БЕЗОПАСНОСТЬ РЕБЕНКА в СЕТИ ИНТЕРНЕТ.

Сеть - Интернет уже стала важной частью нашей жизни, а для подростков иногда и ключевой. 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.

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 подростков.

Очень часто родители не понимают и недооценивают угрозы, которым подвергается подросток, находящийся в сети - Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, как вести себя с незнакомыми людьми, что можно говорить, а что нет, между тем «выпуская» его в Интернет не представляют себе, что точно также нужно обучить его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети.

Не стоит забывать, что Интернет – это не только кладезь возможностей, но и источник угроз. Интернет может негативно влиять на физическое, моральное, духовное здоровье подрастающего поколения, порождать девиантное поведение у психически неустойчивых школьников, представлять для детей угрозу. Поэтому главная задача сегодня – обеспечение безопасности детей, не способных иногда правильно оценить степень угрозы информации, которую они воспринимают или передают.

Какие же опасности ждут подростка в сети-Интернет?

- Сайты порнографической направленности;
- Сайты, разжигающие национальную рознь и расовое неприятие: экстремизм, национализм, фашизм.
- Депрессивные молодежные течения. Ребенок может поверить, что шрамы – лучшее украшение, а суицид – всего лишь способ избавления от проблем.
- Наркотики. Интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья».
- Сайты знакомств. Виртуальное общение разрушает способность к общению реальному, «убивает» коммуникативные навыки подростка.
- Секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам "проникнуть в мысли" и повлиять на взгляды на мир.

Это далеко ни весь список угроз сети- Интернет. Любой подросток может попасть на такие сайты случайно: кликнув по всплывшему баннеру или перейдя по ссылке. Есть дети, которые ищут подобную информацию специально, и естественно, находят. Кроме этого, появились психологические отклонения, такие как компьютерная и Интернет – зависимости, игромания (зависимость от компьютерных игр). Дети могут написать свой адрес и телефон, сведения о родителях, не всегда задумываясь о целесообразности своих действий. Кажущаяся анонимность и безопасность часто провоцирует школьников на поступки, на которые в реальном мире они бы не решились. Этим пользуются различные преступники.

Преступники устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются прельстить свою цель вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей.

Некоторые преступники действуют быстрее других и сразу же заводят сексуальные беседы. Такой более прямолинейный подход может включать решительные действия или скрытое преследование жертвы. Преступники могут также рассматривать возможность встречи с детьми в реальной жизни.

Так как же не стать жертвой в сети - Интернет? Необходимо рассказать и объяснить детям и подросткам простые правила безопасности в сети – Интернет.

Правило 1: Никогда нельзя распространяться о личной информации — своей и семейной. Сообщать свои личные и паспортные данные, ФИО, домашний адрес, координаты учебного заведения, расписание занятий, номера телефонов, личные данные своих родителей, место работы, их график и т.д. Объяснить, что никто не должен узнать, в какие часы подросток находиться дома один или когда в квартире вообще никого нет. Объяснить правила при использовании социальных сетей «Вконтакте», «Инстаграмм», «Одноклассники» и т.д., что нельзя указывать геолокацию, местоположение, выкладывать личные, семейные фото, их отправлять незнакомым людям. Не встречаться без родителей с людьми из Интернета вживую. Объяснить, что в сети никогда нельзя быть уверенным в истинной сущности человека и его намерениях. Родителям подростка необходимо очертить круг запрещённых тем, таких как порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое. Все, что противоречит российскому законодательству и целям образования, воспитания и формирования личности подростка.

Правило 2: Родителям, особенно в первое время, необходимо следить за тем, какие сайты посещает ребенок. Если среди них есть что-то подозрительное, то это повод провести беседу. Уделите внимание теме защиты от спама. Научить определять спам - сообщения и не отвечать на них, не переходить по подозрительным ссылкам. Необходимо научиться определять фишинговые сайты. Ссылки на них часто приходят на электронную почту, но их можно и просто встретить в Сети. Такие сайты выманивают данные пользователей. Их адреса похожи на популярные веб-ресурсы, выглядят они как meil.ru, wk.ru, feisbook.com. Переходить по таким линкам опасно, как минимум, можно поймать вирус.

Правило 3: Необходимо контролировать времяпрепровождения подростка в сети - Интернет. Внимательно, но не навязчиво контролировать деятельность ребенка в Интернете. Выбирать время для неконфликтного совместного просмотра интернет-страниц. Необходимо контролировать действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают. Надежный антивирус, с постоянно обновляемыми базами, с поддержкой функции «Родительского контроля». Вместе с ним

должен быть установлен и хороший фаервол (сетевой экран). Если дети проводят много времени дома одни, то необходимо ограничивать время нахождения его в интернете. Установить на браузер необходимые дополнения для удобной и безопасной работы в интернете и научить пользоваться этим детей.

Правило 4: Очень важно распознать интернет - зависимость детей на ранней стадии и установить пределы на его использование. Если вы обнаружили зависимость вашего ребенка, не ждите чуда, начинайте действовать сегодня! В принципе, ничего плохого в том, что детская «тусовка» собирается в киберпространстве нет. Но все же не стоит забывать, что ребенку нужно и живое общение со сверстниками. Подумайте, не слишком ли сильно Вы его ограничиваете в контактах? Или может быть, ему сложно найти общий язык с одноклассниками? Возможно, он просто пытается уйти в сеть потому, что чувствует себя одиноким. В этом случае Ваша задача состоит в том, чтобы помочь ему расширить круг своих «реальных» друзей — предложите ему пойти в секцию, разрешите приглашать друзей домой.

Правило 5: Компьютер, подключенный к Интернету, должен находиться в общей комнате. Для обеспечения безопасности в интернете, сделайте разные учетные записи. Учетные записи детей сделайте с ограниченными правами, не делайте записи с правами администратора детям, особенно младшего возраста. Свои учетные записи и администратора защитите паролем. Если дети пользуются компьютерами в местах, находящихся вне вашего контроля, – общественной библиотеке, школе или дома у друзей – выясните, какие защитные средства там используются.

Правило 6: Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться с вами перед тем, как воспользоваться теми или иными услугами в Интернете. Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды.

Правило 7: Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы. Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.
Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.
Собственно, поведение подростка в интернете не должно сильно отличаться от поведения в реальном мире.

Для лучшего взаимопонимания и устранения возможных недоразумений, сразу расставьте все точки над «и», и установите некоторые ограничения для самостоятельного выхода подростков в сеть - Интернет. Обсудите это со своими детьми, чтобы они понимали необходимость подобных запретов, тогда вместе вы обязательно сможете сделать прогулки ребенка в Сети наиболее безопасными.