Рекомендации по информационной безопасности.

В соответствии с требованиями Положения Банка России от 20.04.2021 № 757-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" САО «Ганза» (далее — Общество) доводит до Вашего сведения информацию о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации:

- несанкционированный доступ к устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон, с помощью которого клиент может взаимодействовать с Обществом) влечет риск получения третьими лицами несанкционируемого доступа к защищаемой информации;

- несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии счета, другой значимой информации.

- несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

Оптимальным способом защиты от несанкционированного доступа третьих лиц является умение распознать злоумышленные действия.

Основными способами получения несанкционированного доступа к защищаемой информации являются:

- «Фишинг» - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. 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 часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и счетам клиента.

- Техника «Троянский конь» - 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 майнинга, использование IP для нелегальной торговли.

- Техника «Кви про Кво» - используется для внедрения вредоносного программного обеспечения в устройства. Злоумышленники звонят клиенту, представляются сотрудниками техподдержки компании и опрашивают клиентов на наличие каких-либо технических неисправностей в устройстве клиента. Если неисправности имеются,

злоумышленники просят клиента ввести определенную команду, после чего появляется возможность запуска вирусного программного обеспечения.

• Метод «Дорожное яблоко» - состоит в адаптации «троянского коня» и требует обязательного применения какого-то физического носителя информации. Злоумышленники могут предоставить клиенту загрузочные внешние носители информации, подделанные под носители с интересным и/или уникальным контентом.

В связи с чем, Общество доводит до Вашего сведения рекомендации по соблюдению информационной безопасности:

Использование программного обеспечения на Устройствах:

• использовать на устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии;

• регулярно проводить полную проверку устройств на вирусы и вредоносный код;

• прекратить использование устройства в случае обнаружения вирусов и вредоносного кода, до момента полного удаления вирусов и вредоносного кода.

Использовать на устройствах исключительно лицензионное ПО и операционные системы:

• регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на устройствах;

• не использовать на устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств;

• исключить использование средств удаленного администрирования на устройствах. Безопасность паролей:

• выбирать пароли самостоятельно. Проводить регулярную смену паролей;

• использовать сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками;

• не сохранять пароли в текстовых файлах на устройстве либо иных электронных носителях; • не хранить пароль совместно с устройством;

• не передавать третьим лицам пароли, коды доступа к устройству. Соблюдение правил безопасности в сети Интернет:

• при работе с устройств в сети Интернет удостовериться 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) держать его включённым и блокировать все незнакомые или подозрительные подключения;

• не отвечать на подозрительные сообщения, полученные с неизвестных адресов;

• не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты;

• не открывать и не использовать сомнительные Интернет - ресурсы на устройстве. Осуществление контроля подключения:

• не работать с устройств, использующих подключение к общедоступной wi-fi сети. Дополнительные рекомендации:

• для связи с Обществом по телефону и e-mail используйте контактные данные, указанный на официальном сайте Общества в сети Интернет.