**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 Cети. 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.***