Общество с ограниченной ответственностью Микрокредитная компания «Гиллион» (ООО МКК «Гиллион»)

ИНН 2465177117, КПП 246501001, ОГРН 1182468006016
660131, Красноярский край, город Красноярск, Ястынская улица, дом 19а помещение 213, кабинет 1

РЕКОМЕНДАЦИИ
по противодействию совершения незаконных финансовых операций

1. ВВЕДЕНИЕ

Настоящий документ предназначен для ознакомления Клиентов ООО МКК «Гиллион» (далее по тексту - *«Общество»*) с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить им совершить незаконные финансовые операции от имени Клиентов Общества.

В настоящее время активно осуществляется внедрение современных цифровых технологий в различные сферы жизни и производства. Финансовые организации предлагают своим Клиентам большой выбор инструментов для удаленного взаимодействия, позволяющий Клиентам экономить своё время и совершать финансовые операции без личного обращения в офис финансовой организации.

Необходимо отметить, что использование технологий удаленного взаимодействия, несет с собой определенные риски, главным из указанных рисков является незаконное совершение злоумышленниками финансовых операций от имени Клиентов финансовых организаций с целью хищения денежных средств Клиентов.

Выполнение несложных рекомендаций, указанных в настоящем документе, позволит Клиентам Общества свести риск совершения незаконных финансовых операций от их имени к минимуму.

2. РЕКОМЕНДАЦИИ

2.1. Мобильный телефон

Мобильный телефон используется Клиентами Общества для получения Кода подтверждения, Уникального кода, одноразовых паролей в SMS-сообщениях.

При использовании мобильного телефона следует придерживаться следующих советов:

1. При взаимодействии с Обществом указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (договор на услуги сотовой связи, заключен на Ваше имя);

2. Включите запрос пин-кода SIM – карты при включении телефона;

<u>При поддержке телефоном соответствующей функции, выполните следующие действия:</u>

- включите блокирование экрана телефона после определенного времени неактивности;

• включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокировки телефона;

• установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки;

• включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона;

• установите запрет на установку в телефон приложений из ненадлежащих источников.

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

4. Не переходите по ссылкам из SMS и сообщений, особенно если ВЫ не ждали такие сообщения.

5. Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление).

6. 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.

2.2. ПИН-код

ПИН-код - это секретная комбинация цифр, используемая для подтверждения операций с Вашей банковской карты международной платежной системы MasterCard, Visa или МИР.

При использовании ПИН-кода рекомендуется: не сообщать ПИН-код третьим лицам, включая сотрудников Общества, не записывать его на Вашей банковской карте, не хранить записанный ПИН-код там, где он будет доступен третьим лицам.

2.3. 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 Обществом, является залогом безопасности Ваших денежных средств.

Во избежание заражения вирусами Вашего мобильного устройства, рекомендуется:

1. Регулярно обновляйте операционную систему и установленные в ней приложения (включите 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 ненадлежащих источников.