УТВЕРЖДЕНЫ

приказом

ООО МКК «Сентимо»

№ 84 от 31.05.2019

**Рекомендации** **Общества с ограниченной ответственностью микрокредитная компания «Сентимо» по защите информации в целях противодействия незаконным финансовым операциям.**

1. ООО МКК «Сентимо» в рамках соблюдения требований Положения Банка России от 17.04.2019 № 684-П «Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» уведомляет своих клиентов использующих автоматизированные системы для получения, подготовки, обработки, передачи и хранения информации в электронной форме о **возможных рисках** получения несанкционированного доступа к информации, с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции и необходимости защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, своевременному обнаружению воздействия вредоносного кода.

2. В целях предотвращения несанкционированного доступа к информации и нарушения штатного функционирования средства вычислительной техникиООО МКК «Сентимо» рекомендует следующие **меры защиты**:

2.1. В целях защиты мобильных устройств:

* Своевременно устанавливайте обновления безопасности операционной системы;
* При наличии технической возможности включите шифрование данных на своём мобильном устройстве;
* Не отключайте и не взламывайте встроенные механизмы безопасности вашего мобильного устройства;
* Сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в информационные системы и СМС-коды. Не сообщайте эти данные никому;
* Учетные записи операционной системы должны быть защищены паролями;
* Не храните логин и пароль в мобильном телефоне, смартфоне;
* Регулярно производите смену паролей;
* Не используйте одинаковые логин и пароль для доступа к различным системам;
* Длина пароля должна быть не менее 8 символов;
* В пароле обязательно должны присутствовать заглавные и прописные символы, цифры, а также специальные символы, например, #, %, ^, \* и т.д.;
* Не используйте функцию запоминания логина и пароля;
* В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
* Не произносите вслух, не записывайте и не храните в любом доступном посторонним лицам месте пароли.

2.2. В целях защиты персональных компьютеров:

* + используйте только лицензионное системное и прикладное программное обеспечение;
  + установите на компьютер только одну операционная система;
  + не устанавливайте и не используйте на компьютере программы для удаленного управления, например TeamViewe:
  + установите и регулярно обновляйте антивирусные программы (например, Kaspersky, Dr.Web, Symantec, Avira, ESET, NOD 32, McAfee).
  + своевременно проводите обновление системного и прикладного программного обеспечения.
  + для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее)
  + при передаче информации с использованием чужих компьютеров, после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились;
  + не передавайте персональных данных и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами;
  + не переходите по ссылкам в таких письмах, не открывайте вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение);
  + в случае обнаружения подозрительных действий, совершенных в компьютере, незамедлительно смените логин и пароль;
  + при обнаружении совершения незаконных финансовых операций – незамедлительно подайте заявление о данном факте в правоохранительные органы и сохраните доказательства данного факта в устройстве.
  + при работе с иными носителями информации перед началом работы осуществляйте их проверку на предмет отсутствия компьютерных вирусов.

2.3. В целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники:

* обновляйте антивирусные программы на постоянной основе;
* осуществляйте регулярный контроль работоспособности антивирусных программ;
* создайте условия, при которых невозможно несанкционированное отключения средств антивирусной защиты;
* антивирусная защита должна обеспечивать сохранение безопасного состояния информации при любых сбоях;
* вынесите ярлык для запуска антивирусной программы на рабочий стол персонального компьютера и используйте его регулярно.

Дополнительно сообщаем, что настоящие Рекомендации носят диспозитивный информационный характер и призваны донести до сведения Клиентов:

- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом на осуществление таких операций;

- информацию 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.