Памятка родителям по информационной безопасности детей в сети Интернет.

Дети и подростки – активные пользователи интернета. С каждым годом сообщество интернет-пользователей молодеет. 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. Один вид из рисков, которые могут ожидать детей в сети, это контентные.

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. Их размещение: сайты, социальные сети, блоги, торренты, видеохостинги, фактически все, что сейчас существует в Интернете. Материал может прийти от незнакомца по почте в виде спама или сообщения.

Негативные контенты делятся:

1. Незаконные: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным), азартные игры и т.д.. Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

2. Неэтичные, противоречащие принятым в обществе нормам морали и социальным нормам: агрессивные онлайн-игры, азартные игры, нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

3. Вредоносные. Такой контент может нанести прямой вред психическому и физическому здоровью детей и подростков: пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей).

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. Более 40% детей в России сталкиваются с изображениями сексуального характера в интернете или других источниках. И каждый шестой из этих детей видит сексуальные изображения ежедневно или почти ежедневно, каждый пятый – систематически: 1-2 раза в неделю. В странах Евросоюза эти цифры в среднем практически в два раза меньше. Данные исследования по России также показали , что младшие дети сталкиваются с сексуальным контентом реже, но при этом испытывают гораздо больший стресс: 40% детей 9-10 лет, имевшие опыт столкновения с изображениями сексуального характера, указали, что были сильно или очень сильно расстроены этим. Данные однозначно показывают, что Интернет в России по сравнению с телевизором, журналами и книгами лидирует в сексуальном просвещении подрастающих поколений. Причем большинство школьников сталкивается с сексуальным контентом случайно (во всплывающих окнах).

Что может расстроить подростков в сети? Многие дети называли агрессивные видео и фото, сайты, на которых обсуждаются различные способы насилия по отношению к другим и к себе, пропагандируется нездоровый образ жизни, анорексия, наркотики, способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, а также сайты, на которых описываются способы самоубийства. Исследования показывают, что около половины детей не умеют оценивать сайты с точки зрения достоверности информации, чуть меньше половины не умеют удалять историю своих действий на компьютере и блокировать спам.

Уважаемые родители! Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Почти каждый интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика интернет-браузеров можно найти нужную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, что их дети могут просматривать в Интернете, отсекать «плохие» сайты, содержащие нежелательную информацию, в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался Интернетом, устанавливать ограничения пользования компьютером и Интернетом по времени. Родительский контроль можно также

устанавливать непосредственно с помощью операционной системы, антивирусных программ, специальных программ.

Уважаемые родители! Знайте, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые легко можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого безопасного поиска, которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

Уважаемые родители! Создайте на компьютере несколько учетных записей, чтобы каждый пользователь мог входить в компьютер (систему) независимо и иметь собственный уникальный профиль. В таком случае ребенок будет входить в систему только под своим логином и паролем, не имея административных прав на контроль системных настроек, установку программ. Учетная запись администратора должна быть у родителя. Тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Для работы в Интернете необходимо создавать надежные пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения владельца. Напомните вашему ребенку, что нельзя сообщать этот пароль друзьям, в противном случае пароль должен быть изменен.

Уважаемые родители! Поддерживайте доверительные отношения с ребенком, чтобы всегда быть в курсе, с какой информацией он сталкивается в сети. Попав случайно на опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра. Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред такой информации. Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с вами.

Уважаемые родители! Объясните детям, что далеко не всё, что они могут прочесть или увидеть в Сети, – правда. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность в оформлении информации, актуальность данных. Уважаемые родители! Помните, что невозможно всегда находиться рядом с детьми и постоянно их

контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог – гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка контента.

Риски-минусы негативных контентов.

Мобильные телефоны:

♣ Систематическиосуществлять анонимные звонки и сообщать негативные сообщения (угрозы, запугивания, оскорбления).

♣ Делать компрометирующее видео и фото, публиковать их в Интернете (например, Happy Slapping) Instant Messenger(IM):

♣ Рассылать подлые сообщения, картинки или видео

♣ Использовать другой аккаунт, чтобы писать негативные сообщения людям из контакт-листа

Чат:

♣ Отправлять анонимные угрозы или оскорбления.

♣ Создание групп, в которых намеренно игнорируются определенные люди. Выстраивание фальшивых дружеских или родственных отношений (чтобы узнать личную, интимную информацию).

Возможные последствия:

распространение слухов, психологический террор. E-Mail:

♣ Рассылать злые и негативные сообщения.

♣ Рассылать непристойные материалы (видео, картинки или компьютерные вирусы).

♣ Взлом другого аккаунта для использования личного E-Maila, для рассылки различной информации ,для его удаления.

Веб-камера:

♣ Непристойное видео снимать и рассылать.

♣ Убеждать или принуждать молодых людей к непристойным действиям.

♣ Публиковать в Интернете личные фото и видео материалы после расставания, чтобы опозорить экс-друга/экс-подругу

Социальные сети:

♣ Писать обидные комментарии к фотографиям, к видео, на стене пользователя, в сообществах.

♣ Распространять непристойное видео и фото.

♣ Взлом чужого аккаунта, редактирование его с целью очернить другого человека (например, рассылка сообщений с этого аккаунта, дополнение лживой информации).

♣ Намеренное создание группы, для выражения ненависти и травли определенного человека.

♣ Создание фальшивого профиля для третирования другого человека.

Видео-порталы:

♣ Непристойное, компрометирующее, позорящее другого человека видео публиковать в Интернете.

Система управления обучением:

♣ Писать непристойные новости

Игровые порталы, виртуальные миры:

♣ Опытные игроки заведомо выбирают себе слабых соперников и убивают их персонажей.

♣ Намеренное удаление игрока из группы или игровых событий.