БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ: 10 ВАЖНЫХ СОВЕТОВ ДЛЯ РОДИТЕЛЕЙ

03.04.2020

Как обеспечить безопасность детей в Интернете? Этим вопросом озадачены практически все современные родители. Ведь держаться подальше от Интернета или, точнее, от информации из Интернета, в XXI веке практически невозможно. Хотя, если вы приняли осознанное решение отказаться от современного общества, вы можете жить свободно, без влияния извне, как Робинзон Крузо.

В Интернете все, как в жизни: есть польза и вред, есть свет и тьма, есть добро и зло. Выпуская своих детей в самостоятельное путешествие по просторам Интернета, родители должны быть уверены, что дети не получат из Интернета нежелательный контент. Только постоянный родительский контроль может гарантировать безопасность детей в Интернете.

Для начала, мы должны разделить возможные риски и влияние Интернета на жизнь современной семьи на те, которые влияют на общую безопасность и на безопасность детей в Интернете. Прежде чем разобраться с этим, мы должны выяснить, какие темы и сайты интересуют наших детей, а затем определиться, как контролировать или ограничивать посещение сайтов, которые не соответствуют их возрасту и уровню воспитания. Согласитесь, вряд ли можно рассчитывать на то, что наши дети настолько хорошо воспитаны, что сами решат, что хорошо, что плохо, ведь детское любопытство и любознательность, данные им природой, никто не отменял.

0 важных советов родителям для того, чтобы обеспечить безопасность детей в Интернете

#1 Будьте в курсе интересов своих детей

Конечно, в первую очередь, мы говорим о благополучных семьям, в которых существуют доверительные отношения между родителями и детьми. Обычно, такие родители находят время общаться с ребенком, обсуждать его интересы и потребности, в том числе, связанные с выходом в сеть Интернет. Как искать нужную информацию, как выбирать игры и как в них играть, как общаться в сети Интернет с другими людьми — эти и многие другие темы, влияющие на безопасность детей в Интернете, должны быть темой совместных обсуждений. При этом, конечно, обсуждать некоторые «непростые» вопросы и темы нужно очень осторожно и деликатно. Иногда неправильная формулировка может смутить ребенка, он замкнется и предпочтет скрыть важную для родителей информацию о сфере своих интересов в Интернете.

Возможно, вам будет интересно мнение великого Стива Джобса, создателя Айфона. В его семье, для всех его четверых детей, существовал строгий порядок пользования Интернетом. Никаких мобильных телефонов за ужином, никаких гаджетов в ночное время и в выходные дни. Таким образом: правило от Стива Джобса звучит так: родители лучше знают, на что дети должны тратить свое свободное время и сколько этого времени можно отвести на Интернет.

Давайте не будем забывать, что некоторым, даже очень хорошим родителям, трудно, иногда даже невозможно, поспевать за развитием своих собственных детей. Известно множество случаев, когда родители либо совсем не понимают, либо понимают очень плохо все то, что их дети делают в Интернете. Иногда родители так много работают, так заняты, что просто не имеют времени и возможности разбираться с новшествами Интернета, тем более, чему то учить детей или направлять их интерес в нужное русло. Они просто надеются, что все будет хорошо. Ситуация усложняется в том случае, когда родители ошибочно считают, что они имеют достаточный контроль над использованием программного обеспечения для фильтрации вредного контента и могут блокировать определенные веб-сайты. Проблема состоит в том, что информации так много, что можно с уверенностью предположить, что некоторые фильтры, если не все, могут быть обойдены. Следовательно, недостаточный родительский контроль очень сильно влияет на безопасность детей в Интернете.

Итак, первый совет достаточно прост: его нетрудно понять и легко реализовать. Оставайтесь на связи со своими детьми, находите время для общения, учитесь у них и будьте в курсе обновлений, будьте открыты к их вопросам и вкладывайте средства в ПО , создающее безопасность детей в Интернете. Эти ваши затраты времени и финансов окупятся благополучием ваших детей в настоящем времени и в будущем.

#2 Знайте инструменты, риски, правила и подходы

Интернет вошел в нашу жизнь и обратной дороги нет. Чем раньше вы подключитесь к решению проблем и вопросов, тем больше шансов на успех.

Так уж выходит, что зачастую дети осваивают современные технологии быстрее, чем их родители. Они находят новую информацию везде: в школе, в театре, в кафе, на днях рождения друзей, дома и на улице. Неважно, используется ли Интернет для исследовательских проектов в школе, для общения с учителями и другими детьми или для досуга: просмотра фильмов или интерактивных игр.

В большинстве случаев огромное количество общедоступного контента нежелательно для ребенка. Причем, ребенок получает его случайным образом, проявив элементарное любопытство и, например, нажав на всплывающее окно видео YouTube. Самая большая проблема может возникнуть, когда ваш ребенок столкнется со злоумышленниками или мошенниками, которых немало в сети Интернет. Например, киберзапугивание или кибертравля, в том числе детей, стали очень распространенным явлением современной жизни. Это — еще один повод для родителей задуматься о том, как обеспечить безопасность детей в Интернете. Необходимо уяснить всем: и взрослым и детям, насколько важна анонимность в Интернете.

Онлайн-злоумышленники известны тем, что, обычно, они выдают себя за другого человека или даже ребенка, охотно используя программное обеспечение и веб-сайты, на которых взаимодействуют дети. Злоумышленник может изображать из себя ребенка или подростка, который хочет завести нового друга. Их злой умысел состоит в том, чтобы получить как можно больше информации от ребенка (личную информацию, адрес, номер телефона и т. д.). Именно поэтому наш первый совет имеет первостепенное значение — родители должны быть в курсе того, что их дети видят и слышат в Интернете, с кем они общаются и что рассказывают о себе. Используйте свою привилегию родителей для создания доверительных отношений с детьми, регулярно общайтесь с ними, не упускайте их из виду.

\* Закон о защите конфиденциальности детей в Интернете (COPPA) гарантирует безопасность детей в Интернете

Еще в 2000 году в США был принят закон «О защите конфиденциальности детей в Интернете» — Children’s Online Privacy Protection Act (COPPA). Он запрещает запрашивать и хранить личные данные детей, младше 13 лет, без официального на то согласия их родителей или опекунов.

Закон COPPA требует, чтобы веб-сайты разъясняли свою политику конфиденциальности, запрашивали возраст пользователя и, после идентификации ребенка младше 13 лет, в обязательном порядке получали согласие родителей на получение и/или использования личной информации ребенка (имя, адрес, номер телефона, номер социального страхования). В 2013 году в закон были введены дополнительные ужесточающие поправки. В настоящее время сайты не могут использовать виртуальное имя ребенка, его фото и видео, запись его голоса, а также информацию о геолокации, IP-адресе, номере процессора или серийном номере устройства, осуществляющего доступ в сеть Интернет.

Согласно этому закону сайты не имеют права запрашивать с ребенка информации больше, чем это необходимо, например, для онлайн-игры или участия в конкурсе. За нарушение положений закона сайтам грозит внушительный штраф. Этот закон создан в помощь американским родителям специально для того, чтобы обеспечить безопасность детей в Интернете.

#3 Используйте инструменты онлайн-защиты

Использование доступных и известных онлайн-инструментов индивидуальной киберзащиты позволяет родителям в определенной степени контролировать доступ детей к неподходящим материалам для взрослых и помогает защитить их детей от интернет-злоумышленников. Многие поставщики интернет-услуг предоставляют опцию родительского контроля. Родителям также рекомендуется использовать программы и/или специально разработанное программное обеспечение, которое помогает блокировать доступ к определенным сайтам и ограничивает отправку личной информации в сеть Интернет. Многие родители склонны прибегать к использованию возможностей программирования для мониторинга и отслеживания онлайн-активности своих детей.

Объясняйте детям основные правила кибербезопасности и напоминайте им о них каждый раз, когда ваш ребенок приступает к онлайн-игре.

Итак, что нужно внушить своим детям:

Никогда не передавайте основную личную информацию (адрес, номер телефона или название школы или местоположение);

Прибегайте к использованию только псевдонима и никогда никому не сообщайте пароли;

Никогда не соглашайтесь и даже не обещайте встретиться лично с кем-то, с кем вы познакомились в Интернете, без ведома родителей, без из одобрения и/или присутствия.

Никогда не отвечайте на угрожающее электронное письмо, сообщение, сообщение или текст.

Обязательно информируйте родителя или любого другого близкого родственника или взрослого, которому доверяете, обо всех без исключения связях или разговорах, которые были пугающими или вредными.

Несколько очень полезных советов для обеспечения родительского контроля и надзора, создающего безопасность детей в Интернете:

* Совместное времяпрепровождение в Интернете побудит ваших детей обращаться к вам с любыми вопросами и дилеммами, но, что более важно, позволит вам регулярно обучать их правильному и безопасному поведению в Интернете;
* Здравый смысл и логика подсказывают нам — расположение компьютера, которым пользуется ваш ребенок в зоне общего доступа, в зоне видимости взрослых, позволяет родителям контролировать время пользования устройством, а также сферу онлайн-интересов ребенка. Может быть, такое расположение компьютера не очень нравится всей семье, но это все же лучше, и, главное, безопаснее, чем установка устройства в детской комнате, за закрытой дверью. Этот совет также актуален для любого другого устройства, имеющего доступ к Интернету. Главный совет — не оставляйте детей наедине с Интернетом без должного присмотра взрослыми членами семьи и без возможности визуального контроля контента;
* Используйте закладки, чтобы позволить вашим детям иметь простой и легкий доступ к любимым сайтам;
* Если дети часто самостоятельно посещают игровые сайты или некоторые образовательные сайты, отключите функцию покупки и регулярно проверяйте счета вашей кредитной карты и телефона на предмет неизвестных расходов по счету;
* Проанализируйте все варианты и решения, которые предлагаются школой, послешкольным досугом, семьями друзей или любыми другими местами, где ваши ваши дети имеют доступ к Интернету без вашего присмотра;
* Будьте внимательны, моментально реагируйте на любое изменение поведения ваших детей, выходите на разговор о том, что они видели и слышали в Интернете, что их удивило или напугало;
* Будьте бдительны в отношении любых признаков, которые могут указывать на то, что ваш ребенок подвергается нападению со стороны онлайн-злоумышленника, найдите ответы на следующие типы вопросов:

o Проводят ли ребенок слишком много времени в Интернете, особенно ночью?

o Получает ли ребенок звонки по телефону от людей, которых вы не знаете?

o Не приходят ли по почте нежданные подарки?

o Часто ли ваш ребенок моментально выключает компьютер или звук, когда вы входите в комнату?

o Не заметили вы заметили отчужденности в отношениях с ребенком и/или нежелание говорить о его онлайн-деятельности?

Но что делать, когда дети становятся старше?

Родители уже не могут поддерживать тот же уровень контроля и надзора, что практиковали прежде, дети все чаще находятся за пределами досягаемости взрослых.

Естественно, с возрастом детям хочется получить больше конфиденциальности и независимости. Это ответственный момент для родителей. Нужно найти способ и возможность поговорить с ребенком, чтобы предостеречь от пользования теми сайтами и приложениями, которые не подходят ему по возрасту и могут ухудшить безопасность детей в Интернете.

Предупредите своих детей, если вы не сделали этого раньше, о рисках и угрозах интернет контактов, особенно, если речь идет о людях, которых дети раньше не знали. Объясните ребенку, что в виртуальном мире Интернета все не совсем так, как кажется на первый взгляд, и в Интернете людям много проще солгать и обмануть другого, действительно много проще, чем в реальной жизни, когда приходится смотреть глаза в глаза.

Объясните ребенку необходимость применения паролей для защиты личных данных от кражи.

#4 Поощряйте критическое мышление

Если бы все, что мы видим в виртуальном мире, было правдой, мы все были бы летающими волшебниками, всемирно известными новаторами или даже имели бы возможность размножить себя в зависимости от того, сколько профилей мы будем использовать в течение дня.

Заложите долю здоровой критики и неоспоримой логики, здравого смысла и взаимного уважение к мнению другого в ваши разговоры с детьми, но не забывайте об осторожности и такте.

Научите ваших детей распознавать и блокировать нежелательные контакты, возникающие по телефону, электронной почте, в текстовых сообщениях, в социальных сетях или онлайн-играх. Объясните своим детям, что они должны понимать, что то, чем они делятся в сети Интернет, могут увидеть и прочитать совершенно другие люди, те, о существовании которых дети даже не подозревали.

Вы также можете рассказать детям о пользе цифрового следа, который может сохраниться в Интернете вечно. Хороший цифровой след может сослужить добрую службу в будущем, когда дети станут взрослыми. Он будет свидетельствовать о их талантах, достижениях и творческом потенциале.

#5 Настройте свой Интернет так, чтобы обеспечить безопасность детей в Интернете

Мы уже упоминали об использовании фильтров и мониторинге взрослыми использования Интернета детьми. Вы также можете рассмотреть другую возможность — включить безопасный поиск Google на всех устройствах, которые использует ваша семья.

Что вы можете сделать в самом браузере, так это включить родительский контроль в таких службах потоковой передачи, как YouTube, Netflix и AppleTV, а также установить программное обеспечение, которое фильтрует контент или позволяет выбирать, в какое время устройства можно использовать, а в какое – нельзя. Это действие аналогично правилу Стива Джобса об ограничении времени, проведенного нашими детьми в виртуальном мире.

Используйте в своем браузере уже установленные опции, такие как история поиска, узнайте их адреса электронной почты и пароли, чтобы вы могли отслеживать активность. Многие устройства используют облачное хранилище, например Google Drive или Apple iCloud, для хранения таких данных, как документы, фотографии или видео. Доступ к ним также можно контролировать.

И последнее, но не менее важное, ознакомьте детей с функциями GPS и регистрации, поскольку именно они определяют местонахождение вашего ребенка, когда те находятся на улице, их лучше ограничить или навсегда отключить.

#6 Учитывайте риски пользования социальными сетями

Ах, эти социальные сети! Ну как же мы могли раньше обходиться без них? Instagram, Twitter, Facebook, В Контакте, Одноклассники и многие другие соцсети с похожей функцией — они созданы и функционируют для оперативной связи между людьми.

Да, это правда, иметь друзей и общаться с другими людьми очень важно для детей и молодежи. В наши дни коммуникации могут быть разными и для разных целей: для поддержания связи с семьей, для ведения блога в Instagram… Многие используют WhatsApp, Snapchat или Viber для общения с друзьями. Конечно, приложений, которые включают моментальный обмен сообщениями между людьми, очень много, но все они представляют определенную степень опасности, особенно в ситуациях, когда дети обмениваются сообщениями с людьми, которых они не знают в реальной жизни и которым не стоит доверять.

Опять же, используйте здравый смысл, логику, предупреждайте детей о том, что сообщения и фотографии, которыми люди обмениваются, могут быть просмотрены и получены не теми, кому адресованы, но совсем другими людьми. Научите их использовать и настраивать параметры конфиденциальности, чтобы их профиль могли видеть только знакомые, и почаще сами проверяйте эти параметры.

Научите детей, как сообщать о злоупотреблениях или недопустимом контенте в службу социальных сетей или другое агентство, особенно когда речь идет о недопустимом контенте. Убедитесь, что дети и подростки понимают риски, связанные с отправкой или пересылкой сексуальных текстов, изображений или видеороликов (по признаку пола), и вред, который это может причинить им и другим.

Правда в том, что, нравится нам это или не нравится, но дети должны это знать. Им нужно учитывать ваши взгляды на вещи и вашу точку зрения, а также их аргументированное обоснование. Это обеспечит безопасность детей в Интернете и придаст уверенности родителям в том, что, даже без родительского контроля, дети не наделают катастрофических ошибок. Родителям необходимо объяснить своему ребенку, что отправка сексуальных или обнаженных фотографий людей моложе 18 лет, как своих, так и чужих, может быть классифицирована как хранение и распространении детской порнографии. А вот это уже будет иметь более серьезные последствия.