УВЕДОМЛЕНИЕ

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 и защите информации от воздействия вредоносных кодов

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

Настоящим Общество с ограниченной ответственностью Инвестиционная компания «Тренд» (далее по тексту – Общество) в соответствии с п.1.13 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, утвержденного Банком России 20.04.2021 № 757-П, доводит до сведения своих Клиентов, что при осуществлении финансовых операций следует принимать во внимание риски финансовых потерь (убытков), связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления (далее также – злоумышленники). Указанные риски могут быть обусловлены, в том числе, следующими ситуациями:

- кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа, посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени Клиента;
- кража или несанкционированный доступ к устройству, с которого Клиент пользуется услугами/сервисами Общества для получения данных, и/или несанкционированного доступа к сервисам с этого устройства;
- получение пароля, идентификатора доступа и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д., путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Клиента сообщить ему эти конфиденциальные данные или когда злоумышленник направляет поддельные почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства и/или совершению операций от имени Клиента;
- перехват почтовых сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Клиент использует электронную почту для информационного обмена с Обществом. Получение злоумышленником доступа к электронной почте Клиента также позволит осуществить ему отправку сообщений от имени Клиента Обществу.

Указанный выше перечень рисков не является исчерпывающим в виду многообразия ситуаций, которые могут возникать при совершении Клиентом финансовых операций.

Все риски, связанные с утратой и компрометацией учетных данных (логин, пароль) для доступа к информационным системам Общества и/или Клиента, несет Клиент.

Общество не несет ответственности в случаях финансовых потерь (убытков), понесенных Клиентом в связи с пренебрежением правилами информационной безопасности.

2. **Рекомендации по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям:**

- в обязательном порядке установите антивирусное программное обеспечение (далее – ПО) на персональном компьютере или ином устройстве Клиента, с помощью которого осуществляется взаимодействие с Обществом при совершении финансовых операций;
- своевременно обновляйте антивирусное ПО. По возможности используйте максимальный уровень безопасности в настройках антивирусного ПО. В этом случае антивирусная система будет проверять все объекты и при обнаружении вирусов и/или вредоносных кодов удалять их в автоматическом режиме, с уведомлением Клиента о данной операции, но без требования дальнейшего действия. Также при обнаружении антивирусной системой фишинговых сайтов, т.е. сайтов, имитирующих официальные сайты компаний, доступ на такие сайты будет ограничен в автоматическом режиме;
- не реже одного раза в неделю в автоматическом режиме осуществляйте полную проверку жесткого диска персонального компьютера или иного устройства Клиента, с помощью которого осуществляется взаимодействие с Обществом, на предмет наличия вирусов и вредоносного кода. Проверка должна осуществляться согласно расписанию, выставленному в настройках антивирусного ПО;
- при выборе антивирусного ПО отдавайте приоритет российским разработчикам, находящимся в Едином Реестре Российского программного обеспечения по адресу https://reestr.digital.gov.ru/. В антивирусные системы разработчиков, не входящие в данный Реестр, могут быть внедрены в программный код как неявные, так и недокументированные возможности, включая майнинг на оборудовании клиентов данного ПО;
- не используйте бесплатное антивирусное ПО, т.к. оно, как правило, очень ограничено по функционалу и не дает полноценной защиты от разных угроз в сети «Интернет». Используйте антивирусные системы с полным функционалом, которые работают по подписке, и имеют доступ к технической поддержке и помощи при нештатных ситуациях со стороны разработчика;
- подвергайте антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях;
- при использовании сети «Интернет» для обмена почтовыми сообщениями обязательно применяйте антивирусное ПО, разработанное специально для почтовых клиентов;
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание

файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) приостановите работу с системой до полного устранения неисправностей;

- не используйте персональный компьютер или иное устройство, с помощью которого осуществляется взаимодействие с Обществом (включая запуск Системы Интернет-трейдинга), для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети «Интернет» чаще всего распространяются компьютерные вирусы;
- не открывайте файлы, полученные по электронной почте от неизвестных отправителей, а также не переходите по ссылкам в этих письмах. Особую опасность заражения персонального компьютера или иного устройства Клиента могут представлять файлы со следующими расширениями: *.ade, *.adp, *.bas, *.bat; *.chm, *.cmd, *.com, *.cpl; *.crt, *.eml, *.exe, *.hlp; *.hta, *.inf, *.ins, *.isp; *.jse,*.lnk, *.mdb, *.mde; *.msc,*.msi, *.msp, *.mst; *.pcd, *.pif, *.reg, *.scr; *.sct,*.shs, *.url, *.vbs; *.vbe,*.wsf, *.wsh, *.wsc. Часто при пересылке писем для скрытия фактического расширения файлов злоумышленники могут увеличить длину имени файла, в таком случае расширение файла может не отображаться. В этом случае вложенные файлы необходимо сохранять отдельно и запускать их проверку антивирусным ПО.

3. Меры 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

- никогда не сообщайте третьим лицам, включая работников Общества, идентификаторы пользователя и пароли, предназначенные для использования устройств Клиента, с помощью которых осуществляется взаимодействие с Обществом в целях совершения финансовых операций (персональный компьютер, планшет, ноутбук, мобильный телефон, смартфон и т.д.);
- не допускайте к устройствам, с помощью которых осуществляется взаимодействие с Обществом в целях совершения финансовых операций, их материальным носителям, а также к информации, содержащей коды, логины, пароли, ключи, обеспечивающие доступ к указанным устройствам (далее – ключевая информация) лиц, не уполномоченных Клиентом на совершение финансовых операций, не допускайте копирование такой информации. Ключевую информацию необходимо хранить на отчуждаемом носителе (USB-накопителе) и хранить его в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа к нему третьих лиц; в случае, если избежать копирования и/или доступа к таким данным не удается, необходимо сообщить Обществу о данном факте;
- не записывайте логины, пароли и иную ключевую информацию на бумаге, не храните их на видном месте (на рабочем столе, на мониторе, на/под клавиатурой и т.п.), не

используйте в качестве места хранения ключевой информации жесткие диски средств вычислительной техники. Храните указанную информацию в надежном месте, доступ к которому третьим лицам исключен;

- при составлении пароля используйте прописные и строчные буквы, цифры и специальные символы;
- регулярно, не реже чем раз в три месяца, производите смену пароля;
- не используйте одинаковые логин и пароль для доступа к разным устройствам и системам, т.к. получив доступ к учетным данным одной системы, злоумышленники тем самым получат доступ сразу ко всем системам;
- не разглашайте третьим лицам пароли, коды доступа, ключи от электронных ресурсов, предоставленных Обществом, в том числе от Системы интернет-трейдинга;
- Общество не рассылает электронные письма, SMS-сообщения или другие сообщения с просьбой сообщить Обществу ключевую информацию Клиента. Общество ни при каких обстоятельствах не может требовать от Клиента разглашения паролей, в том числе от электронных ресурсов, предоставленных Клиенту Обществом. В случае, если у Клиента имеются сомнения, необходимо связаться с Обществом самостоятельно и уточнить, исходит ли запрос от уполномоченных работников Общества;
- никогда не пересылайте файлы с конфиденциальной информацией, в том числе ключевой информацией, по электронной почте, через SMS-сообщения и мессенджеры (WhatsApp, Telegram, Viber, Skype и др.);
- своевременно устанавливайте обновления операционной системы, в особенности критические обновления безопасности;
- обновляйте программное обеспечение и его компоненты только из проверенных источников, находящихся в ведении их разработчиков;
- при работе в сети «Интернет» не допускайте установку программного обеспечения из недостоверных или сомнительных источников, как правило, оно маскируется под установку плагинов;
- входите в систему под учетной записью пользователя, не имеющей прав администратора. Без необходимости не используйте учетную запись с правами администратора;
- не используйте средства удалённого администрирования (TeamViewer, AnyDesk, Ammyy Admin, Screen Sharing, Real VNC, AeroAdmin и подобные);
- не подтверждайте запросы к управлению персональным компьютером или иным устройством Клиента, с помощью которого осуществляется взаимодействие с Обществом, при использовании программ для организации видео-конференций (Zoom и подобные);
- не используйте функцию сохранения (автозаполнения) логина и пароля в установках браузера, это позволит при получении даже кратковременного доступа к персональному компьютеру или иному устройству Клиента, с помощью которого осуществляется взаимодействие с Обществом, авторизоваться в финансовых системах и сервисах Клиента;

- не подключайтесь на своих персональных компьютерах и иных устройствах к сторонним публичным WI-FI сетям, т.к. они не гарантируют защищенность передачи данных;
- не подключайте к зарядным устройствам, находящимся в общественных местах, мобильные устройства (планшеты, телефоны, коммуникаторы и т.д.) без использования на зарядном проводе модулей блокировки синхронизации данных;
- при обнаружении, что пароль от устройства и/или системы Клиента скомпрометирован, незамедлительно смените пароль на новый (если такая возможность предусмотрена), известный только Клиенту, с учетом вышеописанных требований к сложности состава пароля;
- при обнаружении, что ранее действующий пароль не срабатывает и не позволяет войти в Систему интернет-трейдинга, как можно быстрее обратитесь к Обществу для получения инструкций по смене пароля;
- в случае получения Клиентом уведомления об операции, которую Клиент не совершал, незамедлительно сообщите об этом Обществу;
- незамедлительно уведомить Общество об утрате (потере, хищении) устройства Клиента, с использованием которого совершались действия в целях осуществления финансовой операции, а также о компрометации ключа, пароля или иной ключевой информации;
- при утрате, краже телефона/планшета/смартфона незамедлительно заблокируйте SIM-карту мобильного оператора сотовой сети и обратитесь за ее перевыпуском.
- для защиты от незаконного перевыпуска SIM-карты Клиента следует написать заявление мобильному оператору сотовой сети о запрете данного действия без предоставления оригинала паспорта Клиента.

В целях предотвращения несанкционированного доступа к защищаемой информации путем использования злоумышленниками ложных (фальсифицированных) ресурсов сети Интернет, Клиентам Общества рекомендуется предпринимать следующие меры:

- обращаться только на официальный web-сайт Общества в сети Интернет, адрес которого указан в официальных документах Общества или сообщен Обществом Клиенту при заключении договора. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Клиенту под каким-либо предлогом может предлагаться ввести конфиденциальную информацию, зачастую такие web-сайты являются почти точной копией web-сайтов компаний и предназначены для сбора конфиденциальной информации обманным путем;
- перед просмотром электронного письма всегда проверять адрес отправителя. Адрес электронной почты отправителя изменить очень просто, поэтому необходимо соблюдать бдительность, т.к. строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией адреса электронной почты Общества;
- внимательно читать текст электронного письма. Если в тексте присутствуют слова на иностранном языке, специальные символы, орфографические или грамматические

ошибки, и т.п., скорее всего это электронное письмо, отправленное злоумышленниками;

- следует опасаться безличных обращений, таких как «Уважаемый пользователь», или обращений по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия;
- всегда сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Клиента действовать быстро и необдуманно, многие поддельные сообщения электронной почты пытаются убедить Клиента в том, что его счету угрожает опасность, если лицо немедленно не обновите критически важные данные;
- внимательно анализировать ссылки, содержащиеся в тексте электронного письма. Такие ссылки могут быть почти точной копией подлинных, однако они способны перенаправить Клиента на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), то не следует переходить по ней;
- следует ограничить работу в сети «Интернет» только с надежными сайтами.

При подозрении в компрометации ключей или несанкционированного движения ценных бумаг, денежных средств или иных финансовых активов Вам необходимо оперативно поставить в известность Общество, позвонив по телефону +7 (495) 151-41-00 (доб.117).