Общество с ограниченной ответственностью
«Микрокредитная Компания «АВА-Финанс»

420034, Россия, Республика Татарстан, г. Казань, ул. Декабристов 85б
Тел. (843) 240-99-91

«Утверждаю»
Директор
ООО «АВА-Финанс»
Николин Д.В.
15 июля 2019 г.

РЕКОМЕНДАЦИИ
по противодействию совершению незаконных финансовых операций для клиентов ООО «АВА-Финанс»

Настоящий документ предназначен для ознакомления клиентов ООО МКК «АВА-Финанс» (далее Общество) с рекомендациями ЦБ РФ о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также о мерах по предотвращению 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, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.
Основным риском для клиентов Общества является незаконное совершение злоумышленниками финансовых операций от их имени с целью хищения денежных средств клиентов либо их персональных данных для совершения противоправных действий.
Выполнение несложных рекомендаций, которые мы предлагаем нашим клиентам в настоящем документе, позволит свести риск совершения незаконных финансовых операций от их имени к минимуму.

Рекомендации

Основное средство связи клиента и сотрудника Общества это **Мобильный телефон.**
Мобильный телефон используется Обществом для отправки SMS-сообщений клиентам и получения обратной связи.
При использовании мобильного телефона клиентам 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).

- Взаимодействуйте с сотрудниками Общества только с телефонного аппарата, который принадлежит Вам и постоянно находится в Вашем распоряжении.
- Включите запрос пин-кода 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 пин-кода 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 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.

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 сотрудниками 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 сети 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.

Паспортные данные

Паспортные данные клиента могут быть использованы злоумышленниками для получения займов.

Во избежание использования ваших персональных данных:

1. Храните паспорт в труднодоступном месте.
2. Не передавайте паспорт или копии страничек паспорта посторонним людям
3. Не размещайте свои паспортные данные (копии паспорта) в интернете.
4. Не сообщайте паспортные данные по телефону незнакомым людям.

Договор микрозайма

Договор микрозайма клиента с Обществом содержит информацию о персональных данных Клиента, а также информацию о совершенных финансовых операциях Клиента.

Во избежание использования ваших персональных данных:

1. Храните договор микрозайма в труднодоступном месте.
2. Не передавайте договор микрозайма третьим лицам.
3. Не выбрасывайте договор до истечения срока действия договора.