**Уважаемые дети и родители,**

**здравствуйте!**

**Эта страничка - специально для Вас. Мы надеемся, что советы, которые мы Вам предлагаем, помогут наладить более близкий контакт с Вашим сыном или дочкой, а значит, сделать Вашу семью счастливее...**

**Советы детям:**

|  |  |
| --- | --- |
| **Знакомство с возможностями интернета****Где найти подругу Олю?Прочитать, что было в школе?И узнать про все на свете?Ну конечно, в ИНТЕРНЕТЕ!Там музеи, книги, игры,Музыка, живые тигры!Можно все, друзья, найтиВ этой сказочной сети!** |   http://74210s118.edusite.ru/images/p65_rdgisvoyhf.jpg |
| **Познание** **Как не сбиться нам с пути?Где и что в сети найти?Нам поможет непременноПоисковая система.Ей задай любой вопрос —Все, что интересно!В миг ответ она найдетИ покажет честно.** |   http://74210s118.edusite.ru/images/p65_3gradi.jpg |
|   **Учеба****В Интернете, в Интернете,Пруд пруди всего на свете!Здесь мы можем поучиться,Быстро текст перевести,А в онлайн библиотекеКнижку нужную найти.** |   http://74210s118.edusite.ru/images/p65_plasticlogic2013100.jpg |
|   **Общение на расстоянии** **Расстоянья ИнтернетуСовершенно не страшны.За секунду он доставитСообщенье хоть с Луны.Не печалься, если вдругДалеко уехал друг.Подключаешь Интернет —Расстоянья больше нет!Электронное письмоВмиг домчится до него.Ну а видео-звонок,Сократит разлуки срок.** |   http://74210s118.edusite.ru/images/p65_e_mail_2013.jpg |
|  **БУДЬ** |  **ОСТОРОЖЕН и ВНИМАТЕЛЕН!** |

Для Вас родители!

Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

**Какие угрозы встречаются наиболее часто**? Прежде всего:

  **Угроза заражения вредоносным ПО**. Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

  **Доступ к нежелательному содержимому**. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера.

  **Контакты с незнакомыми людьми с помощью чатов или электронной почты**. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

  **Неконтролируемые покупки**. Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

     Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

     Приведем **несколько рекомендаций**, с помощью которых **посещение Интернет** может стать менее опасным для ваших детей:

1. **Посещайте Интернет вместе с детьми**. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;
2. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а **поделиться с вами** своим **беспокойством**;
3. Объясните ребенку, что **при общении в чатах**, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, **нельзя использовать реальное имя**, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;
4. Объясните ребенку, что **нельзя выдавать свои личные данные**, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;
5. Объясните своему ребенку, что **в реальной жизни и в Интернет нет разницы между** неправильными и правильными **поступками**;
6. Научите ваших детей **уважать собеседников в Интернет**. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
7. Скажите им, что **никогда не стоит встречаться с друзьями из Интернет**. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
8. Объясните детям, что **далеко не все**, что они могут прочесть или увидеть **в Интерне**т – **правда**. Приучите их спрашивать о том, в чем они не уверены;
9. **Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения**. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

**Помните**

**Обсудите с детьми опасные последствия предоставления личной информации**.

Личную информацию рекомендуется скрывать во многих различных ситуациях.

Пользователям никогда не следует сообщать пароли никому, даже давним друзьям. Кроме того, пароль необходимо регулярно менять.

Интернет является общественным местом. Перед публикацией любой информации или своих фотографий (а также фотографий других людей) следует помнить, что любой сможет получить доступ к этой информации. Чтобы выяснить, какая информация о вас доступна в Интернете, используйте поисковый модуль и в качестве поискового слова введите собственное имя.

Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте, полученном в Интернете.

**Электронная почта**

Электронная почта представляет собой широко распространенный способ отправки сообщений через Интернет, но важно использовать ее с осторожностью.

В папку входящих сообщений электронной почты может попадать спам, часто в форме рекламы, которая не предназначена специально для пользователя. Кроме риска получения вирусов через сообщения электронной почты такого типа, в спаме может также содержаться неуместный материал или ссылки, которые непригодны для детей.

Через Интернет могут также распространяться анонимные сообщения электронной почты с целью оскорбления, запугивания или преследования.

**Возможные действия**

**Установка фильтра спама**

Адрес электронной почты для ребенка рекомендуется получить у поставщика услуг Интернета, предоставляющего автоматическую защиту от вирусов и фильтрацию спама. Это помогает предотвратить получение большей части нежелательных сообщений.

**Разрешение только знакомых отправителей**

Вероятно, самый безопасный, хотя и очень ограниченный способ использования электронной почты — это настроить параметры так, чтобы ребенок получал сообщения только от указанных адресов. Многие программы электронной почты позволяют блокировать сообщения, отправляемые с определенных адресов электронной почты.

**Получение анонимного адреса электронной почты**

Адреса электронной почты часто выглядят как «имя.фамилия@домен.ru». Полное имя является личной информацией, которую не следует разглашать. Если ребенок хочет обмениваться сообщениями электронной почты с собеседниками из Интернета, лучшим способом является использование адреса электронной почты, в котором не раскрывается полное имя, например псевдоним01@домен.ru. В адресе электронной почты рекомендуется использовать цифры, поскольку в этом случае адрес будет сложнее «угадать», и, следовательно, на него будет приходить меньше спама. Не рекомендуется использовать этот же псевдоним в интерактивных чатах. От адреса электронной почты такого типа легче отказаться, если на него поступает большое число спама или других нежелательных сообщений. Широкополосная связь, как правило, включает несколько адресов электронной почты.