

О медиабезопасности детей

Медиабезопасность детей в сетях Интернет и сотовой связи.

Медиа-грамотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Медиа-образование выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества.

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").

Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила медиа-безопасности детей при обороте на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

1. Как защитить ребенка от нежелательного контента в Интернете?

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, азартных игр, наркотических веществ и т.д.

Как помочь ребенку избежать столкновения с нежелательным контентом:

- приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;
- объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены;
- старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

2. Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете?

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты, киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Меры предосторожности:

- будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;

- объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;

- если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;

- не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;

- интересуйтесь тем, куда и с кем ходит ваш ребенок.

3. Как избежать кибербуллинга?

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

- 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;

- научите детей правильно реагировать на обидные слова или действия других пользователей;

- объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;

- старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- 1. Беспокойное поведение.** Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- 2. Неприязнь к Интернету.** Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- 3. Нервозность при получении новых сообщений.** Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок

регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

4. Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников?

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

- проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;
- прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности.

Ознакомьтесь с отзывами покупателей:

1. Проверьте реквизиты и название юридического лица – владельца магазина
2. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
3. Поинтересуйтесь, выдает ли магазин кассовый чек.
4. Сравните цены в разных интернет-магазинах.
5. Позвоните в справочную магазина.
6. Обратите внимание на правила интернет-магазина.
7. Выясните, сколько точно вам придется заплатить.

5. Как распознать интернет- и игровую зависимость?

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

6. Как научить ребенка не загружать на компьютер вредоносные программы?

Вредоносные программы (вирусы, черви, «тройные кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных; такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения;
- используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр;
- объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелегальный контент;
- периодически старайтесь полностью проверять свои домашние компьютеры;
- делайте резервную копию важных данных;
- старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

7. Что делать, если ребенок все же столкнулся с какими-либо рисками?

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать;

Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;

Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете.

Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.

Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы).

Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон

доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и др.)

8. Общие рекомендации по обеспечению безопасности детей и подростков в Интернете.

1. Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что делают дети в Интернете.

2. Следите, какие сайты посещают ваши дети. Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.

3. Расскажите детям о безопасности в Интернете. Вы не сможете все время следить за тем, что ваши дети делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.

4. Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.

5. Научите детей ответственному поведению в Интернете. Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в Сети.

6. Оценивайте интернет-контент критически. То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

7. Если Вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если Ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи “Дети Онлайн” (www.detionline.com), по телефону: 8 800 25 000 15 (звонок по России бесплатный). На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет.

9. Рекомендации Абонентам сотовой связи.

1. Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.

2. Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученных посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию.

3. Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.

4. Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

5. Не торопитесь давать телефон на «1 звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

6. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения - то и от известных. С развитием функциональности мобильных телефонов, КПК и коммуникаторов хакеры стали уделять больше внимания созданию вредоносного ПО для этих устройств. По возможности, установите на мобильное устройство одну из многих антивирусных программ, которые вы можете найти на сайтах известных производителей антивирусного ПО.

7. Для разблокировки компьютера от вирусов используйте антивирусное ПО известных разработчиков, в том числе, бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение интернет-баннера при отправке смс на короткий номер.

10. Рекомендуем познакомиться.

Детские поисковые системы:

1. Поисковая система "АгА"
2. Детский браузер Гогуль
3. KINDER online.ru-детский портал

Детские социальные сети:

1. Смешарики (<http://www.smeshariki.ru/>)
2. ClassNet(<http://www.classnet.ru/>
3. Webkinz (http://www.webkinz.com/ru_ru/
4. Твиди (<http://www.tvidi.ru/ch/Main/>)