УТВЕРЖДАЮ
Директор
ООО МКК «Союз микрофинансирования В»
_____ Глебов Д.Н.
«19» июня 2019 г.

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.

ООО МКК «Союз микрофинансирования В» (далее – «Общество») в рамках соблюдения требований 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 (утв. Банком России 17.04.2019 N 684-П) **уведомляет** клиентов Общества о возможных рисках получения несанкционированного доступа к защищаемой информации:

1. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации.

2. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риски совершения юридически значимых действий, включая: совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента.

3. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риск деструктивного воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов компании для реализации своих намерений.

4. **Вредоносные программы** (далее - ВК) способны самостоятельно, то есть без ведома клиента создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных действий до полного разрушения информации, хранящейся на дисках компьютера.

5. Общество не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами безопасности.

Во избежании рисков, связанных с негативным последствием несанкционированного доступа, рекомендуется:

1. Не сообщать посторонним лицам персональные данные или информацию через Интернет, включая логины и пароли доступа к клиентским ресурсам Общества, историю операций, так как эти данные могут быть перехвачены и использованы для получения доступа к Вашим активам.

2. Не записывать логин и пароль на бумаге, мониторе или клавиатуре.

3. Не использовать функцию запоминания логина и пароля в браузерах.

4. Не использовать одинаковые логин и пароль для доступа к различным системам.

5. Не пользоваться системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о доступе к клиентским ресурсам Общества.

6. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу), используйте кнопку «Выход». После возвращения к своему средству доступа обязательно смените логин и пароль.

7. Не открывать ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них.

8. Не открывать приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть Ваши идентификационные данные.

9. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

10. При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию ключей.

11. Используйте лицензированное программное обеспечение. Использование нелицензионного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

12. Регулярно (не реже раза в неделю) проводить проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.

13. Не запускайть на своем компьютере программы, полученные из незаслуживающих доверия источников.

14. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

15. Не хранить незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены злоумышленниками и использованы для получения доступа к Вашим активам.

16. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

17. Для обеспечения конфиденциальности операций пользуйте только защищенное соединение через HTTPS. Защищенное соединение предотвращает перехват или фальсификацию передаваемых данных.

18. В случае утраты устройства необходимо изменить пароли доступа к ресурсам на которые производился вход.

19. Проверяйте новые файлы. Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио и видео файлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов. Подозрительные сообщения лучше немедленно удалять. При открытии ссылок, полученных по электронной почте, скопируйте ссылку, вставьте в адресную строку используемого браузера и убедитесь, что адрес соответствует интересующему Вас ресурсу. Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

20. Резервное копирование гарантия безопасности. Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

21. Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» до полного разрушения информации, хранящейся на дисках компьютера.

22. Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними:

а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер;
б) если они к Вам все-таки попали, ни в коем случае не запускать их;
в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба. Самый действенный способ оградить от вредоносных программ свой почтовый ящик – запретить прием сообщений, содержащих исполняемые вложения.

23. Расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: ade, adp, bas, bat, chm, cmd, com, cpl, crt, eml, exe, hlp, hta, inf, ins, isp, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr; sct, shs, url, vbs, vbe, wsf, wsh, wsc.

24. Если Ваш компьютер или мобильное устройство подверглось заражению, рекомендуется обратиться к квалифицированным специалистам, а также сменить пароли от доступа в кабинет, электронной почты, учетных записей в социальных сетях и т.п. с помощью не зараженного устройства.