РЕКОМЕНДАЦИИ

ООО МКК «Лига денег»
(ОГРН 1147746399129/ ИНН7702836198)

по противодействию совершению незаконных финансовых операций

1. Введение

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

В эпоху бурного развития цифровых технологий финансовые организации, некредитные финансовые организации (далее -НФО) предлагают своим Клиентам большой выбор инструментов для удаленного взаимодействия, позволяющих Клиентам совершать финансовые операции без визита в офис финансовой организации и НФО.

Использование таких инструментов сильно повышает удобство взаимодействия Клиентов с финансовыми организациями и НФО, но одновременно несет с собой и риски, связанные с использованием цифровых технологий. Главным из указанных рисков является незаконное совершение злоумышленниками финансовых операций от имени Клиентов финансовых организаций и НФО с целью хищения средств Клиентов финансовых организаций.

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

2. Рекомендации

Кодовое слово

Кодовое слово – это секретное слово, выбранное Клиентом, которое среди прочих данных используется сотрудниками финансовых организаций и НФО 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, НФО и финансовой организации, 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:

Не сообщать его никому, включая сотрудников Компании, финансовой организации, не записывать его на карте, не хранить записанный пин-код там, где он будет доступен другим лицам.

Мобильный телефон

Мобильный телефон используется Клиентами Компании/финансовой организации для получения одноразовых паролей в SMS-сообщениях, а также для работы с мобильным приложением Компании/финансовой организации/НФО.

При использовании мобильного телефона рекомендуется придерживаться следующих советов:

При взаимодействии с НФО/финансовой организацией 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, включите блокирование экрана телефона после определенного времени неактивности.

При поддержке телефоном соответствующей функции, включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокирования телефона.

При поддержке телефоном соответствующей функции, установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки.

При поддержке телефоном соответствующей функции, включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона.

При поддержке телефоном соответствующей функции, 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).

Клиент Компании обязан не передавать третьим лицам SIM-карты, которые обеспечивают возможность использования их личного номера мобильного телефона, а также предпринимать все меры, необходимые для того, чтобы третьи лица не получили возможность использования указанной SIM-карты.

Клиент обязан уведомить Компанию об изменении контактной информации, используемой Компанией для его аутентификации, для целей предотвращения получения третьими лицами информации, относящейся к осуществлению Клиентом финансовых операций.

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. Однако, практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств.

Для защиты от несанкционированного доступа к компьютерам или мобильным устройствам Клиентам рекомендуется соблюдать следующие меры:

Крайне осторожно относиться к программам и документам Word/Excel, которые получаете из телекоммуникационной сети «Интернет». Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверить их на наличие вирусов.

Использовать специализированные антивирусы, проверяющие файлы, к которым идет обращение. Если это по какой-либо причине невозможно, регулярно проверять свои устройства обычными антивирусными программами.

Не запускать непроверенные файлы, в том числе полученные из компьютерной сети.

Использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно проверять их одним или несколькими антивирусами.

Все это приводит к необходимости ограничения круга лиц, допущенных к Вашим компьютерам или мобильным устройствам. Как правило, наиболее часто подвержены заражению “многопользовательские” персональные компьютеры.

Для предотвращения несанкционированного доступа к данным Клиента, используемым Компанией для его аутентификации, Клиент обязуется обеспечить конфиденциальность аутентификационных данных, хранение их образом, исключающим доступ к ним третьих лиц, а в случае, если такой доступ имел место или если у Клиента имеются основания полагать, что он имел место - незамедлительно связаться с Компанией по телефону, указанному на веб-сайте Компании по адресу https://www.ligadeneg.ru/ и выполнить указанные Компанией действия.

Клиент полностью несет риск всех неблагоприятных последствий, которые могут наступить в связи с неисполнением им обязанностей и рекомендаций, указанных в настоящем документе.