РЕКОМЕНДАЦИИ
по противодействию совершению незаконных финансовых операций

Введение

Настоящий документ предназначен для ознакомления клиентов ООО Ломбард “Меридиан” с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить злоумышленникам совершить незаконные финансовые операции. Мы живем в мире бурного развития цифровых технологий, многие финансовые организации предлагают своим клиентам большой выбор инструментов для удаленного взаимодействия, позволяющих клиентам совершать финансовые операции без визита в офис финансовой организации. Использование таких инструментов сильно повышает удобство взаимодействия клиентов с финансовыми организациями, 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 с целью хищения средств клиентов. Выполнение несложных рекомендаций, приведенных в настоящем документе, позволит свести риск совершения незаконных финансовых операций от их имени к минимуму.

Используемые термины

Кодовое слово - это секретное слово, выбранное Клиентом, которое среди прочих данных используется сотрудниками финансовой компании для аутентификации Клиента по телефону.

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

SMS - технология приёма и передачи коротких текстовых сообщений с помощью сотового телефона. Входит в стандарты сотовой связи.

Мобильный телефон - используется Клиентами Компании для получения одноразовых паролей в SMS-сообщениях, а также для работы с мобильными приложениями.

Мобильное приложение - программное обеспечение, предназначенное для работы на смартфонах, планшетах и других мобильных устройствах.

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.

Рекомендации

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, отвечающих на Ваш звонок на горячей линии Вашей финансовой компании. В любой момент клиент может обратиться на горячую линию своей финансовой компании и узнать, как можно изменить свое кодовое слово.

При использовании пин-кода рекомендуется придерживаться следующих советов: обращаться с пин-кодом карты Вашей финансовой компании необходимо так же, как и с пин-кодом любой банковской карты: не сообщать его никому, включая сотрудников Вашей финансовой компании, не записывать его на карте, не хранить записанный пин-код там, где

он будет доступен другим лицам.

При использовании мобильного телефона рекомендуется придерживаться следующих советов: при взаимодействии с Вашей финансовой компании указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (договор на услуги связи заключен на Ваше имя). Устанавливайте мобильное приложение Вашей финансовой компании на тот телефонный аппарат, 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 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.

Во избежание заражения вирусами Вашего компьютера, следуйте следующим рекомендациям:

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.

Отсутствие вирусов на устройствах (компьютерах, сотовых телефонах, планшетах), с которых Вы работаете с системами дистанционного обслуживания Вашей финансовой компании, является залогом безопасности Ваших денежных средств.