Приложение №2
к Положению об антивирусной защите
АО МС Банк Рус

Памятка клиента по защите от вредоносных программ

Вредоносное программное обеспечение (Вредоносное ПО) - компьютерная программа, приводящая к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи информации в автоматизированных системах, программном обеспечении, вычислительной техники и телекоммуникационном оборудовании.

Под Вредоносным ПО обычно подразумевают - компьютерные вирусы, программы «троянский конь», системы несанкционированного удаленного управления, программы вымогатели, и другое Вредоносное ПО.

Вариантов проникновения Вредоносного ПО на компьютер или мобильное устройство существует очень много, в тоже время наиболее распространенными являются:

1) посещение мошеннических web-сайтов, либо web-сайтов, зараженных вредоносным кодом;
2) получения сообщения, содержащего вредоносный код или ссылку на вредоносный код через электронную почту, систему обмена сообщениями, SMS, мессенджерами или через аккаунты социальных сетях;
3) просмотр или запуск файлов на съемных носителях информации (USB-флешках, оптических дисках и других носителях), содержащих вредоносный код;
4) скачивания файлов, содержащих вредоносный код с файлообменных сайтов или систем обмена файлами в сети Интернет;
5) скачивание программ из магазинов приложений (Google Play, Apple store и других) содержащих вредоносный код.

Вредоносное ПО, может маскироваться под любые данные (текстовые файлы, картинки, фильмы, музыка и пр.) или приложения.

Эффективная защита от Вредоносного ПО должна включать в себя комплекс мероприятий, состоящих из следующих мер.

1) Ограничение возможности попадания вредоносного ПО на компьютер или

мобильное устройство:

- следует избегать или максимально ограничить посещение web-сайтов, только сайтами заслуживающими доверия (официальные сайты компаний и новостных агентств, и пр.), не нажимать на рекламные ссылки и «баннеры». Сайты регулярного посещения рекомендуется либо добавлять в закладки браузера либо вводить их адрес вручную самостоятельно;
- не следует открывать электронные сообщения, полученные от неизвестных источников, тем более переходить по ссылкам в них или открывать вложения;
- программы и приложения следует скачивать только с официальных сайтов производителей, использовать лицензионное ПО скачанное с официального сайта разработчика. При установке мобильных приложений всегда проверяйте уровень разрешений которые программа требует для установки, если права требуемые для работы программы Вам кажутся избыточными рассмотрите имеющиеся альтернативы. При установке программ из магазинов приложений обращайте внимание на оценки репутации, количество скачиваний и отзывы пользователей. Следует избегать малоизвестных приложений.

2) Обязательное использование средств антивирусной защиты. Специализированные программы-антивирусы являются довольно эффективным средством защиты от вредоносного ПО, хотя и не гарантируют 100% защиту.

   В качестве рекомендаций по использованию антивируса предлагается:

   - настроить антивирус на работу в режиме автоматического лечения файлов;
   - проверять все файлы, скачанные из Интернет или полученные на флешках или оптических дисках, а также регулярно проводить полную антивирусную проверку;
   - настроить антивирус на автоматическое обновление антивирусных баз и обеспечить обновления не реже одного раза в день;
   - по возможности устанавливать пароль на отключения системы антивирусной защиты либо на ее деинсталляцию.

3) Регулярную установку обновлений безопасности для операционной системы и используемых прикладных программ или приложений.
4) Осуществление повседневной работы под учетной записью, ограниченной в полномочиях (то есть не обладающей правами администратора).

5) Для осуществления взаимодействия с системой ДБО или Мобильным приложением, по возможности, рекомендуется использовать специально выделенный для этих целей компьютер или мобильное устройство.
6) Регулярно повышать свою осведомлённость в области информационной безопасности.