Утверждено Приказом № 14 от «31» мая 2019г.

исполнительного директора Некоммерческой

микрокредитной компании «Фонд микрокредитования

субъектов малого предпринимательства Саратовской

области.

**РЕКОМЕНДАЦИИ**

**Некоммерческой микрокредитной компании «Фонд микрокредитования субъектов малого предпринимательства**

**Саратовской области (ФМСО) по защите информации, в целях противодействия незаконным финансовым операциям.**

1. Некоммерческая микрокредитная компания «Фонд микрокредитования субъектов малого предпринимательства Саратовской области (ФМСО) в рамках соблюдения требований Положения Банка России от 17.04.2019г. №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 техники Некоммерческая микрокредитная компания «Фонд микрокредитования субъектов малого предпринимательства Саратовской области (ФМСО) рекомендует следующие **меры защиты**:
   1. В целях защиты мобильных устройств:

* своевременно устанавливайте обновления безопасности операционной системы;
* при наличии технической возможности включите шифрование данных на своем 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 или пароля;
* в качестве пароля не рекомендуется использовать имя, фамилию, день рождения, и другие памятные даты, номер телефона, автомобиля, адрес места жительства, и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
* не произносите в слух, не записывайте и не храните в любом доступном посторонним лицам месте пароли.
  1. В целях защиты персональных компьютеров:
* используйте только лицензионное системное и прикладное программное обеспечение;
* устанавливайте на компьютер только одну операционную систему;
* не устанавливайте и не используйте на компьютере программы для удаленного управления, например Team Viewe;
* установите и регулярно обновляйте антивирусные программы например (Kaspersky, Dr.Web, Symantec, Avira, ESET NOD32, 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 сохранилась;
* 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 или пароль;
* при обнаружении подозрительных действий, совершенных в компьютере, незамедлительно смените логин и пароль;
* при работе с иными носителями информации перед началом работы осуществляйте их проверку на предмет отсутствия компьютерных вирусов.
  1. 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 антивирусной программы на рабочий стол персонального компьютера и используйте его регулярно.