«Утверждено»
Приказом Генерального директора от «31» мая 2019 года
Общества с ограниченной ответственностью
Микрокредитная компания «ТВОИ ПЛЮС»
Н.А. Гутара


РЕКОМЕНДАЦИИ
по противодействию совершению незаконных финансовых операций при нарушении штатного функционирования средства вычислительной техники.

Настоящий документ разработан в соответствии с требованиями 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 (утв. Банком России 17.04. 2019 г. № 684-П).

Рекомендации

АСП - аналог собственноручной подписи, в качестве которого рассматривается простая электронная подпись, формируемая в соответствии с требованиями Соглашения об использовании аналога собственноручной подписи и законодательства Российской Федерации. СМС-код – предоставляемый Клиенту посредством СМС-сообщения (SMS) уникальный конфиденциальный символьный код (сгенерированный пароль), который представляет собой ключ электронной подписи в значении, придаваемом данному термину п. 5 ст. 2 Федерального Закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» СМС-код используется Клиентом для подписания электронных документов в ходе дистанционного взаимодействия с Обществом. Получив СМС-код не сообщайте его никому, в том числе и сотрудникам Общества, не записывайте его на бумаге, там, где он будет доступен другим лицам.
Мобильный телефон - используется Клиентами Общества для получения одноразовых паролей в СМС-сообщениях, а также для работы с мобильным приложением Общества. При использовании мобильного телефона рекомендуется придерживаться следующих советов: При взаимодействии с Обществом указывайте в качестве основного номера телефона номер,

который принадлежит Вам лично (контракт на услуги сотовой связи, заключен на Ваше имя). Устанавливайте мобильное приложение Общества на телефонный аппарат, который принадлежит Вам и постоянно находится в Вашем распоряжении. Включите запрос кода-пароля SIM-карты при включении телефона. При поддержке телефоном соответствующей функции, выполните следующие действия:

1. Включите блокирование экрана телефона после определенного времени неактивности.
2. Включите запрос кода-пароля телефона, отпечатка пальца или графического ключа для разблокирования телефона.
3. Установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки.
4. Включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона.
5. Установите запрет на установку в телефон приложений из ненадежных источников.

При установке новых приложений на телефон обращайте внимание на запрашиваемые ими разрешения. Не давайте приложениям разрешение на чтение СМС, если такой доступ не нужен им для выполнения их основных функций.

Не переходите по ссылкам из СМС сообщений, особенно если Вы не ждали такие сообщения. Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление). В случае утраты телефона воспользуйтесь функцией поиска телефона, если ранее ее активировали. Если с использованием функции поиска найти телефон не удалось или Вы ранее не активировали эту функцию, обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном СИМ-карты и выпуска новой. Если на утерянном телефоне установлено мобильное приложение Общества, дополнительно к действиям, указанным в предыдущем абзаце, с любого телефона обратитесь на горячую линию Общества по номеру телефона 8-812-777-78-72 и попросите оператора «отвязать» утерянный телефон от вашей учетной записи в системе дистанционного обслуживания.

Защита от вирусов Вирусы – это программы для компьютеров или мобильных устройств, предназначенные для нанесения вреда. Функционал вирусов может быть разным: показ нежелательной рекламы, кража паролей (в том числе, из СМС-сообщений) и данных банковских карт, совершение незаконных финансовых операций от имени клиента. Практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств. Отсутствие вирусов на устройствах (компьютерах, сотовых телефонах, планшетах), с которых Вы работаете с системами дистанционного обслуживания Общества, является залогом безопасности Ваших денежных средств. Во избежание заражения вирусами Вашего компьютера, следуйте таким советам:

1. Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление).
2. Установите и регулярно обновляйте (не отключайте автоматическое обновление) антивирусную программу.
3. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.
4. Проверяйте антивирусной программой файлы, полученные из Интернет или со съемных носителей (флешек) до их использования.

Во избежание заражения вирусами Вашего мобильного устройства:

1. Регулярно обновляйте операционную систему и установленные в ней приложения (не отключайте автоматическое обновление).
2. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.
3. Установите запрет на установку в телефон приложений из ненадежных источников.