Утверждаю
Генеральный директор
ООО МКК «Главмикрофинанс»

_____ Худиев В.В.

Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционировании средства вычислительной техники, в целях противодействия незаконным финансовым операциям

Настоящим Общество с ограниченной ответственностью Микрокредитная компания «Главмикрофинанс» (ИНН 1513042142) доводит до сведения Клиентов рекомендации по защите информации от воздействия программных кодов во исполнение Положения Банка России № 684-П от 17.04.2019 года.

1. Вредоносные программы.

Вредоносная программа - это программа, наносящая вред мобильному устройству/компьютеру или иным устройствам (далее - устройства), на которых она запускается.

Вредоносные программы способны самостоятельно (то есть без ведома владельца устройства), создавать свои копии и распространять их различными способами, что может привести к полному разрушению информации, хранящейся на устройстве.

2. Антивирусные программы - основные защитники.

Так как вредоносные программы способны самостоятельно (то есть без ведома владельца устройства), создавать свои копии и распространять их различными способами, это может привести к полному разрушению информации, хранящейся на устройстве.

Периодически запускайте полную проверку компьютера. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

Сообщаем, что помимо борьбы с имеющимися вредоносными программами, антивирусы носят еще и профилактический характер, защищая устройства от проникновения в него вредоносной программы.

3. Польза регулярных обновлений.

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

4. Проверяйте получаемые 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 или мессенджерах, 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 и полученные из иных источников. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. Регулярно проверяйте устройство и будьте бдительны при «всплывающих окнах»

По возможности не сохраняйте в системе пароли и периодически меняйте их. При регистрации на сторонних интернет-сайтах всегда сменяйте пароли, которые приходят вам на электронную почту.

При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте устройство антивирусной программой на наличие вредоносных программ.

При использовании браузера не переходите по ссылке и не нажимайте на кнопки во всплывающих окнах. Старайтесь избегать сайтов, которые могут иметь незаконное и/или вредоносное содержание. Проверяйте все съемные носители информации до начала их использования (такие носители могут переносить с одного устройства на другое вредоносные программы). Избегайте использования привилегированных учетных записей (например, Администратор) для ежедневного использования. Для выполнения большинства операций достаточно прав обычного пользователя. Периодически удаляйте программное обеспечение, которое больше не нужно.

6. Резервное копирование как 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.

7. Тактика борьбы с вредоносными программами

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на устройстве. Тактика борьбы с ними достаточно проста:

а) не допускать, чтобы вредоносные программы попадали на Ваше устройство;

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 и иные средства получения сообщений - запретить прием сообщений, содержащих исполняемые вложения.

8. Расширение файла - это важно!

Помните, что в информационно-телекоммуникационной сети «Интернет» действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы. Если Ваше устройство подверглось заражению, рекомендуется обратиться к квалифицированным специалистам, а также сменить пароли от мобильных приложений (в том числе, где возможно совершать финансовые операции), электронной почты, учетных записей в социальных сетях и т.п. с помощью не зараженного устройства.

9. Меры при утере или хищении устройства.

При утере или хищении Вашего устройства, с которого осуществлялся вход в личные кабинеты некредитных финансовых организаций для осуществления финансовых операций, необходимо обратиться в указанные организации для блокировки личного кабинета с указанием причины осуществления такой блокировки.

Дополнительно сообщаем, что данные Рекомендации носят информационный характер и призваны донести да сведения Клиентов:

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 вреда;

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