Мы редко задумываемся о том, что может произойти, если доступ к нашему персональному компьютеру получит тот, кто заинтересован использовать нашу личную информацию в корыстных целях. Мы забываем и о том, что доступ к нашему ПК можно получить не только напрямую, но и через Интернет, где мы проводим много времени и не всегда соблюдаем правила безопасности. С одной стороны, нам кажется, что защита, которую мы обеспечиваем на своем ПК, достаточна. Мы считаем пароли приемлемо сложными, антивирус – всемогущим. Однако мошенники бывают крайне изобретательными в попытках добраться до ценной информации. Злоумышленник легко может использовать ваш компьютер, пока вас не будет рядом, и вы ничего об этом не узнаете. Преступники пользуются нашей беспечностью и отсутствием навыков обеспечения кибербезопасности, вынуждают устанавливать вредоносное ПО в составе взломанных пиратских или поддельных программ. Выход в такой ситуации только один: учиться ответственно относиться ко всем данным, которые вы загружаете и храните на своём ПК, своевременно распознавать угрозы и избегать их.

Учётная запись пользователя на ПК – это ваше личное пространство, где хранятся:

- ваши персональные данные и параметры настройки;
- документы, которые вы создаете, и те, к которым у вас есть доступ в общих пространствах;
- пароли и доступы к онлайн-сервисам и приложениям, которые вы сохраняете в системе.

Если ваша учётная запись защищена паролем, это пространство недоступно никому, кроме вас, поэтому защитите паролем учётную запись на входе в систему и при блокировке экрана, чтобы предотвратить физический доступ к данным на вашем компьютере.

Если вы вынуждены делить компьютер с другими людьми или детьми, настройте для них гостевую учётную запись. При этом для защиты ребёнка от нежелательной информации, а важные данные – от случайного повреждения стоит дополнительно воспользоваться функцией «Родительский контроль».

Вредоносное ПО может проникнуть на ваш компьютер множеством способов:

- заражённые файлы могут оказаться не только в сетевой папке, но и на вашем флеш-накопителе, который использовался на чужих компьютерах;

- вредоносное ПО может запуститься при работе с ранее загруженными файлами, даже если при загрузке проверка не выявила опасности.

По этой причине работающий в фоновом режиме антивирус сможет вовремя распознать вредоносное ПО и остановить его деятельность, прежде чем оно нанесёт вам какой-то ущерб. Если антивирус не обновлен или даже не запущен, последствия могут оказаться непредсказуемыми. В этой связи всегда следует соблюдать простые правила:

- антивирус должен быть включён всегда, когда вы работаете за компьютером. Включив компьютер, проверьте, корректно ли работает антивирус, и только потом запускайте остальные программы;
- даже если вы редко пользуетесь Интернетом и заходите на один-два избранных сайта, вам всё равно следует вовремя обновлять операционную систему и браузер, ведь в каждой ОС постоянно находят всё новые и новые уязвимости, а устаревшая версия браузера затруднит вашу работу в Интернете.

Своевременное обновление операционной системы делает её стабильнее, функциональнее и безопаснее. В этой связи операционная система должна быть настроена на автоматическую проверку и установку новых обновлений. В настоящее время браузеры обновляются автоматически, однако, если вы давно его не закрывали, браузер может устареть. Рекомендуется время от времени вручную проверять, установлена ли у вас актуальная версия браузера.

Работая в Интернете всегда стоит помнить, что программное обеспечение может быть вредоносным по своей сути и маскироваться под чем-то совершенно безобидным и порой полезным: играми, приложениями для прослушивания музыки, забавными видеоклипами, чтобы у вас возник стимул их сохранить. Именно поэтому чаще всего нежелательное программное обеспечение устанавливает на устройство сам пользователь.

Вредоносное ПО может начать загружаться на устройство, если пользователь нажал на ссылку, которая активирует загрузку или запуск файла, при этом ссылка может быть прислана даже от имени знакомого в фальшивом письме или рекомендована анонимом как интересная и хорошая.

Чаще всего вредоносное ПО маскируется под бесплатные программы, поэтому проще всего столкнуться с ним там, где никто не контролирует распространяемые материалы. В зоне риска:

- любые сервисы прямого обмена файлами;
- мелкие магазины игр;

- сайты для загрузки музыки;
- порносайты;
- пиратские библиотеки.

Пиратское ПО очень часто содержит встроенные вирусы. Возможно всё: злоумышленник может похитить вашу конфиденциальную информацию, включая паспортные данные, реквизиты банковских карт, контакты и переписку.

Покупая или загружая бесплатное ПО в проверенном интернет-магазине, вы не получаете полной гарантии отсутствия вредоносного программного обеспечения, но заметно снижаете вероятность с ним столкнуться.

Не стоит забывать, что в настоящее время вредоносное ПО может быть прикреплено к какому-либо файлу, который не вызывает каких-либо подозрений. Так, имеющиеся уязвимость MS Office приводит к тому, что источником вредоносного программного обеспечения может стать на вид совершенно невинный файл Word или Excel. Механика Office использует внутренние действующие механизмы – макросы. Самый обычный файл документа может нести в себе набор макросов, не регистрируемых защитой как самостоятельные исполняемые файлы – и этой лазейкой пользуются некоторые разработчики вредоносного ПО. Файл с макросом может сам по себе не наносить никакого вреда, но создавать в системе внутреннюю «отмычку», открывая доступ извне для злоумышленника. Опасность использования макросов была выявлена более 10 лет назад, и в большинстве версий Windows их запуск по умолчанию заблокирован. В этом случае задача злоумышленника – уговорить вас разблокировать возможность запуска макросов.

Чем ценнее данные на вашем устройстве, тем внимательнее вы должны относиться к тому, что на него загружаете.