Медиа - безопасность. Безопасность детей в сети.

Не секрет, что родители одновременно с детьми постигают азы работы в Интернете. А так же, что дети знают об Интернете больше, чем родители. Чтобы взрослые смогли как-то уберечь ребенка от возможных угроз со стороны Интернета, им нужно знать о них, способах предотвращения, к кому обратиться за помощью.

Не стоит оберегать ребенка от Интернета (как известно, запретный плод сладок), нужно учить его правилам поведения в сети и ограничивать по времени.

Современные дети могут использовать возможности сети с разными целями: для общения, развлечения и самообразования. Пока первые две цели перекрывают последнюю и именно такое времяпровождение может таить различные угрозы: вредоносные программы, небезопасные сайты, интернет-мошенники, плохие знакомства и так далее.

Некоторые советы родителям:

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети и их последствиях.
2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
5. Спрашивайте ребенка о том, что он видел и делал в Интернете
6. Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
7. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
8. Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.
9. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
10. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
11. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
12. Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
13. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;
14. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Как помочь:

- Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
- Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.

- Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
- В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Будет полезно и родителям.

Для того, чтобы обезопасить себя, любой пользователь Сети должен соблюдать несколько простых правил:

- ✓ Пользоваться антивирусом:современный, регулярно обновляемый антивирус обеспечит надежной защитой от разнообразных интернет-угроз;
- ✓ Регулярно загружать обновления:обновления программ закрывают уязвимости, которыми могут воспользоваться злоумышленники;
- ✓ Не оставлять своих персональных данных на открытых ресурсах: данные, оставленные в Интернете, собирают роботы злоумышленников, которые в дальнейшем могут использовать их в своих целях (например, присылать на ваш почтовый ящик больше спама);
- ✓ Не загружать ничего со случайных сайтов: высока вероятность того, что вместе с загруженной программой/книгой/фильмом вы получите и вредоносную программу;
- ✓ Не проходить по ссылкам в спамовых письмах: такие ссылки зачастую ведут на мошеннические, либо зараженные вредоносными программами сайты;
- ✓ Не открывать приложения в письмах, если есть хоть какие-то сомнения в надежности адресанта: Высока вероятность того, что в приложении содержится вредоносная программа (даже если это документ Word);
- ✓ Не пытаться «отписаться» от спама (особенно в том случае, когда в спамерском письме есть соответствующая ссылка): избавиться от спама это не поможет, скорее наоборот. Существуют два наиболее вероятных варианта развития событий: 1) спамеры регулярно запускают автоматическую проверку и чистку своих баз от несуществующих адресов; отвечая на письмо, вы подтверждаете, что ваш адрес (который был, возможно, подобран автоматически) действительно существует, его действительно читают. Это побудит спамеров внести его в отдельные, «чистые» базы, вследствие чего вам будет приходить еще больше спама; 2) пройдя по ссылке, вы попадете на зараженный сайт и получите вредоносную программу на свой компьютер;
- ✓ Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег: откликнувшись, вы или потеряете свои деньги, или, что гораздо хуже, окажетесь замешаны в преступные махинации.