СОВЕТЫ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ.

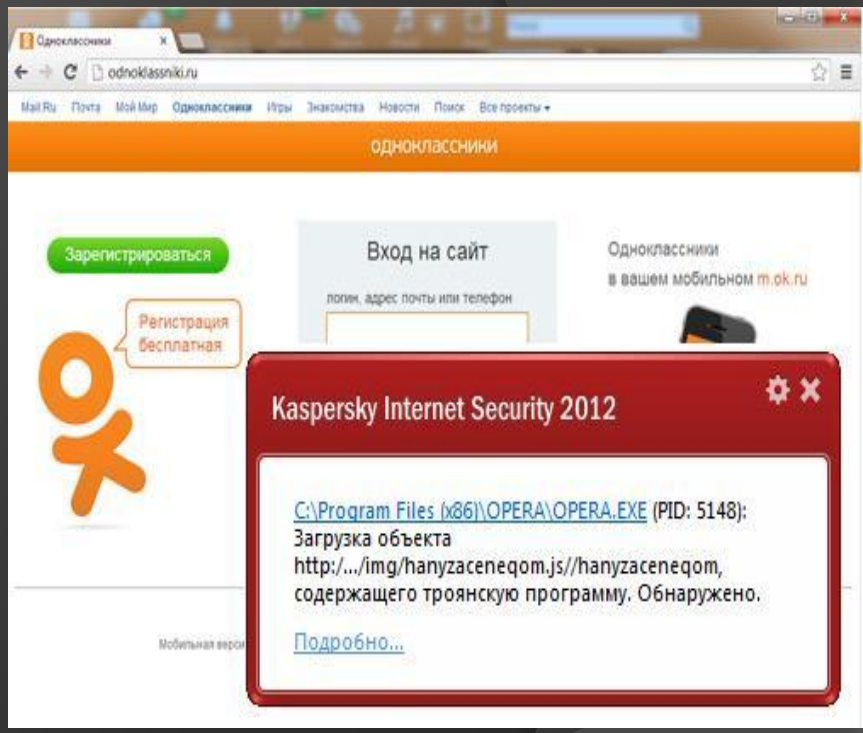
Выполнила работу
ученица 8а класса
Павлова Анастасия.

Введение.

Если вы много времени проводите в Сети, то полноценная защита просто необходима. Я предлагаю вашему вниманию десять советов о том, как сделать веб-серфинг безопасным.

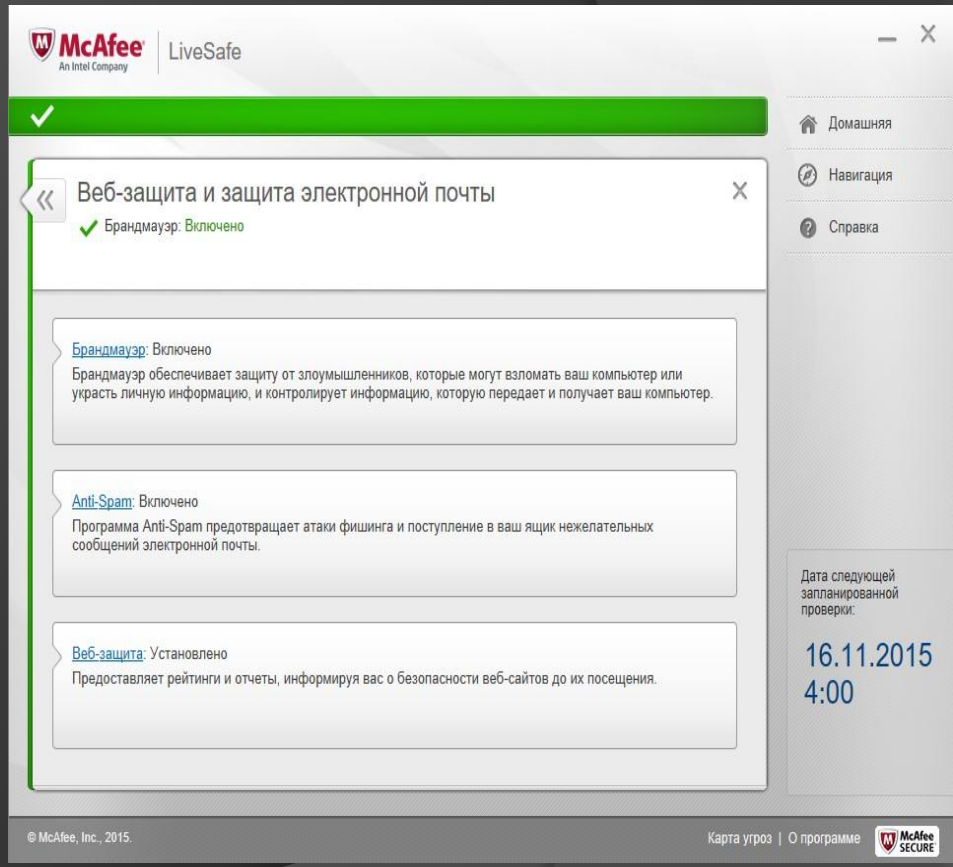
СоветN°1. Не ходите по подозрительным ссылкам.

Если вам пришло письмо от вашего банка с предложением обновить пароль, или с сайта «Одноклассники. ру» поступило уведомление о новом сообщении, не торопитесь открывать предлагаемые ссылки.
Вместо odnoklassniki.ru вполне можно увидеть odnoclassniki.ru или даже odnaklassniki.ru: разница всего в одной букве, и многие этого даже не замечают. Если вы проследуете по этой ссылке, то в худшем случае можете подцепить серьезный вирус, а в лучшем – просто лишитесь своего аккаунта на сайте.



СоветN°2. Доверяйте антиспам-фильтрам электронной почты.

Как правило, они фильтруют практически все письма, обманом завлекающие вас на тот или иной хакерский сайт. И даже если вам все-таки пришло письмо с сообщением о выигрыше миллиона фунтов стерлингов, не кидайтесь радостно на стену с криками «Я богат!»: такие сообщения получают сотни тысяч пользователей по всему миру ежедневно. Великобритания давно бы разорилась, выплачивая каждому победителю по миллиону.



Совет №3. Установите комплексную систему защиты.

«Чистый» антивирус – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Наиболее популярные – Kaspersky Internet Security, ESET Smart Security, Symantec Norton 360. И еще десяток других.

Не экономьте на этих системах: $50-70 за годовую лицензию не сравнить с потерей важнейшей информации, которая может случиться по причине недостаточного уровня защиты вашего ПК. И не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

Совет №4. Пользуйте браузерами Mozilla Firefox, Google Chrome и Apple Safari.

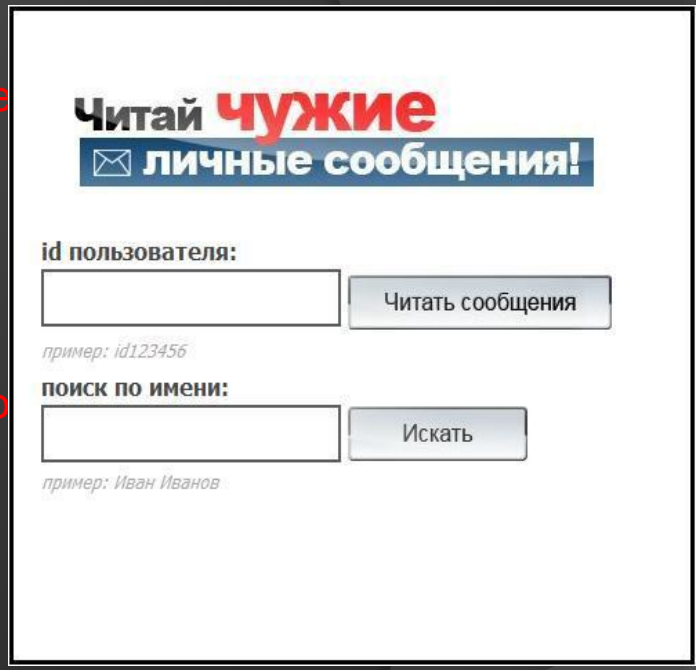
Львиная доля червей и вредоносных скриптов написаны под Internet Explorer и Opera. Первый до сих пор удерживает первую строчку в рейтинге популярности со своими 67% пользователей, но лишь потому, что он встроен в Windows. Opera очень популярна в России из-за ее призрачного удобства и реально большого числа настроек. Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

И не обращайте внимания на регулярно появляющиеся в прессе сообщения о том, что в Firefox больше всего уязвимостей. Во-первых, вы вряд ли будете это проверять, а во-вторых, если даже и так (что весьма сомнительно), ими почти никто не пользуется – настолько быстро разработчики ликвидируют эти «дыры».

Совет №5. Не верьте предложениям прочитать чужие SMS и подобное.

Периодически Рунет (в частности, «В Контакте») потрясают волны спамерского безумия: сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, до них на пике славы были аудионаркотики, еще раньше - «программы, позволяющие заходить в чужие страницы, даже закрытые, под чужим именем». В общем, фантазия мошенников безгранична. Когда спадет волна SMS, придет что-нибудь другое.

Общее у всех этих фальшивок одно – вам предлагается нечто, нарушающее чье-то личное пространство якобы под большим секретом. Люди любопытны и доверчивы, и именно излишняя доверчивость иногда приводит к большим бедам. В лучшем случае, захотев прочитать чужие SMS, можно лишиться 300-600 рублей на счету телефона, в худшем – на компьютере поселится злобный вирус с такого сайта. Запомните одну простую вещь: халявы не бывает. Ни один сотовый оператор не допустит, чтобы возможность просмотра распечаток звонков стала доступна, кому попало через Интернет, а спецслужбы не буду смотреть сквозь пальцы на то, как настоящие аудионаркотики (а не та липа, которой на самом деле являются предлагаемые звуковые файлы) получают широкое распространение.



Совет №6. Купите Apple Macintosh.

«Маки» считаются самыми безопасными компьютерами, но вовсе не потому, что это какая-то «суперзащищенная» система (как любят утверждать ее фанаты). Просто под Mac написано в тысячи раз меньше вирусов по причине его малой распространенности по сравнению с ПК, а также из-за другой архитектуры.

Совет №7. Пользуйтесь лицензионным ПО.

Не стоит смеяться над этим или крутить пальцем у виска. Если вы только что скачали свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить троян на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность. С другой стороны, антивирусы иногда ложно реагируют и на вполне безобидных взломщиков.
В общем, лучше не рисковать.

Совет №8. Делайте покупки только в проверенных онлайн-магазинах.

Если вы любите делать покупки онлайн с помощью пластиковой карты, магазин должен быть полностью безопасным. Если это малоизвестный магазин, лучше всего будет проверить его перед тем, как оставлять там какую-либо финансовую информацию. Самый простой путь – написать название или URL сайта в поисковиках и посмотреть, что пишут другие люди про этот магазин. Второй путь – установить Netcraft Toolbar (для Mozilla Firefox и Internet Explorer). Это небольшое бесплатное дополнение к вашему браузеру покажет потенциально опасный сайт и перекроет доступ к известному сайту мошенников (база данных пополняется постоянно).

Совет №9. Регулярно устанавливайте обновления программ.

Методы взлома постоянно совершенствуются, равно как и методы защиты. Представители Microsoft регулярно рапортуют о том, что их новый Internet Explorer еще безопасней предыдущего, да и уязвимости в Mozilla Firefox устраняются буквально в течение нескольких дней после их обнаружения. Своевременная установка обновлений касается любых программ, не только браузеров, хотя для последних надо это делать как можно быстрее.

Совет №10. С осторожностью относитесь к скачиваемым в Интернете файлам

«И на старуху бывает проруха» - никто не гарантирует, что, скачивая программу даже на известном и уважаемом сайте, вы не подцепите очередной троян. Новые вирусы выходят быстрее, чем защита от них, и антивирусное ПО сайтов вполне может «проморгать» очередной хитрый вирус. Особенно небезопасно скачивать файлы из пиринговых сетей, а также приносить их на флешке неизвестно откуда. Совет один – обязательно сканируйте все новые файлы вашим антивирусом или комплексной системой защиты, а при подозрениях, что такая система не справляется – отправляйте подозрительный файл разработчикам в «Лабораторию Касперского», Eset или «Доктор Веб», чтобы там его исследовали по полной программе и дали вам уверенный ответ.

Вывод.

Если соблюдать все советы, которые представлены в моей творческой работе, то у вашего компьютера будет меньше шансов заразиться вирусом.