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами. Не переходить по ссылкам в таких письмах, не открывать вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение). Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них, для связи использовать номера телефонов и электронные адреса, указанные на официальном сайте Банка.
6. Контролировать конфигурацию устройства, с использованием которого совершаются действия в целях осуществления банковской операции. Не запускать на своем компьютере, телефоне и/или ином устройстве приложений из не заслуживающих доверия источников.
7. Регулярно производить обновление системных и прикладных программных средств.
8. При утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления банковской операции – незамедлительно сообщить об этом оператору сотовой связи для блокировки сим-карты и в Банк для блокировки доступа.
9. При наличии несанкционированных действий с денежными средствами, иных незаконных банковских операций – незамедлительно сообщить в Банк и подать заявление о данном факте в правоохранительные органы, сохранить доказательства таких действий в устройстве.

Меры по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления банковской операции, и своевременному обнаружению воздействия вредоносного кода

1. Использовать только официально приобретенное антивирусное программное обеспечение и межсетевые экраны с целью своевременного обнаружения воздействия вредоносного кода.

2. Установка и регулярное обновление средств антивирусной защиты должны осуществляться в соответствии с технической документацией.
3. В целях обеспечения антивирусной защиты производится антивирусный контроль автоматизированной системы Устройства.
4. Обязательному антивирусному контролю подлежит вся информация.
5. К применению допускаются только лицензионные антивирусные средства.
6. При работе с иными носителями информации необходимо перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
7. Защита от вирусов состоит из нескольких этапов. На первом этапе выполняются регулярные профилактические работы по выявлению вирусов. На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления. На третьем этапе выполняется уничтожение вируса (вирусов) из системы устройства.
8. Ярлык для запуска антивирусной программы должен быть вынесен на основной экран устройства.
9. Обновление антивирусных пакетов осуществлять на постоянной основе.
10. Осуществлять регулярный контроль работоспособности антивирусных программ, обеспечить невозможность самовольного, либо несанкционированного отключения средств антивирусной защиты.
11. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
12. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.
13. Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку в автоматизированной системе, почтовых ресурсах и межсетевых экранах.
14. Антивирусная программа должна обеспечивать сохранение безопасного состояния операционной системы при своих сбоях.