Министерство образования Кировской области
Кировское областное государственное образовательное автономное учреждение дополнительного профессионального образования «Институт развития образования Кировской области»
(КОГОАУ ДПО «ИРО Кировской области»)

Методические рекомендации по проведению работы с родителями и детьми по вопросам защиты персональных данных

Составитель: Скурихина Ю.А., проректор по УМР КОГОАУ ДПО «ИРО Кировской области»

Оглавление

Введение

В преддверии новогодних праздников в интернете появилось большое количество ресурсов, предлагающих написать письмо Деду Морозу. Для того, чтобы сообщение было отправлено, нужно указать имя, фамилию, возраст, адрес, номер телефона и другую информацию о себе. Естественно, чаще всего пользователями этой услуги становятся дети. Указание персональной информации может повлечь серьезные последствия. Именно поэтому важно провести беседы с детьми (в рамках классных часов) и родителями (на родительских собраниях).

I. Вопросы, подлежащие рассмотрению на родительских собраниях

1. Понятие персональных данных

Согласно ФЗ РФ №152 от 27 июля 2006 года персональными данными считается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и так далее. Вся эта информация конфиденциальна и может распространятся только с письменного разрешения субъекта, а в случае с несовершеннолетними – их законного представителя.

Передача персональных данных в письмах деду Морозу, ведет к нарушению законодательства, т.к. обработка, включая использование и распространение персональных данных несовершеннолетних, содержащихся на указанных интернет-страницах, осуществляется без подтверждения наличия согласия законных представителей.

Кроме того, письма детей вместе со всей персональной информацией размещаются в открытом доступе для неограниченного круга лиц, что также является грубейшим нарушением законодательства.

2. Угрозы сети Интернет

Работая в Интернете, каждый из нас обязательно оставляет хоть какую-нибудь информацию о себе. И не всегда мы задумываемся о том, что в Интернете, как в американских детективах, «любая наша информация может использоваться против нас».

Опасность заключается в том, что раз выдав информацию, человек уже перестает ее контролировать. И далеко не факт, что информация о гражданине не будет использована во вред ему же.

Эта информация поможет злоумышленникам совершить целую массу преступлений против собственности. По имущественному положению выбрать себе подходящую жертву. К человеку с неплохим доходом могут нанести визит «домушники», мошенники или вымогатели.

Чужие паспортные данные помогут мошеннику совершить множество Интернет-покупок за чужой счет, а то и взять кредит – за который придется расплачиваться реальному владельцу паспорта.

Информацией, сокрытой в анналах правоохранительных органов, можно шантажировать – а перед выборами, скажем, вбросить «компромат» на местного политика.

Нередко школы и детские кружки, делая свои сайты, публикуют сведения о своих учениках - не только списки классов, но и фотографии детей, а то и домашние адреса. Этими страницами могут пользоваться похитители детей и педофилы. В России закон о персональных данных запрещает публиковать такую информацию без согласия.

Часто Интернет-пользователям приходится страдать от «бытового компромата», который зачастую они сами же на себя и дали. Интернет превратился в удобное место для публикации порочащих и позорящих материалов, которые могут серьезно осложнить жизнь человеку. При этом могут публиковаться как настоящие фото, так и изображения, полученные в результате фотомонтажа.

Однако гораздо чаще пользователи сами выкладывают на себя «компромат» А последствия чаще всего бывают такие: человеку вдруг становится невозможно или очень сложно найти новую работу, ему не дают повышений, не допускают к серьезным проектам, не дают визу, а то и вообще обвиняют в правонарушении или преступлении.

В России явление «краж идентичности», к сожалению, набирает обороты. Доски объявлений в Интернете, спам-рассылки и пиратские лотки переполнены предложениями купить базы данных на миллионы граждан.

Главный совет, который можно дать в сложившейся обстановке, таков: всегда тщательно обдумывать, какую именно информацию он хочет или должен предоставить\опубликовать. И если взрослый способен оценить реальные опасности от размещения персональных данных в сети Интернет, то детям это достаточно сложно. Именно поэтому родители должны обращать особое внимание на то, чем дети занимаются в глобальной сети.

3. Советы родителям

Полученные в сети данных могут использоваться для совершения различных действий, наносящих вред ребенку. Так, мошенник, получивший персональные данные, может завести знакомство с ребенком через сеть Интернет.

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

«Груминг» - установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. 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.

Предупреждение груминга:

1. 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.

2. 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.

3. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.

4. Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;

5. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Рекомендации Центра безопасного Интернета в России

Объясните ребенку основные правила поведения в Сети:

1. Нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей.

2. Если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.

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

Основной площадкой для кибербуллинга в последнее время являются социальные сети. Особенно остро переживают кибербуллинг дети 9-10 лет.

Рекомендации Фонда Развития Интернет по предупреждению кибербуллинга:

1. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов –читать грубости так же неприятно, как и слышать.

2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем.

3. Если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации –практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.

4. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз.

5. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Объясните детям опасность передачи персональных данных в письмах деду Морозу, а лучше напишите такое письмо вместе с ними и отправьте его по почте!

II. Вопросы, которые нужно обсудить с детьми

1. Советы детям по использованию сети Интернет

В Интернете можно встретить самых разных людей и далеко не все из них отличаются дружелюбием и благими намерениями. Многие не прочь поживиться за счет чужого кошелька, зло пошутить или просто испортить настроение. Как же выявить из огромной массы пользователей личностей, которые могут причинить вред?

Для того, чтобы обезопасить себя от неприятных ситуаций, необходимо соблюдать максимальную осторожность и правила безопасности в Сети. Помните: вы не можете быть уверенным в человеке, которого не знаете лично, поэтому заочное недоверие к любому новому знакомому является вполне оправданной мерой. Не сообщайте никакой личной информации о себе, особенно это касается счетов, контактов и персональных данных. Чем меньше знает о вас злоумышленник – тем меньше может сделать. Не принимайте от непроверенных людей никаких файлов и уж тем более не устанавливайте их. Ибо присланная «забавная фишка» или «игрушка» может оказаться трояном или вирусом, который доставит немало хлопот.

Даже если вам предлагают написать письмо деду Морозу, помните: ему не нужны ваши персональные данные.

Не принимайте все слова Интернет-собеседников за чистую монету. Сообщения вроде «срочно положи мне денег на счет, потом верну» или «позвони мне на такой-то номер» в 100% случаев окажутся разводом. Также не стоит переходить по ссылкам, даже если это якобы страничка с чьими-то фотографиями. В лучшем случае по этому адресу окажется реклама или порнография, в худшем – под их прикрытием получите еще и вирус в подарок.

При совершении покупок в Интернете будьте предельно внимательны. Тщательно изучите сайт магазина и способы перечисления денежных средств. Изучите отзывы других клиентов и проверьте черные списки в Сети. Ни в коем случае не покупайте сомнительные товары вроде секрета «как бесплатно пользоваться мобильной связью» или «как соблазнить любую девушку за 5 минут». За такими объявлениями чаще всего прячется обыкновенное мошенничество, и Вы не сможете не только «бесплатно пользоваться мобильником», но и вернуть свои деньги.

Рискованно отправлять свои фотографии сетевым знакомым. Среди них существует немало шутников, которые способны выложить их на сайтах сомнительного содержания и доставить вам немало морального вреда.

Хорошо если простые переживания, а ведь могут не так понять, например, на работе или при устройстве на нее… Если же вы все-таки стали жертвой шутника, постарайтесь реагировать на его проделки как можно спокойнее. Если вы не будете нервничать и расстраиваться – злоумышленник своей цели не достигнет, и ему обычно быстро надоедает «заниматься» именно Вами.

Лучше всего не вступать в переписку со спамерами и подозрительными личностями, рассылающими ссылки. Попытки их пристыдить успехом не увенчаются, только зря потратите свое время. Хотя бы просто потому, что рассылкой обычно занимается робот, совестью пока не обладающий.

Тем не менее, не надо думать, что все обитатели Интернета являются мерзавцами, пытающимися вам навредить - среди них есть много интересных отзывчивых людей, которые могут стать настоящими друзьями. Просто для Интернета более чем характерен старый принцип «Доверяй, но проверяй» - и следование ему обычно окупается сторицей.

2. Памятка «Как защитить персональные данные в сети Интернет)

(с сайта «Персональные данные.дети»)

1) Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

2) Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

3) Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.

4) Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

5) Используйте только сложные пароли, разные для разных учетных записей и сервисов.

6) Старайтесь периодически менять пароли.

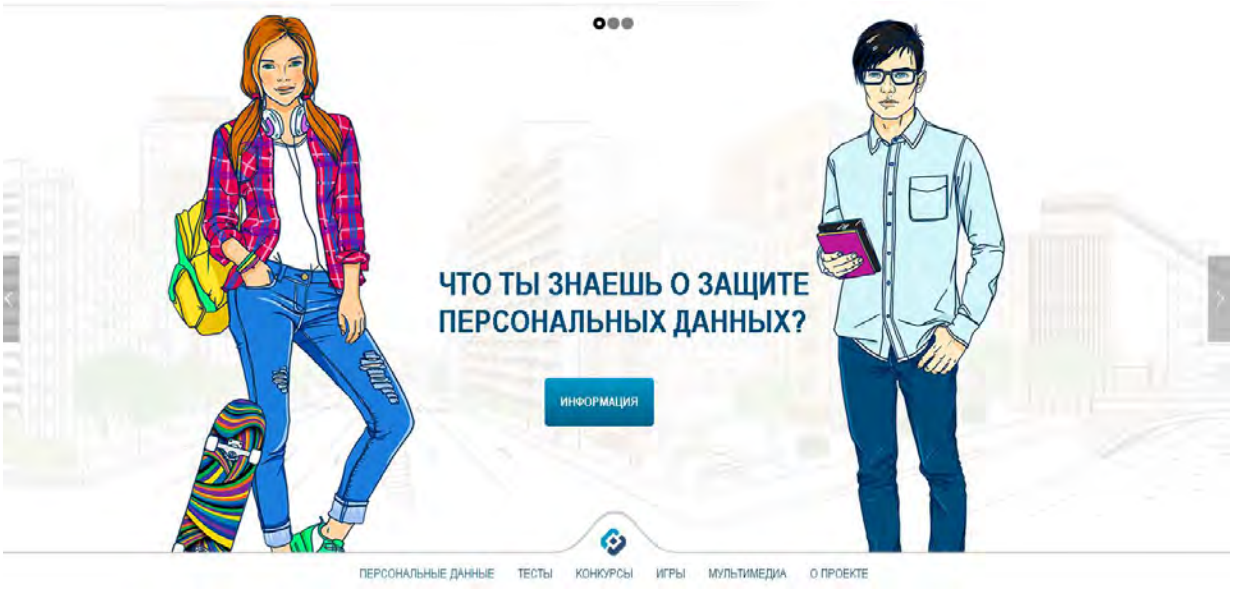
7) Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

3. Полезные ресурсы:

Существует немало полезных сайтов по вопросам безопасности детей в сети Интернет.

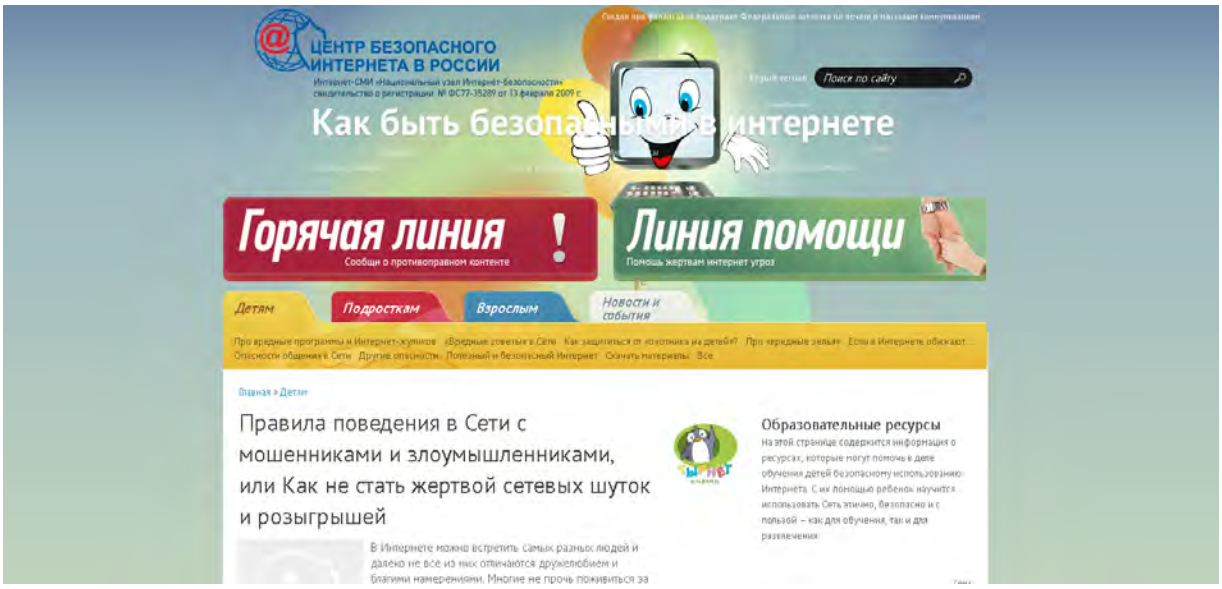
1. Сайт Персональныеданные.дети

На сайте содержится информация о проблеме защиты персональных данных для детей и их родителей, обучающие ролики, игры, тесты, конкурсы.



2. Центр безопасного Интернета (http://www.saferunet.org)

Сайт содержит информацию по актуальным вопросам для детей, подростков, родителей, включает горячую линию и линию помощи.



Заключение

Количество пользователей сети Интернет растет с каждым днем, а сами пользователи стремительно молодеют. Именно поэтому вопросы обеспечения безопасности детей в глобальной сети актуальны всегда. Вопросы общей безопасности ребенка в информационной образовательной среде, основные характеристики социальных сервисов, источники информационной опасности, способы заражения и проникновения угроз, методик и их распознавания, действия по их нейтрализации; меры по ограждению от вредного влияния негативного медийного контента, а также проблемы формирования общей культуры работы детей в информационной образовательной среде и взаимодействия с информационно насыщенном социуме должны стать постоянной темой родительских собраний и классных часов, а не только в преддверии новогодних праздников, когда мошенники решили прикинуться Дедом Морозом.

Список литературы

1. Как защитить ребенка от негативного контента в СМИ и Интернете (методические рекомендации по проведению общешкольных тематических родительских собраний) / Т.С.Пивоварова, М.В.Кузьмина. - Киров: ИРО Кировской области, 2013. -62 с/

2. Материалы сайта «Персональные данные.дети» [Электронный ресурс]: Режим доступа: http://персональныеданные.дети/

3. Материалы сайта «Центр безопасного Интернета» [Электронный ресурс]: Режим доступа: http://www.saferunet.org