КОМПЬЮТЕРНАЯ ГИГИЕНА: КАК БОРОТЬСЯ С ВИРУСАМИ

Аналогично гигиене в медицине существует и компьютерная гигиена, назначение которой – профилактика заражения компьютера вирусами и вредоносным программным обеспечением.

Существует несколько нехитрых правил компьютерной гигиены, следование которым поможет минимизировать вероятность поражения компьютера. Данные правила предназначены больше для пользователей Windows, однако, пренебрегать некоторыми из них не стоит и сторонникам других операционных систем, используемых как на компьютерах, так и на мобильных устройствах сотовой связи:

1) Приобретите и пользуйтесь платным антивирусом. Отсутствие антивируса резко увеличивает вероятность заражения компьютера, а бесплатные продукты обычно имеют сильно урезанный функционал.

2) Используйте антивирус! Часто бывает, что установив на компьютер новейший навороченный продукт от известной компании, пользователь забывает о его существовании. Между тем, простой установки антивируса бывает недостаточно для эффективного противостояния угрозам.

Необходимые меры при работе с антивирусом:

• Регулярное обновление. Без свежих обновлений никакой антивирус не сможет эффективно защитить ваш компьютер.

• Регулярный запуск проверки системы. Функция сканирования не зря существует в интерфейсах антивирусов. Быструю проверку рекомендуется запускать раз в неделю, полную – раз в месяц.

• Проверка антивирусом подключаемых к компьютеру носителей информации (флешек, жестких дисков и т.д.), а так же файлов, скаченных из интернета. Не стоит лениться – время, потраченное на проверку, позволит сэкономить время на ремонт после попадания вируса в систему.

3) Устанавливайте только знакомые вам программы, взятые из известных источников. Это

поможет избежать неожиданностей в виде вирусов, замаскированных под полезное ПО. Лучшие источники драйверов и программ – сайты непосредственных производителей. Из этого правила прямо вытекает следующее.

4) Не используйте пиратское программное обеспечение. Использование взломанных программ чревато заражением компьютера – случается, что в генераторы ключей встраиваются троянские программы, клавиатурные шпионы и т.д.

5) Работая в интернете, обращайте внимание на то, на каком именно сайте вас просят ввести пароль, номер телефона или совершить какое-либо действие (бесплатно проверить компьютер на вирусы, скачать обновление и т.д.). Если вы не опытный пользователь и не уверенны в своих действиях – лучше никаких действий не предпринимать и обратиться за советом к специалисту. Злоумышленники часто пользуются неопытностью, подменяя адреса известных сайтов, предлагая скачать вирусы под видом обновлений программного обеспечение.

6) В Windows пользователь компьютера по умолчанию обладает администраторскими правами. Это значит, что он может вносить любыеизменения в настройки системы. Вредоносное программное обеспечение, попав на компьютер, загруженный под учетной записью с администраторскими правами, так же получает широкие полномочия для воздействия на систему. Выход из этой неприятной ситуации в создании на компьютере нескольких учетных записей, обладающих разными правами. Менять настройки системы, устанавливать программы лучше под администраторскими правами, а работать под пользовательскими – так безопаснее.

7) Используйте длинные и сложные пароли, сочетание цифр, строчных и заглавных букв. Это усложнит злоумышленникам доступ к вашей информации.

15 Февраля 2021

Адрес страницы: https://lenobl.sledcom.ru/Protivodejstvie-kiberprestupnosti/item/1575107