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

_____А.А. Шевченко

«10» февраля 2021 года

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

Москва,

2021 г.

В соответствие с требованиями Положения Банка России от 17.04.2019 № 684-П «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» ООО «Московский Фондовый Центр» (далее – Регистратор) доводит до вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям .

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты) (далее - 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 так же могут быть отражены в договорах, регламентах, правилах и иных документах Регистратора, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части не противоречащей положениям внутренних документов.

В целях снижения риска реализации инцидентов информационной безопасности – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов и (или) нарушить конфиденциальность, целостность и доступность информации вследствие:

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

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

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

4) совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности для снижения риска финансовых потерь:

1. Обеспечьте защиту устройств. К мерам защиты включая, но не ограничиваясь могут быть отнесены:

1.1) Использование только лицензионного программного обеспечения, полученного из доверенных источников;

1.2) Запрет на установку программ из непроверенных источников

1.3) Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;

1.4) Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;

1.5) Хранение, использование устройства с целью избежать риски кражи и/или утери;

1.6) Своевременные обновления операционной системы, особенно в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения вредоносным кодом. Злоумышленники часто используют старые уязвимости;

1.7) Активация парольной или иной защиты для доступа к устройству.

2. Обеспечьте конфиденциальность:

2.1) Храните в тайне аутентификационные/идентификационные данные и ключевую информацию: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и/или блокировки;

2.2.) Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, в случае если у вас запрашивают указанную информацию, по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра.

3. Проявляйте осторожность и предусмотрительность:

3.1) Будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;

3.2) Внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Компанию или иных доверенных лиц;

3.3) Будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта;

3.4) Будьте осторожны с файлами из новых или «недоверенных» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);

3.5) Не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

3.6) Следите за информацией о последних критичных уязвимостях и о вредоносном коде;

3.7) При наличии в рамках вашего продукта сервиса контакт центра, осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Компании. И имейте в виду, что от лица Компании не могут поступать звонки или сообщения, в которых от вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д. Кодовое слово может быть запрошено только, если вы сами позвонили в контакт центр;

3.8) Имейте в виду, что, если вы передаете ваш телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам, которыми пользовались Вы. В связи с этим при утере, краже телефона (SIM-карты), используемого для получения СМС кодов или доступа к системам организации с мобильного приложения целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить SIM-карту, а также сменить пароль в мобильных приложениях;

3.9) При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;

3.10) Помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление вашего устройства;

3.11) Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас;

3.12) Контролируйте свой телефон, используемый для получения СМС кодов. В случае выхода из строя SIM-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

4. При работе с ключами электронной подписи необходимо:

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

4.2) 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;

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

5. При работе на компьютере необходимо:

5.1) Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);

5.2) Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);

5.3) Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;

5.4) Использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;

5.5) Использовать сложные пароли;

5.6) Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

6. При работе с мобильными приложениями необходимо:

6.1) Не оставлять свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование мобильных приложений;

6.2) Использовать только официальные мобильные приложения;

6.3) Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Компании;

6.4) Установить на мобильном устройстве пароль для доступа к устройству и приложениям.

7. При обмене информацией через сеть Интернет необходимо:

7.1) Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;

7.2) Не вводить персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах;

7.3) Ограничить посещения сайтов сомнительного содержания;

7.4) Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;

7.5) Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;

7.6) Не открывать файлы полученные (скачанные) из неизвестных источников.

При подозрении в компрометации ключей электронной подписи/шифрования или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов связанных с деятельностью Регистратора необходимо незамедлительно обратиться в Регистратор.