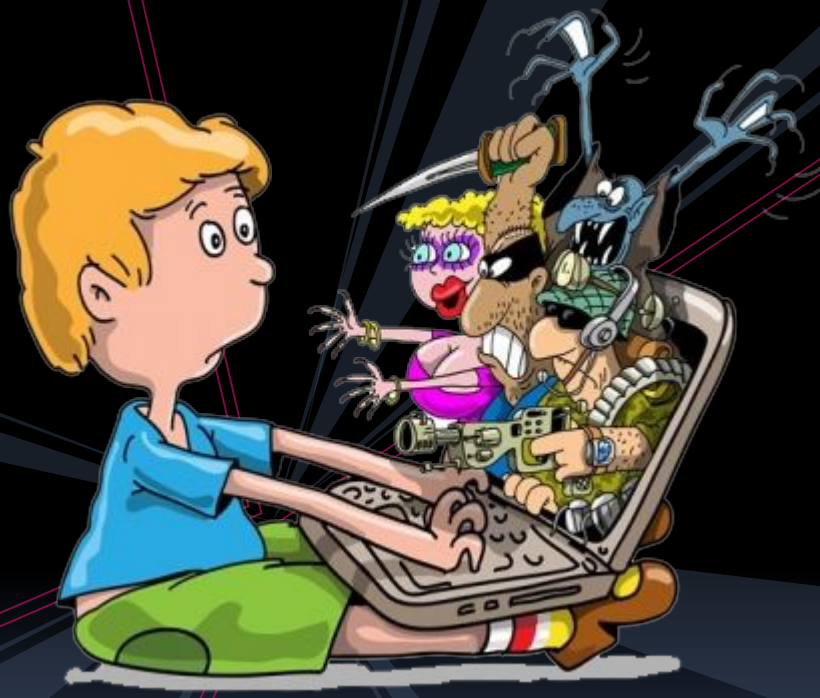
ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ.

Выполнила ученица
8а класса
Новичкова Юлия.

Введение.

Большинство современных пользователей, совершенно не заботится о безопасности в Интернете. Люди делятся личной информацией, доверяют сохранение паролей браузерам и предполагают, что Интернет – это безопасно.

Интернет можно сравнить с темной улицей. В нем есть те же «прохожие» и «преступники», которые



Вы когда-нибудь замечали такую интересную особенность: если вчера обсуждали на форуме котиков, то сегодня у вас обязательно промелькнет информация о новых видах корма. Если обсуждали новые девайсы, то ждите рекламы с предложениями купить новый смартфон и так далее, а ведь это самый безобидный пример слежки за вами со стороны маркетинговых агентств. Хотите заинтересовать специальные службы? Существует целый список слов и выражений, употребление которых вызовет самый недетский интерес к вашей персоне. А ваш новый смартфон (тем более яблочный) – не только быстрый, мощный и красивый, но еще и следящий за вами. Например, он может

Сейчас люди больше всего боятся вирусов.

Но это быстро решаемая проблема, просто нужно скачать антивирус.
Чтобы обезопасить себя от многих ненужных проблем, я предлагаю соблюдать хотя бы основные правила безопасности в Интернете.

1.Контроль над личной информацией.

Главная опасность социальных сетей заключается в непринужденной публикации различной информации о себе. Обратите внимание на количество информационных полей, вовсе не обязательных для заполнения: где вы работаете, куда ходите, где отдыхаете. Вы сами представляете, насколько облегчаете задачу злоумышленникам? Им и взламывать ничего не придется!

2. Надежный пароль.

Придумывайте сложные пароли, состоящие не только из букв и цифр, но и из символов. Хорошо, если ваш пароль содержит такие буквы как «Х» и «Ъ»: они плохо распознаются системой и редко используются при переборке паролей.

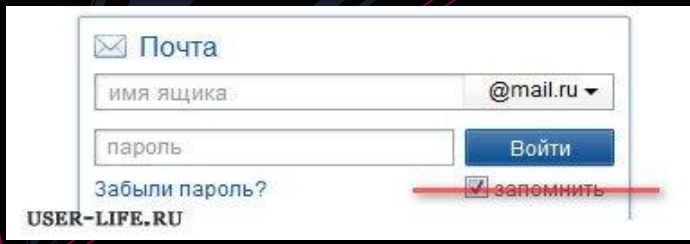
Не используйте один пароль на всех аккаунтах, лучше используйте вариацию пароля. Придумав и запомнив один сложный пароль, например YufG_453@, используйте его для регистрации и на других сервисах.

Достаточно добавлять в конец пароля первые 2 буквы от названия сайта. Например,
YufG453_@vk — для ВКонтакте
YufG4_53@fa — для Facebook.

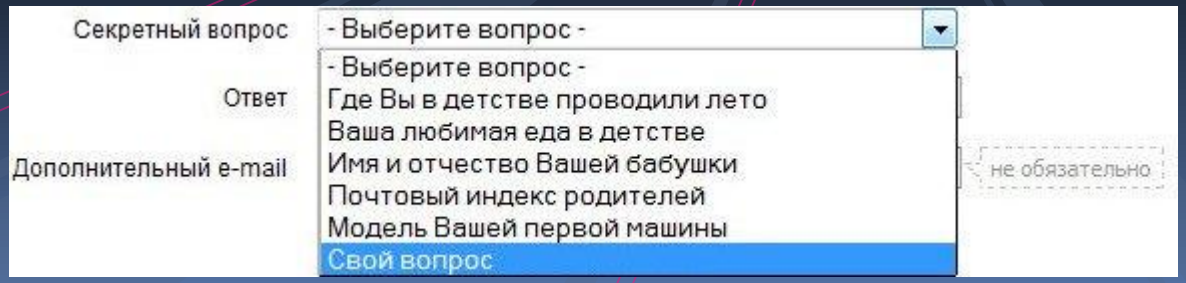
3. Электронная почта – ключ к безопасности.

Это очень важный пункт в борьбе за вашу безопасность. Более того, именно взломанный почтовый ящик — это ключ к несанкционированному доступу к разным сайтам от вашего имени. Будьте очень аккуратны с вашим паролем!

Если ваш почтовый ящик будет взломан, злоумышленник в считанные секунды изменит пароль ко всем вашим сервисам, где данный адрес использовался для регистрации. Помните о важности сложного пароля и старайтесь как можно чаще менять пароль. Не разрешайте браузеру сохранять ваш пароль от почты!



Когда речь идет о секретном вопросе для восстановления пароля, будьте оригинальны. Если вас просят дать ответ на вопрос «Название улицы, на которой Вы росли», укажите, например, ответ на другой вопрос, скажем, «Девичья фамилия вашей матери», главное — не забудьте сами, а лучше придумайте секретный вопрос самостоятельно. Вопрос получился смешным и интересным? Вот и отлично, только знать об этом больше никому не нужно!



4. Защита вашего браузера.

Большинство современных браузеров уже содержит основные средства защиты. Наиболее простой и удобный способ безопасной навигации — режим приватного просмотра (Mozilla Firefox), режим «Инкогнито» (Google Chrome), приватные вкладки и окна (Opera).

В этих режимах не сохраняются сведения о посещенных сайтах, файлы cookies, пароли и другие данные, по которым можно было бы восстановить историю работы в Интернете.

Но самый надежный способ — это использование portable-версии браузера с вашими данными на USB-накопителе. Правда, нужно позаботиться и о безопасности вашего USB-накопителя. Это можно сделать с помощью программы TrueCrypt, создав зашифрованный контейнер.

5. Чем опасны файлы cookies, и почему за ними нужно следить.

В 1990-х, когда еще господствовал браузер Netscape Navigator, прародитель современного Firefox, появилась поддержка файлов cookies («печеньки»). Эти так называемые «печеньки» были придуманы с целью сбора информации о посетителях и их поведении в сети. Примечательно, что хранить cookie-файлы, было решено не на серверах компании, а дисках посетителей.

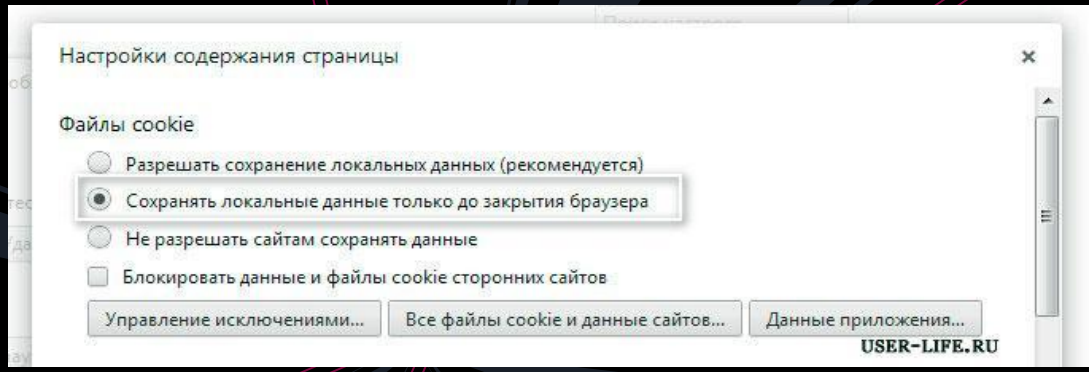
Как это работает? Сайт, на который вы пришли, чтобы прочитать утреннюю почту, присваивает вам код (к примеру, 5yfjg847gkfdk8y5hfkdh74rguiw). Этот код в качестве текстового файла высылается и сохраняется (!) на вашем компьютере и начинает, как и вы, читать вашу драгоценную почту, которую мы как бы спрятали под семью замками надежным паролем. Будьте уверены, «печенька» обязательно запишет всю вашу интересную переписку: куда вас звали в кино, в какой ресторан, какой марки вы купили телефон, на каком самолете летали, а затем обрушит на вас поток соответствующей рекламы.

Но основная опасность в том, что этот код с легкостью можно перехватить и использовать в своих корыстных целях. Мало того, у «печенек» есть друзья, так называемые маячки (биконы), они себя не высылают, они просто находятся на просматриваемом вами сайте в качестве картинки или битого пикселя, они запоминают все введенные с клавиатуры данные, распознают, в каком месте страницы курсор мышки, и делают много других «приятных» неприятностей.

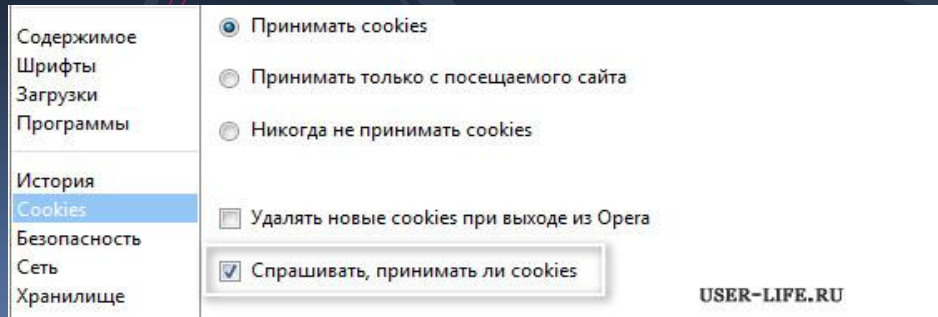
Для того чтобы знать, какие сайты запрашивают cookie-файлы, нужно активировать соответствующую функцию в браузере и при необходимости их заблокировать. Главное — не переусердствовать. Помните, что сервисы, где нужен вход под своей учетной записью (те же соцсети), используют cookie-файлы, в противном случае нам бы пришлось вводить логин и пароль снова и снова, переходя от одной страницы этого сайта к другой.

Следует отметить, что целый ряд сайтов используют cookies с неограниченным сроком жизни, то есть ваши личные данные могут храниться на них годами, поэтому cookie-файлы иногда следует удалять.

Настройки. → Показать дополнительные настройки (внизу). → Личные данные. → Настройка конвента.



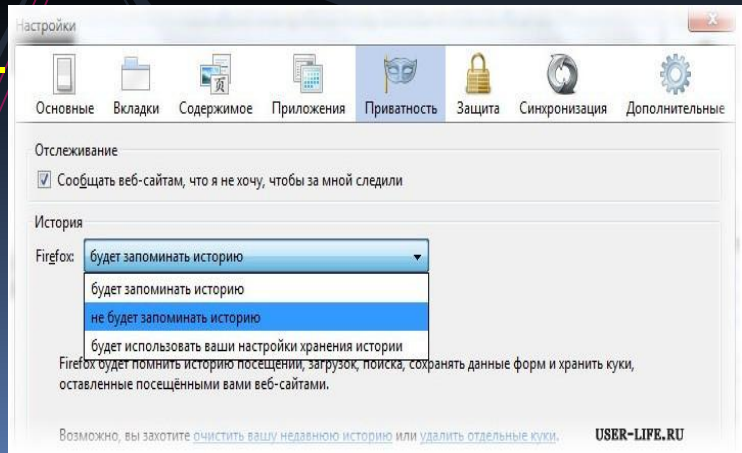
В Opera → Настройки → Общие настройки → Расширенные → Cookies.



Заметать следы можно и с помощью программ CCleaner. Она избавит систему от лишнего мусора: cookies, истории посещения сайтов, временных файлов, ActiveX-элементов. Старайтесь использовать программу если не ежедневно, то, как можно чаще.

Будьте внимательны при установке программ и более тщательно изучайте пользовательские соглашения. Если программа обязуется от вашего имени пользоваться Интернетом, телефоном или узнавать, где вы находитесь, будьте предельно бдительны.

Для большей анонимности можно скрыть свой IP-адрес. Делается это с помощью специальных программ, так называемых анонимайзеров. При совершении запроса программа передает данные провайдеру через специальное зашифрованное соединение. После этого все ваши данные отправляются на сервер анонимайзера, где проходят расшифровку, а затем маскируются.



Вывод.

Думаю, о необходимости иметь надежный антивирус, корректно работающий брандмауэр и об учете контрольных записей говорить не нужно. Соблюдая эти простые правила, можно избавить себя и близких от многих неприятностей, подстерегающих нас в сети Интернет. Надеюсь, эта информация была для вас полезна