

Рекомендации для родителей



Чтобы помочь своим детям, вы должны это знать:

1. Будьте в курсе того, чем занимаются ваши дети в интернете.

Попросите их научить вас пользоваться различными приложениями,

которыми вы не пользовались ранее.

2. Помогите своим детям понять, что они не должны

предоставлять

никому информацию о себе в интернете – номер мобильного телефона,

домашний адрес, название/номер школы, а также показывать фотографии

свои и семьи. Ведь любой человек в интернете может это увидеть.

3. 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.

4. Объясните детям, что нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.

5. Помогите ребенку понять, что некоторые люди в интернете могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

6. Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в интернете.

7. 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 обратиться.

8. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Возможные опасности, с которыми сопряжен доступ детей к интернету

1. Неприемлемые материалы. В интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий.

2. Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что в конечном счете приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.

3. Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию.

Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол и информация о семье, могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации.

4. Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, «червь», «троян», «зомби» или другой код, разработанный со злым умыслом.

Меры предосторожности:

1. Побеседуйте с детьми. Первое, что необходимо сделать, – это объяснить им, что нахождение в интернете во многом напоминает пребывание в общественном месте. Многие опасности, подстерегающие пользователя интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности.

2. Разработайте правила пользования интернетом:

1) четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при использовании интернета. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами;

2) пароли. Предупредите детей о том, что они не должны никому сообщать свои пароли, даже если человек утверждает, что является сотрудником вашего поставщика интернет-услуг (например, представляется вашим провайдером). Поставщик услуг интернета никогда не будет спрашивать, какой у вас пароль;

3) разработайте «домашнюю» политику. Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании интернета. Например: нельзя разглашать информацию личного характера.

Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию. Ребенок ни в коем случае не должен

соглашаться на личную встречу с виртуальным другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых;

4) следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемым и поддерживается заслуживающей доверия компанией или организацией;

5) установите компьютер в помещении, используемом всеми членами семьи, а не в комнате ребенка. Это упростит контроль за пребыванием детей в интернете. Воспользуйтесь современными технологиями;

6) контролируйте входящие и исходящие сообщения электронной почты своего ребенка. Знакомьтесь с его виртуальными друзьями подобно тому, как вы знакомитесь с реальными;

7) регулярно просматривайте журнал веб-обозревателя. Из него вы узнаете, какие веб-узлы посещали ваши дети и как часто они это делали;

8) настройте веб-обозреватель в режиме обеспечения безопасности.

Помните!

Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.

Как сделать посещение интернета для детей полностью безопасным:

1. Поощряйте детей делиться с вами их опытом в интернете.

Посещайте Сеть вместе с детьми.

2. Научите детей доверять интуиции. Если их в интернете что-либо беспокоит, им следует сообщить об этом вам.

3. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

4. Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

5. Объясните детям, что разница между правильным и неправильным одинакова: как в интернете, так и в реальной жизни.

6. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

7. Настаивайте, чтобы дети уважали собственность других в интернете.

Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

8. Скажите детям, что им никогда не следует встречаться с друзьями из интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

9. Скажите детям, что не все, что они читают или видят в интернете, правда. Приучите их спрашивать вас, если они не уверены.

10. Контролируйте деятельность детей в интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

Дети могут предпринимать следующие меры предосторожности:

– никогда не скачивать изображения из неизвестного источника – они могут иметь откровенно сексуальный характер;

– использовать фильтры электронной почты;

– немедленно сообщать взрослым обо всех случаях в интернете, которые вызвали смущение или испуг;

– использовать нейтральное в половом отношении экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений;

– никогда и никому в интернете не сообщать информацию о себе (включая возраст и пол) или о семье; никогда не заполнять личные профили в Сети;

– прекращать любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вопросы личного характера или содержащие сексуальные намеки.