**Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Одной из важнейших координат их развития становятся инфо-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для их родителей. Используя исследования рисков онлайн-среды и статистику работы Линии помощи «Дети онлайн», мы предлагаем Вам полезную информацию и серию рекомендаций. С их помощью Вы сможете помочь своему ребенку использовать интернет более грамотно и безопасно.**

***В основе рекомендаций лежит разработанная Фондом Развития Интернет классификация интернет-рисков, результаты исследования «Дети России онлайн», которое было проведено Фондом Развития Интернет по методологии международного исследовательского проекта Еврокомиссии «EU KidsOnline II» (2010—2011 годы), а также обращения пользователей, поступившие на Линию помощи «Дети Онлайн».***

***Основные правила безопасности для родителей***

***Как помочь? Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой?***

***Вы можете***[***скачать эти рекоммендации***](http://detionline.com/assets/files/helpline/parents_rules.doc)***.***

***Так же Вы можете скачать буклет с рекомендациями для родителей:***[***По коммуникационным рискам***](http://detionline.com/assets/files/helpline/kommunikacionnye_riski.pdf)[***По контентным рискам***](http://detionline.com/assets/files/helpline/kontentnye_riski.pdf)[***По интернет-зависимости***](http://detionline.com/assets/files/helpline/Internet-zavisimost.pdf)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Профилактика основных интернет-рисков и борьба с ними***

***Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.***

***Предупреждение кибермошенничества. Как справляться с кибермошенничеством ?***

***Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.***

***Предотвращение кибербуллинга. Как справляться с кибербуллингом?***

***Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Исследования буллинга начались еще в 70-х годов.прошлого века. Это поведение всегда присутствует в подростковой среде. В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Многие исследования показывают, что кибербуллинг часто сопровождает традиционныйбуллинг.***

***Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.***

***Встречи с незнакомцами и груминг. Как противостоять грумингу?
Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информаию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.***

***Контентные риски. Рекомендации по предупреждению контентных рисков
К контентным рискам относятся материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.
Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.
Вредоносный (опасный) контент - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков. Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию,способную оскорбить пользователей.Подобное содержимое может распространяться ограниченно (например, "только для взрослых").
Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения,способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообещния, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы,психологического развития, социализации, а также физического здоровья детей и подростков.***

***Предупреждение интернет-зависимости. Как справляться с интернет-зависимостью?***

***Интернет-зависимость — навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.***