Рекомендации по защите информации
от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

Уважаемые клиенты!

В целях предупреждения последствий недобросовестных действий третьих лиц, противодействия проведению незаконных финансовых операций в отношении ваших активов, учитываемых на счетах в ООО «ПСБ-Форекс» (далее - Общество), представляем настоящее уведомление о рисках, а также перечень рекомендуемых мер по обеспечению защиты информации.

В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах в рамках вашего обслуживания в Обществе, содержащаяся в электронных документах, которыми вы обмениваетесь с Обществом (электронные сообщения), информация, необходимая для авторизации клиента и удостоверения его прав на распоряжение активами (ключи, логины, пароли, СМС подтверждения и т.п.), информация об осуществленных финансовых операциях, а также ключевая информация применяемых средств криптографической защиты (криптографические ключи) (далее в совокупности – защищаемая информация), может быть подвергнута воздействию вредоносных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код).

Также в результате неправомерных третьих лиц существует риск получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций по вашим счетам лицами, не обладающими правом их осуществления, что может повлечь за собой, в том числе, следующие негативные последствия:

− совершение злоумышленниками юридически значимых действий: операций с доступными активами, подключения и отключения услуг (в том числе платных), внесение изменений в ваши регистрационные данные, использование ваших счетов и находящихся на них активов для прикрытия каких-либо действий, носящих противоправный характер, иных действий против вашей воли;

− деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения вами или Обществом своих обязательств по договору или невозможности использования сервисов Общества для реализации Ваших намерений;

− разглашение относящейся к вам информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации.

Настоятельно рекомендуем вам соблюдать рекомендации и принимать меры, изложенные в них. Они направлены на защиту информации от воздействия вредоносных кодов, предотвращение несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого вами совершались действия в целях осуществления финансовой операций, контроль конфигурации данного устройства, и своевременное обнаружение воздействия вредоносного кода.

Рекомендации
по безопасному использованию мобильных приложений

1. Устанавливайте приложение исключительно по ссылкам в авторизованных магазинах приложений (App Store или Google Play).

2. Регулярно устанавливайте обновления безопасности для операционной системы вашего мобильного устройства.

3. Используйте лицензионные, постоянно обновляемые средства антивирусной защиты.

4. Используйте средства блокировки входа на ваше мобильное устройство (Пароль, Пин-код, TouchID, FaceID и иные).

5. Никому не сообщайте пароль для доступа в приложение и одноразовый SMS-код подтверждения операций.

6. Не храните пароль для доступа в приложение на своем мобильном устройстве в открытом виде.

7. Если у вас есть подозрение, что ваши реквизиты доступа в приложение стали известны третьим лицам, заблокируйте устройства и незамедлительно обратитесь в клиентскую поддержку Общества.

8. Завершайте сеанс работы в приложении сразу после проведения всех необходимых операций при помощи кнопки «Выход».

9. В случае потери или хищения вашего мобильного устройства незамедлительно сообщите об этом в клиентскую поддержку Общества.

10. Не посещайте с использованием мобильного устройства, на котором установлена клиентская часть приложения, сайты сомнительного содержания.

11. Не устанавливайте на мобильное устройство, на котором используется клиентская часть приложения, программное обеспечение неизвестных разработчиков, распространяемое из сторонних источников (малоизвестных сервисов распространения приложений).

12. Не используйте приложение на мобильных устройствах, системная программная часть которых подверглась модификации, несанкционированной производителем. (устройство подвергнуто процедурам «Jailbreak», получению «Root»-прав, разблокировке загрузчика, установке версий операционных систем от неофициальных разработчиков).

13. При отсутствии необходимости, не используйте приложение для совершения операций по счету или совершения иных юридически значимых действий при подключении телефона к публичным сетям WiFi.

Рекомендации
о мерах безопасного использования систем дистанционного обслуживания

Общие рекомендации

1. Организуйте режим использования компьютера, с которого осуществляется использование систем дистанционного обслуживания таким образом, чтобы исключить возможность его несанкционированного использования.

2. Используйте на вашем компьютере только лицензионное программное обеспечение, не устанавливайте программное обеспечение, полученное из сомнительных источников.

3. По возможности используйте на компьютере только лишь программное обеспечение, необходимое для работы с системой дистанционного обслуживания.

4. Устанавливайте обновления операционной системы и интернет-браузера вашего компьютера, выпускаемые компанией-производителем для устранения выявленных в них уязвимостей.

5. Всегда используйте встроенные средства межсетевого экранирования (брандмауэр или firewall) операционной системы.

6. Рекомендуется ограничить права пользователя, использующего систему дистанционного обслуживания, минимально необходимыми для работы с системой. Пользователь не должен обладать административными привилегиями.

7. Рекомендуется хранить ключи для доступа к системе дистанционного обслуживания на съемном носителе (USB). Организуйте хранение ключевых носителей в недоступном для посторонних лиц месте. После завершения работы с системой дистанционного обслуживания не оставляйте подключенными к компьютеру ключевые носители, используемые при работе с ним.

8. Осуществляйте регулярный контроль состояния ваших счетов и сообщайте сотрудникам Общества обо всех подозрительных или несанкционированных операциях.

Рекомендации по использованию парольной защиты

1. Не записывайте пароли, служащие для доступа к системе дистанционного обслуживания на бумажных носителях или в файлах на жестком диске вашего компьютера. Не сообщайте их другим лицам, в том числе вашим знакомым, друзьям, родственникам.

2. Используйте для доступа к системе дистанционного обслуживания сложные пароли, с наличием букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (!@#$%^&*(),.?)

3. Не используйте простые пароли, представляющие собой осмысленные слова (password), дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (77777777, 111adZZZ).

Антивирусная защита

1. Для защиты от вредоносного программного обеспечения необходимо использовать лицензионное антивирусное программное обеспечение, функционирующее в автоматическом режиме.

2. Антивирусное программное обеспечение должно регулярно обновляться.

3. Не реже одного раза в неделю проводите полное антивирусное сканирование компьютера. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы.

4. Не отключайте антивирусное программное обеспечение ни при каких обстоятельствах.

Рекомендации по защите при использовании сети Интернет

1. По возможности, не используйте для просмотра сайтов в сети Интернет компьютер, с которого осуществляется доступ к системе дистанционного обслуживания.

2. Не посещайте сайты сомнительного содержания.

3. Не используйте для работы в системе дистанционного обслуживания компьютеры, расположенные в местах общего пользования (отелях, бизнес-центрах). Рекомендуется не использовать для работы с системой дистанционного обслуживания общедоступные каналы связи (например, Wi-Fi в кафе, отелях или аэропортах).

4. Не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Такие письма подлежат немедленному удалению.

5. По возможности, не сохраняйте пароль от системы дистанционного обслуживания в браузере.

6. При работе с системой дистанционного обслуживания обращайте внимание на адреса сайтов (убедитесь, что они являются официальными сайтами Общества).

Рекомендации по использованию СМС подтверждений

1. При подтверждении ваших операций одноразовым СМС- кодом (паролем), всегда обращайте внимание на условия, реквизиты и иные данные поручения (иного вашего распоряжения), которые вы подтверждаете, содержащиеся в полученном СМС-сообщении. Они должны соответствовать вашему волеизъявлению.

2. В случае утери мобильного телефона, на который Общество отправляет СМС- сообщения, незамедлительно обратитесь к оператору сотовой связи для блокировки вашей сим-карты, а также в клиентскую поддержку Общества для выявления возможных несанкционированных операций.

3. Не устанавливайте на телефон, используемый для СМС-подтверждения, приложения из сомнительных источников.