"УТВЕРЖДАЮ"
Генеральный директор
ООО МКК «ЮристЪ»
Екимов Вячеслав Викторович
_____
Приказ № 1 от "01" июня 2019 г.
М. п.

Рекомендации
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям
(в соответствии с Положением Банка России от 17 апреля 2019 г. N 684-П)

Настоящий документ предназначен для ознакомления клиентов Общества с ограниченной ответственностью микрокредитной компании «ЮристЪ» (ООО МКК «ЮристЪ») с рекомендациями по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

В настоящих рекомендациях Общество обеспечивает доведение до своих клиентов следующей информации:

о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

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.

Многие финансовые организации используют в своей деятельности технологии дистанционного обслуживания клиентов, что не только повышает удобство взаимодействия клиентов с организацией, но и создает риск получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Клиенту финансовой организации необходимо соблюдать указанные ниже рекомендации для уменьшения риска совершения незаконных финансовых операций от его имени.

Рекомендации:

В случае использования кодового слова (слово, используемое сотрудниками организации для идентификации клиента по телефону) выбирайте его таким образом, чтобы в нем не содержалась информация, хорошо известная иным третьим лицам (ФИО, дата рождения и т. д.). Не сообщайте кодовое слово посторонним лицам, кроме сотрудников финансовой организации.

В случае использования пин-кода (комбинации цифр, используемых для подтверждения операций по карте), не сообщайте его никому, не записывайте его на карте, не храните в общедоступных местах.

При использовании мобильного телефона для получения одноразовых паролей в SMS - сообщениях, а также для работы с мобильным приложением финансовой организации, используйте номер телефона, который оформлен на Ваше имя. Мобильное приложение устанавливайте на телефонный аппарат, который принадлежит Вам и находится в вашем распоряжении.

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.

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

В случае утраты телефона обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном SIM-карты и выпуска новой. В случае, если на утерянном телефоне размещено мобильное приложение, обратитесь в финансовую организацию и сообщите об утере телефонного аппарата, чтобы отключить телефон от системы дистанционного обслуживания.

Защита от вирусов (вредоносного кода) компьютера или мобильного устройства необходима во избежание кражи паролей, данных банковских карт, совершения незаконных финансовых операций от имени клиента.

Для предотвращения заражения вирусами Вашего компьютера или мобильного устройства:

1. Включите автоматическое обновление операционной системы и установленных в ней приложений.
2. Установите антивирусную программу и регулярно обновляйте ее.
3. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты и социальных сетей, которые Вы не ждете.
4. Файлы, полученные из Интернет или со съемных носителей (флешек) до их использования проверяйте антивирусной программой.
5. Установите запрет на установку в телефон приложений из ненадежных источников.

Генеральный директор
ООО МКК «ЮристЪ»
Екимов В. В. _____

М. п.