Правила работы в сети Интернет и мобильных сетях связи для детей и родителей

Наиболее частые угрозы в сети:

1. Угроза заражения вредоносным Программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить почту, компакт-диски и прочие сменные носители информации или скачанные из сети Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня стало простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов.
2. Доступ к нежелательному содержимому. Сегодня любой ребенок, выходящий в сеть Интернет, может просматривать любые материалы. К таким материалам относится насилие, наркотики, порнография, страницы с националистической или откровенно фашистской идеологией и многое другое.
3. 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.
4. Интернет-магазины. Несмотря на то, что покупки через сеть Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Рекомендации по уменьшению опасности от посещений детьми Интернет.

1. Посещайте сеть Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения сети Интернет;

2. Объясните детям, что если в сети Интернет что–либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;
3. 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.;
4. Научите ваших детей уважать собеседников в сети Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково и в Интернет, и в реальной жизни;
5. Объясните детям, что далеко не все, что они могут прочесть или увидеть в сети Интернет - правда. Приучите их спрашивать о том, в чем они не уверены;
6. Не забывайте контролировать детей в сети Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Домашний контроль работы в сети.

Родителям необходимо постоянно вести разъяснительную работу, т.к. без понимания данной проблемы невозможно ее устранить силами только учителей. Очень часто родители не понимают или недооценивают те угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, тому, как вести себя с незнакомыми людьми, что можно говорить о себе, а что нет, между тем, «выпуская» его в сеть Интернет, не представляют себе, что точно так же нужно обучить его основам безопасности в сети Интернет.

Ребенок абсолютно беззащитен перед потоком информации. Дома необходимо выработать общие правила, которые бы сводились к следующему:
* Какие сайты могут посещать дети и что они могут там делать;
* Сколько времени дети могут проводить в сети Интернет;
* Как защитить личные данные;
* Как следить за безопасностью;
* Как вести себя вежливо;
* Как пользоваться чатами, группами новостей, службами мгновенных сообщений.

Соблюдайте выполнение данных правил и рекомендаций!!! Регулярно, по мере необходимости, вносятся изменения!