В Контакте. Мой мир. You Tube. Они у всех на слуху. Знаменитые сайты, социальные сети постепенно начинают проживать с нами всё больше и больше времени. Мы сами не замечаем, как уже автоматически кликаем на очередную ссылку, регистрируемся на новом сайте и придумываем логин для еще одного форума.Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в то же время, Сеть таит в себе много опасностей. Как обезопасить себя в Интернете?

Безусловные преимущества использования Интернет

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

Скрытые и открытые угрозы Интернет

Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки. Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

- Киберзависимости
- Заражению вредоносными программами при скачивании файлов
- Нарушению нормального развития ребенка
- Неправильному формированию нравственных ценностей
- Знакомству с человеком с недобрыми намерениями

Классификация Интернет-угроз

- **Контентные риски**

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контент

В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

- **Электронная безопасность**

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.
- Вредоносное ПО
- Рекламное ПО
- Шпионское ПО
- Браузерный эксплойт

Спам

Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы. подробнее

Кибермошенничество

Кибермошенничество - это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг. подробнее

- **Коммуникационные риски**

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Незаконный контакт

Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследования

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Способы защиты от Интернет-угроз

Комплексное решение в области использования сети Интернет

Опираясь на мировой опыт и анализируя ситуацию в России можно сказать, что решение вопроса по обеспечению безопасного использования Интернет представляет комплексное решение.

Оно включает в себя:

Административные (нормативно-правовые) меры, которые обеспечивает государство посредством создания/изменения законопроектов. Воспитание и обучение пользователей эффективной работе с информацией, которым занимаются специальные ресурсы (в том числе наш). Обучением работе в Интернете детей должны так же заниматься родители и педагоги. Использование современных технологических решений в области повышения эффективности использования Интернет. Разработкой специального программного обеспечения занимаются частные компании (в том числе и мы).

БЕЗОПАСНЫЙ ИНТЕРНЕТ

Родителям

Чтобы помочь своим детям, Вы должны это знать:

- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывайте файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Джентельменское соглашение

Полезные программы

Программа «Интернет Цензор» устанавливается на компьютер и обеспечивает фильтрацию для всех веб-браузеров и программ. Отличительной особенностью полной версии является высокий уровень надежности и защиты от взлома.

Загрузить бесплатно

NetPolice Lite. Облегченная версия персонального фильтра, который предоставляет наиболее важные функции для ограничения доступа пользователей к негативным, нежелательным и опасным Интернет-ресурсам. Поддерживаются самые необходимые категории и функции для безопасного использования сети Интернет.

Скачать бесплатную версию персонального фильтра

Детям и подросткам

Если ты любишь сидеть в Интернете, запомни эти правила безопасности!

Школьникам младших классов

Правило 1
Не указывай настоящее имя и фамилию. Придумай себе НИК

Правило 2
Не размещай на сайтах свои фотографии. Пользуйся аватаркой или картинками

Правило 3
Не говори никому свой адрес и номер телефона. Общайся только в Интернете.

Правило 4
Не встречайся с людьми, которых ты знаешь только по Интернету. Если кто-то приглашает тебя встретиться или оскорбляет тебя - срочно расскажи об этом родителям

Школьникам средних классов

Вы должны это знать:

- При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
- Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
- Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
- Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.
- Если вас кто-то расстроил или обидел, расскажите все взрослому.

Школьникам старших классов

Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете.

Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

- Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
- Не отвечайте на Спам (нежелательную электронную почту).
- Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
- Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
- Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Учителям и преподавателям

Чтобы помочь учащимся, Вы должны это знать:

- Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет—угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.
- Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
- Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
- Выберите интересные ресурсы и предложите детям изучить их вместе.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

Использование Интернета является безопасным, если выполняются три основные правила.

1. Защитите свой компьютер

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

2. Защитите себя в Интернете

С осторожностью разглашайте личную информацию.

Думайте о том, с кем разговариваете.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Дети онлайн. Линия помощи

- Если тебя оскорбляют и преследуют в Интернете...
- Если делают неприличные предложения в Интернете...
- Если ты стал жертвой сетевых мошенников...
- Если ты столкнулся с опасностью во время пользования сетью Интернет или мобильной связью...

Обратись на линию помощи «Дети онлайн»

Звони по телефону: 8-800-25-000-15 Звонок по России бесплатный, прием звонков — по рабочим дням с 9-00 до 18-00 мск.

Пиши по адресу: helpline@detionline.org