Материал для родительского инструктажа по мерам безопасного использования Интернет

По материалам
http://detionline.com
http://www.saferunet.ru

С каждым годом Интернет становится доступнее и популярнее, охватывая все больше аудитории. Большинство родителей не запрещают своим детям пользоваться Интернетом. И это естественно, ибо Сеть – не только развлекательный, но и познавательный инструмент.

Однако для использования этого инструмента, как и любого другого, нужно представлять риски, связанные с его использованием.

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения. ***Поинтересуйтесь у оператора связи, предоставляющего доступ к сети, о наличии услуги контентной фильтрации для детей.***

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты, киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

Коммуникационные риски включают в себя «незаконный контакт» и «киберпреследование» (или кибер-буллинг).

Незаконный контакт – это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече.

Киберпреследование (или кибер-буллинг) – это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование. По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.

Подобный унизительный контент может исходить от одного человека или группы людей по одному или нескольким электронным контактам жертвы, на электронный ящик

или в сообщениях онлайн-мессенджеров. Распространены также случаи преследования в социальных сетях или на подобных им ресурсах. При этом помимо рассылки оскорбительных сообщений и вывешивания унизительных материалов, изображений или видеозаписей, буллер может также взломать профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

К сожалению, кибербуллинг – очень распространенное явление среди российских подростков. Каждый пятый ребенок может признать, что подвергался буллингу онлайн или в реальной жизни. И это беда не только России, она распространена во всем мире.

Лучше всего не вступать в общение со спамерами, подозрительными личностями, рассылающими ссылки или публикующими оскорбительные сообщения. Попытки их пристыдить успехом не увенчаются, только зря потратите свое время.

Электронные (кибер-) риски – это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный и финансовый ущерб. ***Основное средство защиты – установка и регулярное обновление антивирусной программы и другие настройки защиты компьютера.***

Защита в социальных сетях – это задача, которая не так давно стала особенно актуальна для их пользователей. Взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете. Что может сделать пользователь? – ***Внимательно относиться к своим логинам и паролям, не устанавливать пароли типа «123» и никому их не передавать и, тем более, не пересылать по электронной почте.***

Потребительские риски включают в себя: риск приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции, потерю денежных средств без приобретения товара или услуги, хищения персональной информации с целью кибер-мошенничества и др.

Как правило, для совершения покупки в сети достаточно указанных на банковской карте реквизитов. Дети, совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ. ***Не разрешайте детям совершать покупки или сделки в сети без вашего участия.***

Основные правила для родителей

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) 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. Постарайтесь 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.

Много интересных материалов по данной тематике Вы можете найти на сайтах:

- Подросток и закон (раздел «Интернет-угрозы») http://podrostok.edu.yar.ru/safety/index.html
- Центр безопасного интернета в России *(сайт рекомендован Уполномоченным при Президенте РФ по правам ребенка*) http://www.saferunet.ru/ruaoi
- Лига безопасного интернета. Энциклопедия безопасности http://www.ligainternet.ru/encyclopedia-of-security
- Сетевичок.рф Проводник в мире интернета http://сетевичок.рф
- WWW.I-DETI.ORG Безопасный интернет для детей: законодательство, советы, мнения, международный опыт http://i-deti.org/
- Управление «К» МВД России http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii
  Памятка «Управление «К» предупреждает: будьте осторожны и внимательны!» http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Pamjatka_Upravlenie_K_preduprezhdaet

Так, например, на сайте «WWW.I-DETI.ORG Безопасный интернет для детей» в разделе «Видео» (http://i-deti.org/video/) размещена подборка обучающих и развивающих видеоматериалов, которые помогут детям получить представление о приемлемых моделях поведения в Интернете. Все представленные здесь видеоролики в простой и доступной форме информируют юного пользователя сети о всевозможных аспектах взаимодействия с другими пользователями Интернета, о неоднозначных и затруднительных ситуациях, которые могут возникнуть во время пребывания в виртуальном пространстве, о том, как можно решить те или иные проблемы и куда можно обратиться в случае столкновения с недоброжелательностью и нарушением законов об информационной безопасности.