«Утверждено»
Приказом генерального директора от 13.12.2023
Общества с ограниченной ответственностью
Микрокредитная компания «М-Деньги»

Рекомендации

по противодействию совершению незаконных финансовых операций

Настоящий документ предназначен для ознакомления клиентов (далее по тексту – Клиент, Клиенты) ООО МКК «М-Деньги» (далее по тексту – Компания) с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить им совершить незаконные финансовые операции от имени клиентов.

1. Пароль от личного кабинета. Пароль используется Клиентами Компании для доступа в личный кабинет. Пароль должен состоять из букв верхнего и нижнего регистра. Также в нем должны присутствовать цифры**.** Компания рекомендует вам придумать длинный и сложный пароль, чтобы его было труднее подобрать. Однако Компания никак не может проверить его уникальность. Если вы воспользуетесь тем же самым паролем, которым защитили еще десяток аккаунтов на других сервисах, то утечка данных с любого из них поставит ваши данные под угрозу. Поэтому мы рекомендуем для каждого аккаунта — придумывать уникальный пароль.

2. Восстановление пароля. Если вы забыли пароль от Личного кабинета, вы можете отправить SMS с его восстановлением на телефон, который был указан при регистрации.

3. Мобильный телефон. Мобильный телефон используется Клиентами Компании для получения одноразовых паролей в SMS- сообщениях. При использовании мобильного телефона рекомендуется придерживаться следующих советов:
— При взаимодействии с Компанией указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (контракт на услуги сотовой связи, заключен на Ваше имя);
— Включите запрос пин-кода SIM-карты при включении телефона;
При поддержке телефоном соответствующей функции, выполните следующие действия:
— Включите блокирование экрана телефона после определенного времени неактивности;
— Включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокирования телефона;
— Установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки;
— Включите и настройте функцию поиска, удаленного блокирования и удалённой очистки потерянного телефона;
— 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 SMS, если такой доступ не нужен им для выполнения их основных функций;
— Не переходите по ссылкам из SMS и 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 SIM-карты и выпуска новой;
— При утере телефона обратитесь на горячую линию Компании по номеру телефона 88005559532 и попросите оператора «отвязать» утерянный телефон от вашей учётной записи в системе дистанционного обслуживания Компании.

4. 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 SMS-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 Компании, является залогом безопасности Ваших денежных средств. Во избежание заражения вирусами Вашего компьютера или мобильного устройства, следуйте следующим советам:
— Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление);
— Установите и регулярно обновляйте (не отключайте автоматическое обновление) антивирусную программу;
— 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;
— Проверяйте антивирусной программой файлы, полученные из Интернет или со съемных носителей (флешек) до их использования.