Безопасная работа в социальных сетях: общение, публикация материалов

Презентация подготовлена для конкурса Интернешка http://interneshka.org/.

Подготовила ученица 9 класса Распопова Анастасия Павловна.

Цели:

1. Рассказать о пользе безопасного интернета.
2. Узнать о 3 простых правилах безопасной работы в интернете.
3. Показать, к чему может привести неосторожное поведение пользователя.
4. Выяснить источники опасностей при работе в интернете.

Безопасность в интернете

Перед подключением к Интернет, Вы должны подумать о том, как обезопасить себя и свои данные. За очень короткий промежуток времени в интернете без надлежащей защиты, можно серьезно навредить своему компьютеру.

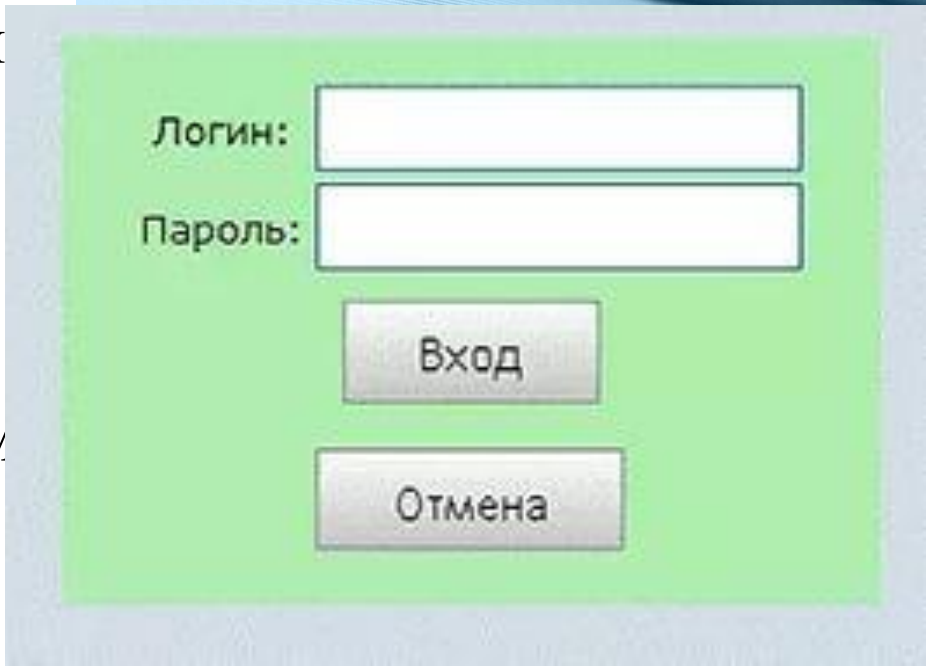
Безопасная работа в интернете: 3 простых правила

Первое и самое главное правило безопасной работы в интернете. Работая в интернете необходимо быть внимательным и немного подозрительным. Очень часто приходится наблюдать как неопытный пользователь мгновенно кликает на все ссылки, которые ему предлагают, не раздумывая ни секунды. Такое поведение, рано или поздно, неизбежно приведет к заражению вирусами.

Итак, вот несколько простых советов по «сетевой гигиене»

Необходимо следить за адресами, на которые ведут ссылки. Для того чтобы узнать адрес, на который ведет ссылка необходимо просто навести на нее курсор. Если вам предлагают перейти на сайт X, а ссылка ведет на сайт Y, то тут что-то не так. Возможно, вас пытаются обмануть.

Второе правило. Перед вводом личной информации проверяйте адресную строку браузера. Если вы там увидите что то вроде vkontokte.ru вместо привычного vkontakte, то можете быть уверены, что вы находитесь на поддельном сайте и у вас пытаются украсть парол для доступа к вашему аккаунту. После получения данных для доступа к вашему аккаунту злоумышленники могут использовать его для рассылки спама и вирусов вашим друзьям



Третье правило. Не переходите по незнакомых ссылках, которые приходят вам на почту, в «аську», или в социальные сети. Даже если ссылка пришла от знакомого человека, необходимо быть максимально внимательным. Вполне возможно аккаунт вашего знакомого уже взломан, и теперь от его имени рассылают вирусы.

Неосторожное поведение пользователя

Неосторожное поведение пользователя - неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.

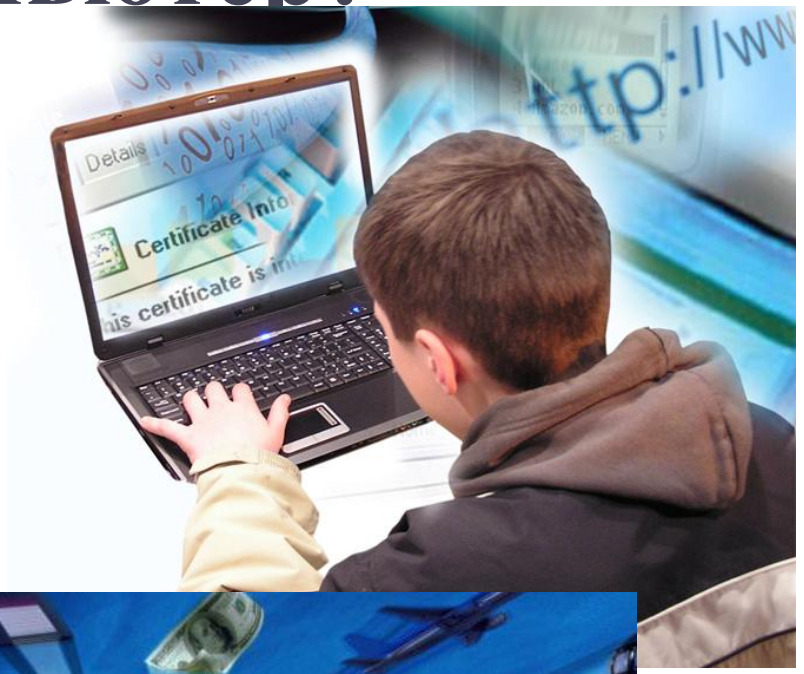
Безопасный интернет

Не думая о безопасности в интернете, люди совершают ошибки. Например, регистрируясь в какой либо социальной сети, где просят указывать верные личные данные - фамилия и имя.

Пользователи бездумно вводят все это, разумеется это же не секрет, какая мол тут интернет безопасность. Далее, разумеется нужно фото, и тут вроде бы нет никакой угрозы безопасности в интернете.

Для чего кому-то нужно взламывать ваш компьютер?

Даже если вы самый что ни на есть обыкновенный пользователь и на вашем компьютере нет какой-либо ценной и секретной информации, не нужно пребывать в иллюзии, что ваш компьютер никому (в плане его взлома) не интересен. С точки зрения хакеров и людей, распространяющих вредоносные программы, он всё равно будет представлять ценность. Времена, когда вирусы писали ради спортивного интереса, уже прошли и сегодня весь хакерский инструментарий используется ради получения коммерческой выгоды.



Источники опасностей

Подхватить вредоносную программу, к сожалению, значительно легче, чем многие себе представляют. Для взлома компьютеров пользователей сети и кражи важных данных, например, паролей электронных платёжных систем, применяются следующие методы…

1. Социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен.

2. Трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.

3. Взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях.

Интернет ресурсы

http://softuhitel.com/bezoprneteasnost-v-inte/
безопасный интернет