«УТВЕРЖДЕНО»
Общим собранием участников
ООО ИК «Хамстер-Инвест»
(Протокол № 2024/09/18 от 18.09.2024г.)

Рекомендации по соблюдению информационной безопасности клиентами ООО ИК «Хамстер-Инвест» в целях противодействия незаконным финансовым операциям

Общество с ограниченной ответственностью Инвестиционная компания «Хамстер-Инвест» (далее – Общество) в рамках соблюдения требований 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» уведомляет клиентов Общества о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления (далее по тексту – третьи лица):

- несанкционированный доступ к техническим средствам, включая, но не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон или иное, с использованием которых клиентом Общества совершаются действия в целях осуществления финансовой операции или иные действий в рамках договора, заключенного с Обществом (далее по тексту – Устройства), влечет риск получения третьими лицами логина и пароля, используемых для доступа к Устройствам, что может повлечь за собой получение несанкционируемого доступа к защищаемой информации;
- несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риск разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, активах, о состоянии счетов, иной 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 аутентификационных данных, использование счетов и находящихся на них активов для прикрытия действий, носящих противоправный характер, совершения иных действий против воли клиента и направленных против его интересов.

Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой деструктивное воздействие на Устройства и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения клиентом своих обязательств по договору, заключенному с Обществом, или невозможности использования сервисов Общества для реализации своих намерений.

Для минимизации вышеуказанных рисков Обществом предпринимаются меры организационного и технического характера, направленные на предотвращение доступа третьих лиц к защищаемой информации. В то же время, в рамках защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования Устройств, в целях противодействия незаконным финансовым операциям, а также для предотвращения несанкционированного доступа к защищаемой информации, Общество рекомендует следующее:

Рекомендации по обеспечению безопасности Устройств:

- Использовать настройки Устройства, требующие ввода пароля для его разблокировки и использования. Блокировать Устройство после использования.
- Не передавать третьим лицам и не оставлять Устройства без присмотра.
- Не использовать Устройства третьих лиц для совершения финансовых операций или получения информации в отношении таких операций.
- Не работать с Устройства, использующего подключение к общедоступной wi-fi сети.

Рекомендации по использованию программного обеспечения на Устройстве:

- Использовать на Устройстве антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО в актуальном состоянии.
- Регулярно проводить полную проверку Устройства на наличие вирусов и/или иных вредоносных программ.
- Прекратить использование Устройства в случае обнаружения вирусов и/или иных вредоносных программ до их полного удаления с Устройства.
- Использовать на Устройстве исключительно лицензионное ПО и операционные системы.
- Регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на Устройствах.
- Не использовать на Устройстве ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.
- Исключить использование средств удаленного администрирования на Устройстве.

Рекомендации по использованию паролей:

- Выбирать пароли самостоятельно. Проводить регулярную смену паролей.
- Использовать 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, а также пароли доступа в информационную систему Общества, предназначенную для удаленного обслуживания клиента.

Рекомендации по соблюдению правил безопасности в сети Интернет:

- Не посещать сайты сомнительного содержания.
- Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.
- Не переходить по подозрительным ссылкам, полученным от неизвестных отправителей.
- 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.

Дополнительные рекомендации:

- Незамедлительно информировать Общество в случаях:
    - совершения или подозрения на совершение третьими лицами незаконных финансовых операций, несанкционированного доступа к защищаемой информации.
    - компрометации или подозрения на компрометацию аутентификационных данных и/или кодов, направляемых на номер мобильного телефона клиента.

- Соблюдать конфиденциальность и осуществлять защиту от несанкционированного доступа аутентификационных данных и/или кодов, направляемых на номер мобильного телефона посредством SMS - сообщения.

- В случае утраты (потери/хищении) мобильного телефона, с использованием которого клиентом совершались действия в целях осуществления финансовой операции, незамедлительно обратиться к оператору сотовой связи для осуществления блокировки сим - карты.

- Для связи с Обществом по телефону необходимо использовать только номер телефона, указанный на официальном сайте Общества в сети Интернет по адресу http://hamster-invest.ru , http://hamsterinvest.ru