Безопасность ребёнка в сети Интернет: что могут сделать взрослые?

Предисловие

В современном обществе, где интернету всё больше отводится роль нескончаемого источника информации – часто приходится задумываться о безопасности.

Особенно это касается тех, кто только начинает знакомиться с данной технологией. Поэтому следует знать чего опасаться:

Предисловие

Есть много различных видов киберпреступлений. Злоумышленники обычно пытаются заполучить вашу личную информацию: пароль аккаунта электронной почты, номер мобильного телефона и т.д. Для этого используется немало приемов – установка на компьютер вредоносных программ, взлом аккаунта или просто обман. Получив желаемое, преступники могут обокрасть вас, выдавать себя за вас, удалить все ваши данные или в крайнем случае уничтожить устройство компьютера .

Следует опасаться

Вирусы

Вирусы, трояны и черви представляют собой опасные программы, которые могут распространяться через электронную почту или веб-страницы.

Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере.

СЛЕДУЕТ ОПАСАТЬСЯ

СМС – ВИРУСЫ / ВЫМОГАТЕЛИ

Довольно недавно появившийся тип вирусов.
Такой вымогатель может заблокировать доступ к системе на неопределённый срок.

Следует опасаться

Хакеры и взломщики

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных.

Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

Следует опасаться

Социальные сети

Социальные сети - замечательный способ общения с друзьями, а также место где можно познакомиться с новыми. Но следует помнить, что в там не все люди хорошие, и не всех их можно назвать настоящими друзьями.

СЛЕДУЕТ ОПАСАТЬСЯ

СПАМ

Несмотря на то что спам всегда расценивается как массовая рассылка нежелательных сообщений электронной почты, он тоже может считаться источником многих бед.

Письма присланные в виде спама, в большинстве имеют ссылки на сайты с вредоносным ПО.

В случае заражения компьютера, ваш электронный ящик тоже может стать источником рассылки спама.

Как можно обезопасить Интернет

Способы родительского контроля

Есть два основных пути обеспечения родительского контроля: данная услуга может быть обеспечена антивирусными программами, либо специально созданными под эту задачу утилитами (программами).

Среди антивирусных программ:

- Kaspersky Internet Security 2012 и Kaspersky CRYSTAL,
- Panda Internet Security
- Avira Premium Security Suite
- Dr.Web Security Space
- Microsoft Windows Live Family Safety

Как можно обезопасить Интернет

Еще один способ родительского контроля заключается в **фильтрации сайтов по их содержимому**. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается. Родителям, возможно, придется отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Вот пример нескольких утилит и программ, выполняющих функции родительского контроля:

- Crawler Parental Control 1.1
- KidsControl 2.02
- ParentalControl Bar 5.22
- Spector Pro 6.0
- КиберМама
- KinderGate
- ОдинДома

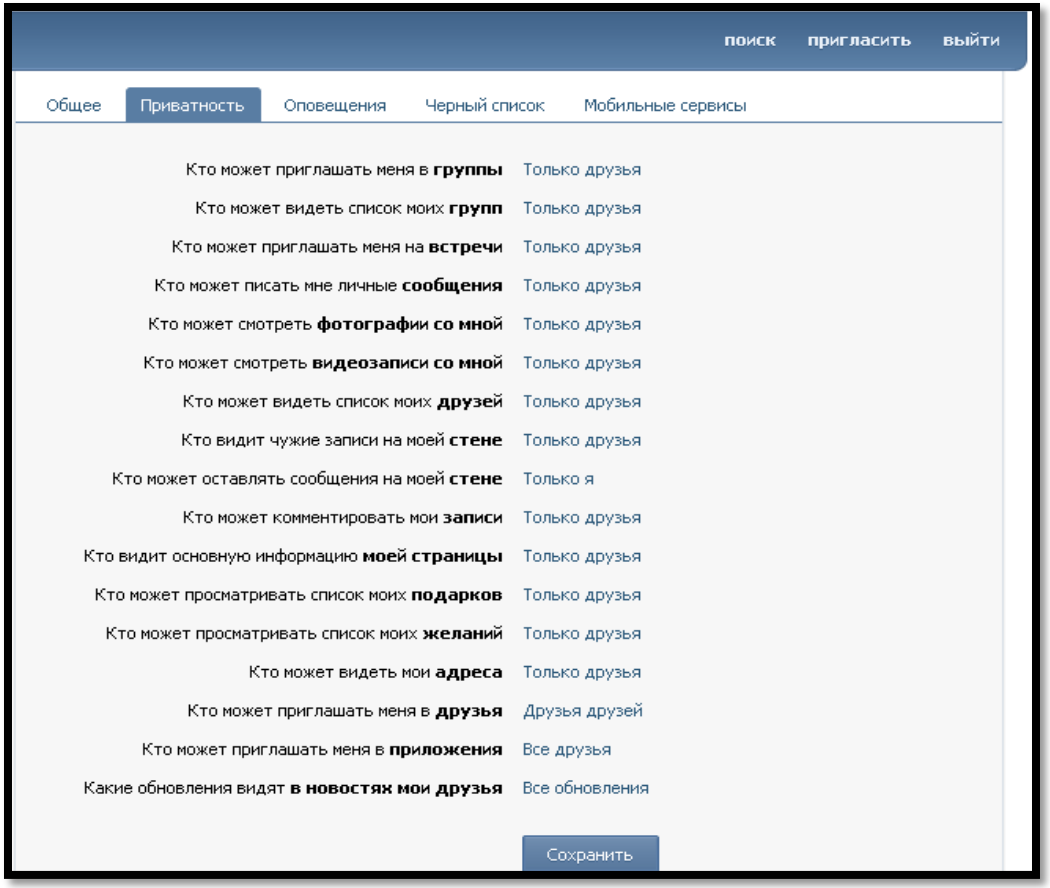
Как можно обезопасить Интернет

Так же нельзя не сказать о настройки безопасности в популярных социальных сетях. Антивирусные программы и фильтры обезопасят только от вирусов и нежелательного интернет контента.

Но как обезопасить ребёнка внутри социальной сети от недоброжелательных знакомств?

Как можно обезопасить Интернет

В любой социальной сети есть ряд настроек, которые помогут сделать профиль максимально безопасным.



Итоги

- Старайтесь держать компьютеры с подключением к Интернету в общих комнатах, в которых можно легко осуществлять визуальный контроль над тем, что делает ваш ребенок в Интернете.
- Создайте ребенку в операционной системе собственную учетную запись с ограниченными правами, чтобы он не мог заниматься чем-то посторонним без вашего ведома.
- Используйте средства фильтрования нежелательного материала. Среди бесплатных можно установить Internet Censor, который блокирует страницы исходя из общего он-лайн голосования пользователей интернета. К тому же вы без труда можете установить пароль на изменение параметров программы, а также её удаления.

Итоги

- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету без вашего присутствия.
- Требуйте от детей никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.

Итоги

- Требуйте от детей не загружать из Интернета программы без вашего разрешения. Кроме того, объясните детям, что, делая файлы общими или загружая из Интернета тексты, фотографии или рисунки, они могут нарушать чьи-то авторские права.
- Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами. Контроль лучше всего осуществлять ненавязчиво, уважая личное достоинство и право ребенка на самостоятельность.

Итоги

- Расскажите детям об ответственном, достойном поведении в Интернете.
- Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.