«УТВЕРЖДАЮ»
Генеральный директор Общества
с ограниченной ответственностью
«Московский Фондовый Центр»

А.А. Шевченко

Приказ №д/22-45
от «06» сентября 2022 года

Рекомендации
по соблюдению информационной безопасности клиентами ООО «Московский Фондовый Центр» в целях противодействия незаконным финансовым операциям.

Москва,
2022 г.

В соответствии с требованиями 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 20.04.2021 № 757-П), ООО «Московский Фондовый Центр» (далее - Регистратор) доводит до вашего сведения информацию о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации, и основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям (далее – Рекомендации).

Рекомендации не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации. В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, правилах и иных документах Регистратора, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям иных документов Регистратора. Перед заключением договоров внимательно изучайте документы Регистратора, регламентирующие предоставление услуг/сервисов, в частности ознакомьтесь с разделами, которые напрямую касаются информационной безопасности.

Данные рекомендации разработаны в целях снижения рисков информационной безопасности – вероятностей возникновения негативных событий, которые нанесут ущерб организации или физическому лицу:

1) несанкционированный доступ к вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);

2) потеря (хищение) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;

3) воздействие вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;

4) совершения в отношении Вас иных противоправных действий, связанных с нарушениями информационной безопасности клиента Регистратора.

1) Под защищаемой информацией понимается:

1.1) информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде вами и (или) работниками Регистратора;

1.2) информация об осуществляемых вами финансовых операциях;

1.3) информация, необходимая Регистратору для авторизации вас как клиента Регистратора в целях осуществления финансовых операций и удостоверения вашего права распоряжаться денежными средствами, ценными бумагами или иным имуществом;

1.4) ваши персональные данные.

2) Целью Рекомендаций являются доведение до вас информации:

2.1) о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

2.2) 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.

3) Основные риски получения несанкционированного доступа к защищаемой информации:

3.1) риск совершения финансовых операций с активами клиентов, в том числе путем формирования и отправки от имени клиента распоряжения на проведение финансовой операции;

3.2) риск совершения иных юридически значимых действий, включая внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для противоправных действий, совершение иных действий против воли клиента;

3.3) риск повреждения программного обеспечения на устройстве клиента Регистратора, а также риск изменения, искажения, уничтожения или шифрования информации об активах клиента или данных самого клиента на данном устройстве или на устройстве, с которого клиент осуществляет доступ к сервисам Регистратора;

3.4) риск разглашения конфиденциальной информации клиентом Регистратора злоумышленнику.

4) Несанкционированный доступ к защищаемой информации происходит в случае:

4.1) кражи устройства клиента;

4.2) удаленного доступа к устройствам клиента в результате взлома системы защиты;

4.3) получения данных клиента для проведения/подтверждения проведения операций с помощью метода социальной инженерии (фишинг);

4.4) заражения устройства клиента вредоносным кодом.

5) Защитой от методов социальной инженерии является умение распознать злоумышленные действия. Основными способами получения несанкционированного доступа к защищаемой информации являются:

5.1) Фишинг - вид мошенничества, целью которого является получение доступа к конфиденциальным данным клиента - логинам, паролям, платежной информации. Это достигается путём проведения массовых рассылок электронных писем от имени популярных компаний, а также личных сообщений внутри различных сервисов, например, от имени финансовых организаций или внутри социальных сетей. В письме, как правило, содержится прямая ссылка на сайт, внешне неотличимый от настоящего. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими

приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, платежную информацию, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и счетам клиента, либо осуществить хищение денежных средств.

5.2) Заражение устройств клиента вредоносным кодом, с помощью:

Троянских программ - разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации банковских карт и её передачу злоумышленнику, её использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях злоумышленника.

Использования социальной инженерии для внедрения вредоносного программного обеспечения в устройства клиента. Злоумышленники во время звонка клиенту Регистратора, представляются сотрудниками техподдержки и опрашивают клиентов на наличие каких-либо технических неисправностей в устройстве клиента с которого он осуществляет юридически значимые действия (или операции). Под видом устранения неисправностей, злоумышленники просят клиента установить специальное программное обеспечение, после чего у злоумышленника появляется возможность контроля над устройством клиента Регистратора.

6) Рекомендации по защите информации от воздействия вредоносного кода:

6.1) Обеспечьте защиту устройства:

- используйте только лицензионное программное обеспечение, полученное из доверенных источников;
- не совершайте установку программ из непроверенных источников;
- установите средства защиты, такие как: антивирус (или брандмауэр);
- своевременно обновляйте операционную систему устройства, для минимизации рисков заражения вредоносным ПО;
- регулярно осуществляйте проверку устройства на наличие вирусов;
- Ограничьте доступ к устройству, с которого производятся юридически значимые действия (операции). Например с помощью установки на данное устройство пароля или ограничения доступа к устройству третьих лиц.

Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах. Длина пароля должна быть не менее 8 символов клавиатуры латинского алфавита и представлять собой сложное сочетание строчных и прописных букв, цифр и специальных символов.

6.2) Обеспечьте конфиденциальность:

- блокируйте устройство после использования, используйте настройки устройства, требующие ввода пароля для его разблокировки и совершения финансовых операций;

- не передавайте третьим лицам и не оставляйте устройство с помощью которого осуществляются юридически значимые операции без присмотра;

- храните в тайне данные для авторизации на веб-ресурсах (логин/пароль), в случае компрометации немедленно примите меры для блокировки учетной записи;

- соблюдайте принцип разумного раскрытия информации о номерах договоров, номерах ваших счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах, в случае если у вас запрашивают указанную информацию в привязке к сервисам Регистратора по возможности оцените ситуацию и уточните полномочия и процедуру через официальный канал связи с Регистратором, указанный в договоре или на официальном сайте.

6.3) Соблюдайте правила безопасности в сети Интернет:

- при использовании различных сайтов удостоверьтесь в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка);

- при наличии на устройстве программ фильтрации сетевого трафика (брандмауэра) держите его включённым и блокируйте все незнакомые или подозрительные подключения;

- не отвечайте на подозрительные сообщения, полученные с неизвестных адресов;

- не устанавливайте и не сохраняйте подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет;

- не сохраняйте пароли в памяти интернет-браузера;

- не открывайте и не используйте сомнительные Интернет-ресурсы на устройстве.

6.4) Контроль подключения:

- не используйте устройства третьих лиц для совершения финансовых операций или получения информации в отношении таких операций;

- не работайте в сервисах Регистратора с устройства, использующего подключение к общедоступной сети Wi-Fi.

6.5) Проявляйте осторожность и предусмотрительность:

- будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным ПО, например троянской программой. Троянская программа, попав к вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на Вашем устройстве;

- внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под сотрудника Регистратора или иных доверенных лиц;

- не открывайте подозрительные или сомнительные вложения в виде исполняемых файлов (с расширением exe, bat и т.п.) в электронных письмах, даже, если письмо поступило от известного адресата, так как электронная почта отправителя могла быть взломана, а вложение может являться вредоносной программой;

- будьте осторожны с файлами из новых или непроверенных источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);

- следите за информацией в прессе о последних критичных уязвимостях и о вредоносном коде;

- осуществляйте звонок Регистратору только по номеру телефона, указанному в договоре или на официальном сайте Регистратора. Имейте в виду, что от Регистратора не могут поступать звонки или сообщения, в которых от вас требуют передать данные для авторизации в личном кабинете сервисов Регистратора (логин, пароль, и т.д.), кодовое слово или СМС-код. Указанные сведения могут быть запрошены только если вы сами позвонили Регистратору.

- имейте в виду,что если Вы передаете Ваш телефон и/или устройство другим лицам, они могут установить на него вредоносное ПО, а в случае кражи или утери Вашего мобильного устройства, злоумышленники могут воспользоваться им для доступа к системам Регистратора, которыми пользовались Вы. В связи с этим при утере, краже телефона (SIM карты), используемого для получения СМС-кодов или доступа к системам Регистратора с Мобильного приложения:

незамедлительно проинформируйте Регистратор через контактный телефон, указанный в договоре или на официальном сайте;

целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить SIM карту, а также сменить пароль в личном кабинете веб-сервиса Регистратора.

- при подозрении на несанкционированный доступ к сервисам Регистратора и/или компрометацию устройства, с которого осуществляется доступ к таким сервисам, необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ к сервисам Регистратора, обратившись к Регистратору;

- по возможности, используйте для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас или работать на компьютере под выделенной для таких целей учетной записью, доступ к которой имеется только у Вас.;

7) При работе с ключами электронной подписи необходимо:

7.1) Использовать для хранения ключей электронной подписи специальные защищенные носители ключевой информации (ключевые носители), например, e-token, смарт-карта и т.п.;

7.2) Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы;

7.3) Использовать сложные пароли для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли открытом виде на компьютере/мобильном устройстве.