Общество с ограниченной ответственностью «Управляющая компания «ОТКРЫТИЕ» (далее – Общество) в целях соблюдения требований «Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (утв. Банком России 17.04.2019 N 684-П) уведомляет Клиентов Общества о следующем.

О возможных рисках получения несанкционированного доступа к защищаемой информации

1. Доступ к защищаемой информации со стороны третьих лиц может повлечь за собой риски разглашения инсайдерской информации и информации конфиденциального характера, в том числе, сведений об операциях; активах, составляющих инвестиционный портфель; состоянии счетов; получаемых/оказываемых услугах; персональных данных и иной значимой информации.

2. Получение доступа к защищаемой информации третьими лицами может повлечь за собой совершение финансовых операций с активами клиента лицами, 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 и активов для совершения незаконных операций и др.

3. Использование лицами, не обладающими таким правом, доступа к защищаемой информации может повлечь за собой деструктивное воздействие на программное обеспечение Общества, носители информации и их содержимое, что, в свою очередь, может привести к приостановке деятельности Общества, невозможности использования клиентами сервисов компании, потерям и убыткам, как для клиентов, так и для Общества.

4. Использование лицами, не обладающими таким правом, доступа к защищаемой информации может повлечь за собой блокирование работы компьютера либо иного устройства, используемого клиентом для совершения операций, получения услуг.

О мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода

В целях защиты ПО и оборудования от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям, а также для предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства (далее – Устройство), посредством которого им совершались финансовые операции, контроля конфигурации такого Устройства и своевременного обнаружения воздействия вредоносного кода, Общество рекомендует:

1. использовать Устройство таким образом, чтобы исключить возможность его несанкционированного использования третьими лицами;

2. использовать на Устройстве только лицензионное программное обеспечение, не устанавливать программное обеспечение, полученное из сомнительных источников (например, скачанное с публичных файловых хостингов или торрентов);

3. устанавливать обновления операционной системы и интернет-браузера Устройства, выпускаемые компанией-производителем для устранения выявленных в них уязвимостей;

4. использовать встроенные средства межсетевого экранирования (брандмауэр) операционной системы;

5. регулярно обновлять антивирусное программное обеспечение; проводить не реже одного раза в неделю полное антивирусное сканирование Устройства (в случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы); ни при каких обстоятельствах не отключать антивирусное программное обеспечение.

6. использовать для доступа к устройству сложные пароли, удовлетворяющие следующим требованиям:

· длина пароля должна быть не менее 8 символов;

· пароль должен состоять как минимум из символов трех приведенных далее групп: букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (например !@#$%^&*(),.?);

Не использовать 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).

Не записывать пароли, служащие для доступа к устройству на бумажных носителях или в файлах на жестком диске вашего компьютера, не сообщайте их другим лицам, в том числе родственникам и иным лицам.

7. не посещать сайты сомнительного содержания; не открывать вложения электронных писем, полученные от неизвестных адресатов (такие письма лучше немедленно удалить); не сохранять пароль от доступа к Устройству в браузере;

8. в случае подтверждения операций одноразовым СМС-паролем, всегда обращать внимание на реквизиты платежа, а также на сумму, указанные в полученном СМС-сообщении. Они должны соответствовать параметрам (реквизитам) проводимой операции;

9. в случае утери мобильного телефона, незамедлительно обратиться к оператору сотовой связи для блокировки сим-карты, а также в Общество для предупреждения и выявления возможных несанкционированных операций.