ГПБ Инвестиции

УТВЕРЖДЕН

Генеральным директором

ООО «ГПБ Инвестиции»

Приказ №Д/050421/1 от 05.04.2021

# Рекомендации по соблюдению информационной безопасности клиентами ООО «ГПБ Инвестиции» в целях противодействия незаконным финансовым операциям

Москва

2021 год

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 17.04.2019 № 684-П), ООО «ГПБ Инвестиции» (далее по тексту - Брокер) 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 Брокера, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям иных документов Брокера. Перед заключением внимательно изучайте документы Брокера, регламентирующие предоставление услуг/сервисов, в частности ознакомьтесь с разделами, посвященными информационной безопасности.

Под защищаемой информацией понимается:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде вами и(или) работниками Брокера;
- информация об осуществляемых вами финансовых операциях;
- информация, необходимая Брокеру для авторизации вас как клиента Брокера в целях осуществления финансовых операций и удостоверения вашего права распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- ваши персональные данные.

Целью Рекомендаций являются доведение до вас информации:

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

Основные риски получения несанкционированного доступа к защищаемой информации:

- риск совершения финансовых операций с активами клиентов, в том числе путем формирования и отправки от имени клиента распоряжения на проведение финансовой операции;
- 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;
- риск повреждения программного обеспечения клиента, а также риск изменения, искажения, уничтожения или шифрования информации об активах клиента или данных самого клиента;
- риск разглашения конфиденциальной информации.

Несанкционированный доступ к защищаемой информации происходит посредством:

- кражи устройства клиента;
- удаленного доступа к устройствам клиента в результате взлома системы защиты;
- получения данных клиента для проведения/подтверждения проведения операций с помощью метода социальной инженерии;
- заражения устройства клиента вредоносным кодом.

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

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.
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 звонят клиенту, представляются сотрудниками техподдержки и опрашивают клиентов на наличие каких-либо технических неисправностей в устройстве клиента. Если неисправности имеются, злоумышленники просят клиента установить специальное программное обеспечение, после чего появляется возможность контроля над устройством клиента.

Рекомендации по защите информации от воздействия вредоносного кода:

- 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 (с регулярно и своевременно обновляемыми базами) и персональный межсетевой экран;
    - своевременно обновляйте операционную систему устройства, особенно в части обновлений безопасности;
    - регулярно осуществляйте проверку устройства на наличие вирусов;
    - используете парольную или иную защиту для доступа к устройству.

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

- Обеспечьте конфиденциальность:
    - блокируйте устройство после использования, используйте настройки устройства, требующие ввода пароля для его разблокировки и использования;
    - не передавайте третьим лицам и не оставляйте устройство без присмотра;
    - храните в тайне аутентификационные/идентификационные данные, используйте методы двухфакторной аутентификации, в случае компрометации немедленно примите меры для смены и/или 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 Брокера по возможности оцените ситуацию и уточните полномочия и процедуру через официальный канал связи с Брокером, указанный в договоре или на официальном сайте.

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.
4. Контроль подключения:
    - не используйте устройства третьих лиц для совершения финансовых операций или получения информации в отношении таких операций;
    - не работайте в сервисах Брокера с устройства, использующего подключение к общедоступной wi-fi сети.
5. Проявляйте осторожность и предусмотрительность:
    - 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;
    - внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Брокера 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 Брокеру только по номеру телефона, указанному в договоре или на официальном сайте Брокера. Имейте в виду, что от лица Брокера не могут поступать звонки или сообщения, в которых от вас требуют передать аутентификационные/идентификационные данные (логин, пароль, и т.д.), кодовое слово или СМС-код. Указанные сведения могут быть запрошены только если вы сами позвонили Брокеру.
    - имейте в виду,что если вы передаете ваш телефон и/или устройство другим лицам, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Брокера, которыми пользовались вы. В связи с этим при утере, краже телефона (SIM карты), используемого для получения СМС-кодов или доступа к системам Брокера с Мобильного приложения:
        - незамедлительно проинформируйте Брокера 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 Мобильном приложении.
    - при подозрении на несанкционированный доступ к сервисам Брокера и/или компрометацию устройства, с которого осуществляется доступ к таким сервисам, необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ к сервисам Брокера, обратившись к Брокеру;
    - 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;

- помните, наличие «эталонной» резервной копии вашего устройства (компьютера, смартфона) может облегчить и ускорить восстановление вашего устройства.