Приложение № 1

УТВЕРЖДЕНО
Приказом Генерального директора
АО «ИК «Ай Ти Инвест»
от « 13 » августа 2024 г. № 24-13/08-2

Рекомендации по соблюдению правил информационной безопасности клиентами АО «ИК «Ай Ти Инвест» в целях противодействия незаконным финансовым операциям

Версия 3.0.

г. Москва, 2024 г.

Содержание

1. Общие положения

1.1. Настоящие «Рекомендации по соблюдению правил информационной безопасности клиентами АО «ИК «Ай Ти Инвест» в целях противодействия незаконным финансовым операциям» (далее – Рекомендации) разработаны в соответствии с Положением Банка России от 20.04.2021 г. № 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».
1.2. Целью разработки настоящих Рекомендаций является доведение до клиентов АО «ИК «Ай Ти Инвест» (далее – Общество) рекомендаций по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.
1.3. Основной задачей Общества в рамках процесса защиты информации клиентов от воздействия вредоносного кода является доведение до клиентов информации:

- О возможных рисках 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.

1.4. Рекомендации по соблюдению правил информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты) 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.
1.5. Настоящие Рекомендации не противоречат положениям внутренних нормативных документов Общества, касающихся информационной безопасности, защиты информации и защиты и обработки персональных данных.
1.6. Настоящие Рекомендации подлежат публикации на официальном сайте Общества в целях доведения их положений до сведения клиентов Общества.

2. Риск несанкционированного доступа

2.1. К основным рискам получения несанкционированного доступа к защищаемой информации, в том числе с использованием вредоносных программ, относятся:

- Риск разглашения информации конфиденциального характера: сведений об операциях, активах, состоянии счетов, подключенных услугах, персональных данных, иной значимой информации;
- Риск совершения юридически значимых действий, включая совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента;
- Риск воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов Общества для реализации своих намерений.

2.2. Наиболее распространенные способы получения несанкционированного доступа реализуются злоумышленниками с применением методов социальной инженерии. Возможными сценариями реализации угроз несанкционированного доступа могут являться:

- **Фишинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Один из самых распространенных способов фишинга заключается в отправке электронных писем от злоумышленников, которые выдают себя за представителей государственных органов или известных компаний, а также за близких и знакомых жертвы. Как правило, в электронных письмах от злоумышленников содержится ссылка на небезопасную страницу в информационно-телекоммуникационной сети «Интернет», на которой предлагается ввести свои личные данные. Зачастую такие сайты являются точной или приближенной копией известных сайтов.

- **«Троянский конь»** – техника мошенничества, основанная на расчете злоумышленников на любопытство, страх, сострадание и другие эмоции жертвы. В целях реализации данного вида мошенничества жертве отправляется по электронной почте, СМС-сообщения, в мессенджерах или социальных сетях сообщение с вложением, в котором якобы находятся компромат на знакомых, обновления антивируса, информация о социальных выплатах, результатах розыгрышей лотерей и т.д. На самом деле во вложениях таких сообщений находится вредоносная программа.
- Заражение устройства жертвы осуществляется также через рассылки по электронной почте, СМС-сообщения, в мессенджерах или социальных сетях сообщений, содержащих ссылки на внешние ресурсы. При переходе по ссылкам вредоносная программа устанавливается на устройство клиента. Далее с использованием вредоносного программного обеспечения злоумышленники получают полный контроль над устройством.

3. Рекомендации по защите информации от воздействия вредоносного кода

3.1. На устройствах, на которых хранятся ваши персональные, авторизационные данные и другая значимая информация, используйте лицензионное программное обеспечение, в том числе антивирусное программное обеспечение.
3.2. Своевременно обновляйте программное обеспечение и операционную систему на ваших устройствах. Настройте свое антивирусное программное обеспечение на автоматическое обновление вирусных баз и запуск с загрузкой операционной системы.
3.3. Периодически осуществляйте полную проверку своих устройств на предмет наличия вирусного и вредоносного программного обеспечения.
3.4. Настройте автоматическое сканирование съемных носителей при их подключении к устройству.
3.5. На компьютерах и ноутбуках для решения повседневных задач используйте учетную запись, не имеющую прав администратора.
3.6. При подозрениях на наличие вирусов и вредоносных программ ограничьте доступ устройства к информационно-телекоммуникационной сети «Интернет».

4. Рекомендации по защите информации от несанкционированного доступа

4.1. Не оставляйте без присмотра мобильные устройства, на которых хранятся ваши персональные, авторизационные данные и другая значимая информация.
4.2. Всегда устанавливайте и периодически изменяйте пароли на ваших устройствах. Рекомендуется использовать сложные пароли, удовлетворяющие следуюшим требованиям:
4.3. Длина пароля должна быть не менее 8 символов,
4.4. Пароль должен содержать минимум одну букву в верхнем регистре (A-Z), одну букву в нижнем регистре (a-z), одну цифру и один специальный знак или знак пунктуации. Не используйте простые пароли, содержащие осмысленные слова, даты рождения, номера телефонов или представляющие собой последовательности знаков на клавиатуре или повторяющихся символов.
4.5. Вводите логины и пароли только на сайтах в информационно-телекоммуникационной сети «Интернет», которым вы доверяете. Проверяйте адрес сайта и сертификат безопасности, расположенный рядом с адресной строкой в браузере. Наполнение мошеннического сайта может оказаться точной или приближенной копией сайта, за который его хотят выдать злоумышленники.
4.6. Не сохраняйте пароли на устройствах, к которым есть доступ третьих лиц.
4.7. При получении сообщений по электронной почте, СМС-сообщений, в мессенджерах или социальных сетях проверяйте отправителя. Будьте внимательны, так как мошеннический контакт может являться почти точной копией.
4.8. Внимательно изучайте ссылки перед переходом по ним. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http://, не https://), не переходите по этой ссылке.
4.9. Опасайтесь сообщений с обезличенными обращениями, такими как «Уважаемый клиент», или с обращениями по адресу вашей электронной почты.
4.10. Обращайте внимание на текст письма. Если в тексте письма присутствуют слова на иностранном языке, частые орфографические ошибки, специальные символы, такое письмо с большой вероятностью является фишинговым.
4.11. Сохраняйте спокойствие при получении сообщений со словами «Срочно», «Незамедлительно», «Только в течение часа/дня/недели». Мошенники рассчитывают на вашу панику и быстрые необдуманные решения, поэтому используют в фишинговых письма призывы к незамедлительному действию.

4.12. В случае утраты мобильного устройства или неожиданного прекращения работы SIM-карты незамедлительно обратитесь к своему оператору сотовой связи. Сообщите ему о необходимости блокировки абонентского номера и замены SIM-карты. Также рекомендуем незамедлительно сообщить о таком случае в Общество для выявления и предупреждения возможных несанкционированных операций.
4.13. В случае поступления СМС-сообщения или уведомления о совершенной операции, немедленно свяжитесь с Обществом, если вы не были инициатором такой операции.

При подозрении о компрометации авторизационных данных или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов незамедлительно обращайтесь в Общество по адресу электронной почты cybersecurity@d8.capital.