Компьютерная безопасность.
Как правильно жить в Интернете.

Права пользователей

Если права пользователя компьютера ограничены, да еще включен контроль учетных записей пользователей, да еще работает брандмауэр, то при возникновении лишней активности (например, при попытке трояна запустить какую-то программу или передать на какой-то сайт логины-пароли-сертификаты) система либо запретит ее, либо переспросит пользователя, либо попросит ввести пароль администратора.

Конечно, раздражает необходимость часто вводить пароли и отвечать на вопросы, но за удобство можно заплатить дороже, чем рассчитывали. И не только деньгами. Мне теперь менять пароли от всех сайтов, на которые я входил, пока в системе сидел вирус.
Хотя это как раз периодически делать нужно! И ни в коем случае не сохранять пароли в браузерах. Во-первых, троян их заберет в первую очередь, а во-вторых, вы же их забудете, если не вспоминать долго.

Можно, впрочем, не помнить и не вспоминать, а пользоваться программами хранения паролей.

Программы хранения паролей

Удобно: вносите свои логины и пароли от всех сайтов, где зарегистрированы (а также пин-коды банковских карт и другую секретную информацию, которую боитесь забыть). Пароли может вам сгенерировать и сама программа, хорошие, стойкие. Вы, главное, основной не забудьте – с которым эту программу запускать надо. Хранят такую программу на флешке, пользуются с любого компьютера. А потеряете флешку – никто ее не расшифрует, не зная пароля к программе. Правда, и вы больше никуда не зайдете... Но вы же не одну копию сделаете, да? Пользоваться просто – программка сама вас авторизует на сайтах, набирать ничего не придется, а значит вирусы-кейлоггеры вам не навредят. (Это те, которые перехватывают и отсылают своему хозяину всё, что вы набираете на клавиатуре.)

Вот представьте, тот хакер, что у меня webmoney увел, вдобавок так перехватил и прочитал абсолютно всё, что я в тот день писал друзьям по аське, в комментариях на форумах, в том числе анонимно. Хорошо еще, что я интимный дневник не веду. С рецензиями на просмотренные порнофильмы, ага... (Да не качал, не качал я порно!) Чтобы не повторять моих ошибок, давайте повторим мой урок (в смысле, урок, который я получил).

Защита

Первой программой, которую вы ставите на компьютер до подключения к Интернету, должен быть антивирус.

Антивирус, как любые программы, – лицензионный или бесплатный. С дистрибутивами взломанных антивирусов легко и просто распространяются вирусы.
Периодически подстраховывайте работу антивируса другими средствами проверки, только выбирайте не конфликтующие.

Установите и в процессе работы в Интернете настройте брандмауэр. Не отключайте обновления системы и программ. Большая их часть – это как раз ликвидация уязвимостей, а не просто совершенствование работы.

Отключите автозапуск внешних носителей. У вас перестанут автоматически запускаться фильмы с DVD, но и вирусы не проникнут на компьютер сразу при вставке флешки или диска.

Установка программ

Флешку или диск с программами, которые вам записал друг, обязательно вручную проверьте антивирусом.

Все бесплатные программы, в том числе драйвера, качайте с официальных сайтов производителей, потому что на других интернет-ресурсах они могут быть и с довесками в виде вирусов.

Пока вы устанавливаете на чистую систему свой привычный набор программ, можете действовать из учетной записи с правами администратора. Установили – перейдите в ограниченную учетную запись или понизьте права текущего пользователя и создайте отдельную учетную запись с правами администратора и паролем. (Если умеете вызвать встроенную учетную запись администратора, просто задайте пароль на ней.) Если нужно еще что-то установить, запускайте файл дистрибутива, кликая на нем правой кнопкой, выбирая «Запуск от имени» и вводя пароль администратора.

Браузер

Браузер – любой, кроме IE. Не верьте заявлениям, что он становится лучше, краше с каждым днем...

Не ходите по сомнительным сайтам, особенно малоизвестных интернет-магазинов. Верьте браузеру, который предупредит вас об опасном содержимом сайта, установите дополнительные средства оценки репутации сайта. Нужна образовательная информация – пользуйтесь поиском edu.mail.ru, чтобы даже случайно не забрести на сайт с рефератами. Не поддавайтесь заманчивым предложениям браузеров запомнить ваши пароли.

Пароли

Назначайте пароли сложные: достаточно длинные, цифро-буквенные и со спецсимволами, разные для разных сервисов. Не запоминаете – записывайте. В блокнотик, а не в программе Блокнот. Меняйте их достаточно часто. Не блокнотики, пароли. Легче делать это с программой хранения паролей.

Не храните в почте письма с напоминанием паролей от сайтов. Понадобится – снова запросите.

Не устанавливайте в качестве секретных вопросов для напоминания паролей такие, ответы на которые легко получить в вашем окружении или ваших аккаунтах в социальных сетях. Например, на вопрос «Имя домашнего питомца» есть ответ в подписях фото вроде «Это наша Мурка». А девичью фамилию вашей матери можно выяснить у кого-то из ваших родственников, познакомившись с ними в «Одноклассниках».

Платежи

Пользуясь системами электронных платежей, внимательно читайте их инструкции по безопасности и выполняйте их. Главное – вход в систему не должен быть завязан на чисто компьютерные действия (логин-пароль и даже сертификат). Нужно еще что-то, что можете сделать только вы сами: установить сертификат с флешки в хранилище, ввести код с карты кодов безопасности или из SMS интернет-банкинга и т. п.

Предполагайте, что ваш компьютер открыт всем ветрам, и не держите на нем компромата, а также важных и нужных вещей – сбрасывайте их на внешние носители, делайте тем больше копий и обновляйте их тем чаще, чем важнее для вас эти файлы.

Правила лечения

Если возникло подозрение на вирусную активность (не открываются сайты разработчиков антивирусов, тормозит система, появляются непонятные папки и файлы там, где их быть не должно, запускаются какие-то процессы) – проверяйтесь. Нужно от Интернета отключиться и всю информацию о вирусе и свежие средства проверки искать с помощью «чистого» компьютера. Зараженный скорее всего и не позволит этого сделать, а время потеряете.

Удалив вирус, обезопасьтесь от последствий. Часто в системе остаются следы, хвосты, а то и живоспособные части, которые могут активизироваться при каких-то условиях. Об этом можно прочитать на тематических форумах, там же предлагаются способы избавления. Обычно нужно зарегистрироваться, скачать какую-то специально разработанную программку, запустить, отчитаться, как она себя ведет, загрузить на форум результаты, выполнить рекомендации разработчиков... Да, долго, нудно, но так совершенствуются антивирусы и пополняются их базы. Поспособствуйте – пригодится не вам, так людям.

Возможно, будет проще переставить систему, но учтите, среди той информации,

которую Вы будете сохранять перед переустановкой, могут быть зараженные файлы, так что полечиться перед этим все равно надо. Надежнее – отформатировать диски перед установкой системы и возвращением на компьютер сохраненных данных.

Ну что ж, счастливого и безопасного серфинга по волнам Интернета после серьезной и основательной подготовки!