Рекомендации по защите от вредоносных программ

ИНГОССТРАХ ПЕНСИЯ
НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД

В настоящее время распространены действия злоумышленников по причинению вреда компьютерам/смартфонам, в том числе обычных граждан – пользователей. Основным побудительным мотивом этих действий является кража значимой информации, в том числе финансовой (доступ к мобильным банкам и пр.) и персональных данных.

Данные действия злоумышленников производятся с помощью вирусных программ, программ шпионов и др.

Вирус это вредоносная программа, созданная злоумышленником. Сегодня подавляющее большинство вирусов направленно на незаконное получение денежных средств тем или иным способом.

Для того чтобы эффективно защититься от вирусов, нужно знать как они действуют. Основными задачами вирусов являются: проникновение на компьютер/смартфон пользователя, обеспечение своего запуска, защита себя от обнаружения и удаления, осуществление деструктивных действий.

Виды вирусов – файловый вирусы, трояны, рекламные вирусы, вирусы-шифровальщики (вымогатели), вирусы-блокировщики, ботнеты.

Файловые вирусы разрушают структуру файлов и приводят их в негодность. Трояны проникают в компьютер и маскируясь совершают кражу значимой информации. Рекламные вирусы загружают навязчивую рекламу требуя, за ее блокировку и удаление, выплату денег. Шифровальщики после проникновения на компьютер, шифруют все файлы и требуют за их восстановление денежные средства. Примерно также действуют и вирусы-блокировщики, блокируют любые действия компьютере требуя денежный выкуп. Вирусы-ботнеты максимально маскируясь подключают компьютер к глобальной вредоносной сети и используют его в качестве распространения вирусов.

Кроме того, рядовой пользователь, для эффективной защиты должен понимать пути проникновения вирусов. Самыми распространенными из них являются зараженные сайты Интернета, сайты двойники, носители информации (USB-флешки, CD/DVD-диски).

Переходя непосредственно к рекомендациям по защите от вредоносных вирусов и программ, необходимо отметить, что 90% успеха в защите, зависит от внимательности и действий со стороны самого пользователя.

Рекомендуем вам:

1. Установить специализированное антивирусное программное обеспечение с настройкой постоянного обновления баз (сигнатур) вирусов.
2. Использовать защищенные браузеры и регулярно устанавливать обновления, рекомендуемые разработчиком.
3. Включить и настроить функции браузера для проверки загружаемых сайтов.
4. Использовать дополнительные аппаратные средства защиты, специализированные программы и/или дополнения для браузера в целях защиты от ботнетов, кейлогеров, фишинга.
5. Проявлять бдительность, осмотрительность и обращаться на официальные сайты производителей программного обеспечения и поставщиков услуг.