Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать транзакции от лица клиента. Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ.

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц.

1. Несанкционированный доступ со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации.

2. Несанкционированный доступ со стороны третьих лиц может повлечь за собой риски совершения юридически значимых действий, включая: совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента.

3. Несанкционированный доступ со стороны третьих лиц может повлечь за собой риск деструктивного воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов некредитной финансовой организации (НФО) для реализации своих намерений.

4. Вредоносные программы способны самостоятельно, то есть без ведома клиента создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных до полного разрушения информации, хранящейся на дисках компьютера. Все риски, связанные с утратой и компрометацией секретных ключей, несет Владелец ключа. НФО не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами безопасности.

II. Рекомендации по защите информации от противоправного доступа.

1. Не сообщайте посторонним лицам персональные данные или информацию через Интернет, включая логины и пароли доступа к клиентским ресурсам НФО, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашим активам.

2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

3. Не используйте функцию запоминания логина и пароля в браузерах.

4. Не используйте одинаковые логин и пароль для доступа к различным системам.

5. Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о доступе к клиентским ресурсам НФО.

6. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему средству доступа обязательно смените логин и пароль.

7. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

8. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть Ваши идентификационные данные.

9. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

10. При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию ключей.

11. Используйте лицензированное программное обеспечение.

12. Регулярно проводите проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.

13. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников.

14. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

15. Не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены злоумышленниками и использованы для получения доступа к Вашим активам.

16. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

17. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

18. Для обеспечения конфиденциальности операций пользуйте только защищенное соединение через HTTPS. Защищенное соединение предотвращает перехват или фальсификацию передаваемых данных.

19. В случае утраты устройства необходимо изменить пароли доступа к ресурсам на которые производился вход.