БЫСТРОЗАЙМ
время – деньги!

РЕКОМЕНДАЦИИ

по противодействию совершению незаконных финансовых операций

1. Введение

Настоящий документ предназначен для ознакомления клиентов ООО МКК Быстро-Займ» (далее по тексту – Клиент, Клиенты) с рекомендациями по предотвращению риска несанкционированного доступа злоумышленников к защищаемой информации, с целью осуществлению финансовых операций (совершения незаконных финансовых операций) лицами не обладающими правом их осуществления от имени клиентов ООО МКК «Быстро-Займ».

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

ООО МКК «Быстро-Займ» рекомендует:

2. Рекомендации

Кодовое слово

Кодовое слово – это секретное слово, выбранное Клиентом, которое среди прочих данных используется сотрудниками Компании для аутентификации Клиента по телефону.

При использовании кодового слова рекомендуется придерживаться следующих советов:

Выбирайте кодовое слово таким образом, чтобы его было сложно угадать даже людям, которые хорошо Вас знают. Не выбирайте в качестве кодового слова Ваше имя или фамилию, имена и фамилии близких вам людей, даты рождения и другую информацию о Вас, которая известна многим людям.

Не сообщайте кодовое слово никому кроме сотрудников Компании, отвечающих на Ваш звонок на горячую линию Компании.

Если Вы записываете кодовое слово чтобы его не забыть, не храните запись с кодовым словом в местах, доступных для других лиц.

Пин-код

Пин-код – это секретная комбинация цифр, используемая для подтверждения операций с Вашей картой.

При использовании пин-кода рекомендуется придерживаться следующих советов:

Обращаться с пин-кодом необходимо так же, как и с пин-кодом любой банковской карты: не сообщать его никому, включая сотрудников Общества, не хранить записанный пин-код там, где он будет доступен другим лицам, не записывать его на банковской карте.

Мобильный телефон

Мобильный телефон используется Клиентами Компании для получения одноразовых паролей в SMS-сообщениях.

При использовании мобильного телефона рекомендуется придерживаться следующих советов:

При обращении в ООО МКК «Быстро-Займ» 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:

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 системами дистанционного обслуживания Компании, является залогом безопасности Ваших денежных средств.

Во избежание заражения вирусами Вашего компьютера и мобильного устройства, 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.
5. Установите запрет на установку в телефон приложений из ненадежных источников.
6. Не передавайте третьим лицам документы или устройства, при помощи которых выполняется управление финансовыми операциями (паспорт, доверенность, мобильные устройства, персональные компьютеры и т.д.).
7. Используйте средства физического контроля доступа ко всем средствам вычислительной техники (мобильные устройства, персональные компьютеры и т.д.).
8. Не передавайте третьим лицам логины и пароли доступа к средствам вычислительной техники.
9. Используйте надежные пароли и регулярно их меняйте.
10. Остерегайтесь почтовых вложений и загружаемых из Интернета модулей.
11. Установите, поддерживайте и применяйте антивирусные программы.
12. Установите и используйте межсетевые экраны.
13. Удаляйте неиспользуемые программы и учетные записи пользователей, надежно удаляйте все данные на выводимом из эксплуатации средствах вычислительной техники.
14. Создавайте архивные копии важных файлов, папок и программ.
15. Устанавливайте обновления для программного обеспечения.
16. Ограничивайте доступ к ценным и конфиденциальным данным.