Рекомендации Клиентам ООО «УК «Горизонт» по соблюдению информационной безопасности в целях противодействия незаконным финансовым операциям

Москва, 2019 г.

1. Общие положения

1.1. В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-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» Общества с ограниченной ответственностью «Управляющая компания «Горизонт» (далее по тексту - Общество) доводит до сведения своих клиентов:

- рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям;
- рекомендации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- меры по предотвращению несанкционированного доступа к защищаемой информации.

2. Возможные риски получения несанкционированного доступа к защищаемой информации

2.1. Общество уведомляет своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, такие риски включают в себя**,** но не ограничиваются:

- Несанкционированным доступом со стороны третьих лиц к Вашим техническим устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон), что может повлечь за собой получение третьими лицами доступа к защищаемой информации.
- Кражой пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода и использование третьими лицами указанных данных с других устройств для несанкционированного доступа.
- Установкой на техническое устройство вредоносного кода, который позволит третьим лицам осуществить финансовые операции от Вашего имени.
- Использованием третьими лицами утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту.
- Получением пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда третье лицо представляется сотрудником Организации или техническим специалистом и просит Вас сообщить ему эти конфиденциальные данные или направляет сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства.
- Перехватом электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, в случае, если Ваша электронная почта используется для информационного обмена с Обществом или в случае получения доступа к вашей электронной почте, отправка сообщений от Вашего имени в Общество.

2.2. Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, другой значимой информации.

2.3. Несанкционированный 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.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации и рекомендации по защите информации от воздействия вредоносного кода

3.1. Общество уведомляет своих клиентов о мерах, позволяющих снизить риски несанкционированного доступа к защищаемой информации, снизить риск финансовых потерь включая, но не ограничиваясь:

- Организация надлежащего контроля за персональными компьютерами, мобильными или иными устройствами, с использованием которых совершаются действия в целях осуществления финансовых операций (далее – устройства);
- Регламентация доступа к устройствам и запрет доступа к устройствам третьих лиц;
- Использование на устройствах исключительно лицензионного программного обеспечения;
- Установление надежных логинов и паролей для доступа к устройствам и электронному почтовому ящику, а также оперативная замена логинов и/или паролей в случае их компрометации и/или утраты устройств;
- Использование специализированного программного обеспечения, обеспечивающего защиту устройств от вредоносного кода (антивирусных программных средств);
- Организация регулярного обновления безопасности операционных систем и антивирусных баз данных;
- Ограничение возможности загрузки и установки на устройства программ и компонентов, полученных из ненадежных источников;
- Запрета запуска файлов, загруженных с ненадежных интернет-сайтов и полученных от неизвестных адресатов (в том числе, посредством электронной почты);
- Запрета на использование открытых общедоступных сетей Wi-Fi при взаимодействии с Обществом;
- Обеспечение сохранности и секретности аутентификационных данных, а также ключей электронной подписи при их наличии;
- Оперативное уведомление Общества об утрате (хищении) ключевых носителей и иных случаях компрометации ключей электронной подписи, при их наличии, используемых в программном обеспечении Общества;