ООО «ТМ-ТРАСТ» (далее – Общество) в рамках соблюдения требований Положения Банка России от 20.04.2021г. №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 получения несанкционированного доступа к защищаемой информации* с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Доступ со стороны третьих лиц может повлечь за собой:

- риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации;
- совершение юридически значимых действий, включая: совершение операций с доступными активами, 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.

В целях для предотвращения 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, Общество *рекомендует*:

1. Организовать режим использования устройства, с использованием которого совершаются действия в целях осуществления финансовой операции (далее – «устройство») таким образом, чтобы исключить возможность его несанкционированного использования.

- настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;
- хранение, использование устройства с целью избежать рисков кражи и/или утери;
- ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

2. Используйте на вашем устройстве только лицензионное программное обеспечение, полученного из доверенных источников.
3. Устанавливайте обновления операционной системы и интернет-браузера вашего устройства, выпускаемые компанией-производителем для устранения выявленных в них уязвимостей.
4. При использовании паролей:

- не записывайте пароли, служащие для доступа к устройству на бумажных носителях или в файлах на жестком диске вашего компьютера. Не сообщайте их другим лицам.
- рекомендуется использовать для доступа к устройству сложные пароли, длиной не менее 8 символов, состоящий как минимум из символов: букв латинского алфавита в верхнем и нижнем регистре, цифр (0-9), специальных символов и знаков пунктуации (!@#$%^&*).
- не используйте простые пароли, представляющие собой осмысленные слова, дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (555555, 444js77777).

5. Для защиты от вредоносного программного обеспечения необходимо использовать лицензионное антивирусное программное обеспечение, функционирующее в автоматическом режиме, которое регулярно обновляется. Не отключайте антивирусное программное обеспечение ни при каких обстоятельствах.
6. При использовании сети Интернет

- не открывайте письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходите по содержащимся в таких письмах ссылкам;
- не вводите персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах;
- ограничьте посещения сайтов сомнительного содержания;
- не сохраняйте пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
- не нажимайте на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
- не открывайте файлы полученные (скачанные) из неизвестных источников.