Личная информационная безопасность

Посещение сайтов стало настолько привычным, что мы не задумываемся об опасностях, которые может скрывать любая страница в Интернете. Сайт — это программа, неявным для вас образом взаимодействующая с вашим браузером и операционной системой и конечные цели такой программы могут быть совершенно разными.

Зачастую действия интернет-мошенников направлены на людей, которые не знают, чему можно, а чему нельзя доверять в глобальной сети. Вредоносные файлы и программное обеспечение могут скрываться за не вызывающим подозрений интерфейсом, могут быть встроены в архив с любыми данными, которые могут понадобиться пользователю или могут быть замаскированы под документы, файлы мультимедиа или ничем не примечательное расширение для браузера. Мошенники могут отвлекать внимание жертвы множеством ярких картинок на сайте или призывами немедленно что-то сделать.

Основная опасность бездумного серфинга в том, что вредоносное ПО может быть размещено на любом сайте и перейдя по непроверенной ссылке мы незаметно загрузим его на свой компьютер. Ссылка может быть замаскирована под заманчивое предложение скидки, интересный

видеоролик, скандальные факты о знаменитостях и т.д. Сайт, который на первый взгляд кажется вам знакомым и проверенным, может быть взломан или подделан злоумышленниками.

Стоит также понимать, что ни один сайт, рассчитанный на нормальное взаимодействие с посетителем, не будет пытаться рассеять ваше внимание открытием нескольких всплывающих окон или яркими контрастными предупреждениями. Основная цель создателей подобных ресурсов заключается в том, чтобы человек растерялся и интуитивно выполнил какие-либо действия. Заходя на любой сайт, вы примерно представляете, зачем вы это сделали, поэтому попав на заполненный «информационным шумом» сайт, просто покиньте его и закройте все вкладки, которые открылись автоматически.

Таким образом вас всегда должно насторожить если:

- при загрузке из Интернета музыку или видео, сайт предлагает установить проигрыватель;

- осуществляя покупки в интернет-магазине, сайт предлагает установить специальное приложение;

- попав на сайт, вы заметили, что на странице неестественно много ярких кнопок и ссылок со словом «скачать», «загрузить» и «установить»;

- установленный антивирус информирует о том, что сайт является мошенническим.

Чтобы не допустить ущерба вашей информации и компьютеру, необходимо соблюдать следующие правила:

- не нажимайте кнопки «Скачать» на любых сайтах, кроме сайтов производителей программного обеспечения или официальных поставщиков нужных вам материалов;

- не загружайте ничего с сайтов, вид которых вас настораживает обилием всплывающих окон или множеством рекламных объявлений;

- если вам необходимо установить какую-либо программу, загружайте ее только с сайта разработчика или в надежном интернет-магазине;

- проверяйте любой загруженный файл антивирусом;

- обращайте внимание на расширение загружаемых файлов и соответствие их стандартному для такого рода файлов;

- не запускайте и не открывайте подозрительные файлы, которые неожиданно загрузились на ваш компьютер

- доверяйте рекомендации антивируса, если он считает сайт подозрительным.

Еще одним важным аспектом на пути обеспечения личной информационной безопасности является регулярной обновление операционной системы и установленных программ. Пользователь относится к однажды установленному и налаженному программному обеспечению, как к чему-то вроде домашней мебели: куплено недешево, установлено специалистами, должно работать долго. По этой причине оповещения программ о необходимости обновления кажутся чем-то лишним или даже подозрительным. Вместе с тем обновления содержат последние исправления, которые повышают безопасность вашей работы в Интернете в том числе с личными и конфиденциальными данными и не позволяют злоумышленникам использовать известные уязвимость для совершения противоправных действий с вашим компьютером.

Вместе с тем обновлять ПО стоит исключительно на официальных сайтах. Подлинное предложение установить новую версию программы всегда будет исходить от уже установленной у вас версии этой программы, а не от постороннего веб-сайта, ведь установка вредоносных программ, замаскированная под обновление ПО — излюбленный трюк злоумышленников, поэтому очень часто на мошеннических сайтах предлагают обновить версию вашего браузера или Flash Player, а также обновить или установить бесплатную версию антивируса.

Для того, чтобы удостовериться, что предложение об обновлении прислано самой программой, полностью закройте интернет-браузер и если просьба об обновлении исходит от одной из программ, установленных в вашей системе, то всплывающее окно не исчезнет после закрытия сайта. Кроме этого можно посетить официальный сайт программы и проверить наличие свежих обновлений.

Столь же внимательно стоит относиться и к установке расширений браузера (небольшая программа, расширяющая возможности браузера). Как и прочие программы, расширения браузера

могут содержать вредоносный код. Через зараженные расширения браузера мошенники смогут собирать о вас информацию: персональные данные, номера банковских карт, мобильных телефонов и так далее. Устанавливайте только нужные вам расширения с официальных сайтов их разработчиков.

Загружая что-либо из Интернета, обращайте внимание на мелкие подписи к ссылкам для загрузки, на дополнительные предложения (от таких предложений можно отказаться без ущерба для устанавливаемой программе, просто «снимайте» все ненужные галочки). Если что-то начало устанавливаться и вызвало у Вас подозрение, смело отменяйте установку. Даже если вы загружаете что-либо с известного вам сайта, всегда нужно проверять такой файл антивирусом перед его первым открытием или установкой.

Чтобы не стать жертвой злоумышленников, не подвергать риску свои данные, не терять доступ к важным учетным записям или средства со своих счетов:

- будьте предельно бдительны, перемещаясь от сайта к сайту в поисках того, что вам нужно;

- оперативно обновляйте ПО для выхода в Интернет и используйте для этого официальные сайты производителей;

- следите за тем, чтобы антивирус всегда работал и проверяйте любые файлы перед тем, как их загрузить.