Рекомендации по защите информации

в целях противодействия незаконным финансовым операциям

Настоящие рекомендации по защите информации в целях противодействия незаконным финансовым операциям разработаны ООО УК “СМАРТС-ИНВЕСТ” (далее - Общество) в соответствии с требованиями 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" и направлены на защиту информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

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

Клиенты Общества несут риски негативных последствий вследствие следующих обстоятельств:

- несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии счета, имуществе, переданном в доверительное управление, другой значимой информации;
- несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски утраты, потери (хищения) идентификаторов доступа клиента (в случае их применения), с использованием которых осуществляются финансовые операции;
- воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции;
- совершение в отношении клиента иных противоправных действий, связанных с информационной безопасностью.

2. В целях 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, для контроля конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременного обнаружения воздействия вредоносного кода рекомендуем принимать следующие меры:

- использовать и хранить устройство таким образом, чтобы исключить возможность его хищения и несанкционированного использования;
- использовать современные и актуальные методы блокировки устройств (TouchID, FaceID, Пин-код и др.)

- использовать на устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии;
- регулярно проводить полную проверку устройств на вирусы и вредоносный код;
- прекратить использование устройства в случае обнаружения вирусов и вредоносного кода, до момента полного удаления вирусов и вредоносного кода.
- регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на устройствах;
- использовать только лицензионное ПО, не использовать на устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств;
- исключить использование средств удаленного администрирования на устройствах.
- выбирать пароли самостоятельно. Проводить регулярную смену паролей;
- использовать сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов.
- 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.
- при работе с устройств в сети Интернет удостовериться в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка);
- не отвечать на подозрительные сообщения, полученные с неизвестных адресов;
- 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.
- не работать с устройств, использующих подключение к общедоступной wi-fi сети.
- для связи с Обществом по телефону и e-mail используйте контактные данные, указанный на официальном сайте Общества в сети Интернет.

Настоящие рекомендации подлежат доведению до сведения клиентов путем размещения на официальном сайте Управляющей компании в информационно-телекоммуникационной сети Интернет по адресу: http://www.smarts-invest.ru.