Памятка клиента по защите от вредоносных программ

Вредоносный код - компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспеченье, средства вычислительной техники, телекоммуникационное оборудование, приводящего 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.

Вредоносный код обычно представляется в виде компьютерных вирусов, программ троянских коней, систем несанкционированного удаленного управления, программ вымогателей и других вредоносных программ.

Вариантов проникновения вредоносного кода на компьютер или мобильное устройство довольно большое количество, 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, MMS или из социальной сети;
3) просмотр или запуск файлов на флэшках, оптических дисках и других носителях, содержащих вредоносный код;
4) скачивания файлов, содержащих вредоносный код с файлообменных сайтов или систем обмена файлами;
5) скачивание программ из магазинов приложений (Google Play, Apple store и других) содержащих вредоносный код.

Вредоносный код, может содержаться практически в любых файлах начиная с файлов приложений, скринсейверов, плагинов к браузерам, заканчивая электронными документами и файлов мультимедиа.

Эффективная защита от вредоносного кода должна включать в себя комплекс мероприятий, состоящих из следующих мер.

1) Ограничение возможности попадания вредоносного кода на компьютер или мобильное устройство:
    а) следует ограничить посещения web-сайтов, только сайтами заслуживающими доверия (например, официальными сайтами компаний, общеизвестными новостными ресурсами и так далее);
    б) не следует открывать электронные сообщения, полученные от неизвестных источников;
    в) программы и приложения следует скачивать только с официальных сайтов производителей, при установке программ из магазинов приложений рекомендуется оценить репутацию приложения по отзывам пользователей.
2) Обязательное использование средств антивирусной защиты. Специализированные программы-антивирусы являются довольно эффективным средством защиты от вредоносного кода, хотя и не гарантируют 100% защиту. При выборе антивируса рекомендуется отдать предпочтение решениям, обеспечивающим комплексную защиту и включающими в себя антивирус, межсетевой экран и систему оценки репутации сайтов (так называемые решения класса Internet Security). При этом рекомендуется отдать предпочтения системам, прошедшим сертификацию во ФСТЭК России или ФСБ России. В качестве рекомендаций по использованию антивируса предлагается:
    а) настроить антивирус на работу в режиме автоматического лечения файлов;
    б) проверять все файлы, скачанные из Интернет или полученные на флешках или оптических дисках, а также регулярно проводить полную антивирусную проверку;
    в) настроить антивирус на автоматическое обновление антивирусных баз и обеспечить обновления не реже одного раза в день;
    г) устанавливать пароль на отключения системы антивирусной защиты либо на ее деинсталляцию.

3) Регулярную установку обновлений безопасности для операционной системы и прикладных программ, в том числе Интернет-браузеров. При выборе нового мобильного устройства, рекомендуется отдать предпочтения устройствам, производители которого регулярно выпускают обновления безопасности.
4) Осуществление повседневной работы под учетной записью, ограниченной в полномочиях (то есть не обладающей правами системного администратора).
5) Для осуществления взаимодействия с системой Интернет Клиент-Банк, по возможности, рекомендуется использовать специально выделенный для этих целей компьютер или мобильное устройство.
6) Регулярно повышать свою осведомлённость в области информационной безопасности.