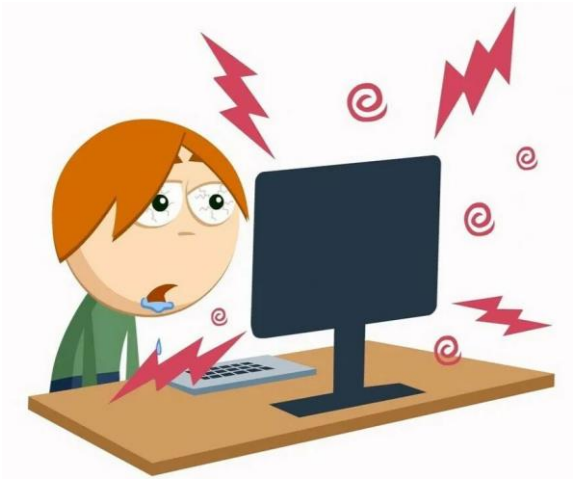
БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ: КАК ЗАЩИТИТЬ СВОЕГО РЕБЕНКА В СЕТИ

В интернете можно обнаружить практически любую информацию и любые изображения. Поэтому родители должны быть уверены, что их дети не столкнутся в Сети с нежелательными людьми, не соответствующим возрасту или травмирующим контентом, или вредоносным ПО. Знание нескольких простых правил безопасности поможет защитить ваших детей в интернете.

Интернет стал для многих людей давно привычным пространством. Те, кто постарше, стали свидетелями перехода от телефонных модемов к кабельным сетям и широкополосному доступу и наблюдали, как мобильные технологии захватывали мир. А наши дети с момента рождения оказываются в мире, оснащенном интернетом: в школе и дома, во время игры или общения со сверстниками они постоянно взаимодействуют с интернетом. И это не может не вызывать тревогу у внимательных родителей.

Почему необходимо защищать детей в интернете:

Родители постоянно слышат о том, как важно защищать детей в интернете. Новостные ленты богаты историями о детях, которые столкнулись с интернет-хищниками. А случаи, рассказанные другими родителями, и предупреждения от местных правоохранительных органов еще больше пугают людей и заставляют их вообще лишать ребенка доступа в Сеть.



При этом статистические данные, приведенные на сайте NetSmartz (онлайн-ресурс, созданный Национальным центром по делам без вести пропавших и эксплуатируемых детей США) свидетельствуют, что сегодня дети проводят больше времени в Сети, чем когда-либо ранее. 93% детей в возрасте от 12 до 17 лет имеют доступ к интернету. 75% детей из этой же возрастной группы пользуются мобильными телефонами. 73% подростков имеют профили в социальных сетях, таких как Facebook, и почти половина из них размещает там свои фотографии.

Какие опасности поджидают детей в интернете:

Поскольку дети используют компьютеры и подключенные к Сети устройства все чаще (для работы, игры или выполнения школьных заданий), родителям становится все труднее защитить ребенка от многочисленных угроз в интернете.

Вот какие опасности могут поджидать ребенка в Сети.

Нежелательные контакты, в том числе:

- интернет-хищники, которые могут встретиться, например, в социальных сетях или игровых чатах;
- кибербуллеры – как виртуальные, так и реальные;
- мошенники, которые с помощью фишинга выманивают у детей конфиденциальную информацию о них самих или их родителях.

Травмирующий или нелегальный контент, в том числе:

- откровенный контент сексуального характера, в частности порнографические изображения и видео;
- контент, содержащий сцены насилия или жестокости;
- неприличный или несоответствующий возрасту контент, например, нецензурная брань или сцены потребления наркотиков и алкоголя;
- загрузка пиратских копий, в том числе музыки или видеофайлов.

Угрозы компьютерной безопасности, в том числе:

- drive-by («попутная») загрузка – когда ваш ребенок просто заходит на какой-либо сайт, и на компьютер автоматически устанавливается вредоносное ПО;
- заражение вредоносными программами, например, через пиринговые файлообменники, ссылки или вложения, в результате чего посторонние люди могут получить доступ к компьютеру ребенка;
- нежелательная реклама, всплывающие окна, рекламное и шпионское ПО, которое часто устанавливается автоматически во время загрузки бесплатных или условно бесплатных программ.

Безопасность детей в интернете вызывает серьезную озабоченность, учитывая, что дети во многих отношениях более продвинуты в вопросах онлайн-технологий, чем их родители. К счастью, вопросам семейной безопасности в интернете сегодня начали уделять гораздо больше внимания.

Что можно сделать для защиты детей в интернете:

Многих родителей пугает вопрос **обеспечения безопасности ребенка в интернете**: они полагают, что родительский контроль требует обширных технических знаний.

Но благодаря простым в использовании защитным решениям в области интернет-безопасности, практически любой родитель может защитить своего ребенка от нежелательного контента или не допустить скачивания вредоносных программ.

Как контролировать доступ детей к интернету и управлять им

Крайне важно, чтобы родители могли управлять доступом ребенка в Сеть. Есть два способа такого управления.

1. Программы родительского контроля. Они часто включены в пакет решений для интернет-безопасности и позволяют следить за тем, сколько времени ребенок проводит в Сети.

2. Антивирусное ПО. Оно помогает справиться с вирусами и программами-шпионами, попадающими на компьютер с сайтов, куда случайно зашел ваш ребенок.

Функции родительского контроля позволяют полностью управлять взаимодействием ребенка с интернетом, в том числе определять количество времени, которое он может проводить в Сети, и списками приложений и веб-сайтов, которые ему разрешено посещать. Любая попытка ребенка войти в запрещенную программу пресекается и заносится в специальный журнал.

Использование более продвинутых настроек позволяет ограничить переписку ребенка с отдельными контактами в социальных сетях, запретить передачу личной информации и даже установить блок на отдельные слова и фразы в исходящих сообщениях.

Качественные программы для родительского контроля предоставляют родителям рычаги воздействия: каждый пользователь без проблем может устанавливать требуемые ему ограничения. Однако при этом нужно не забывать выходить из собственного профиля по окончании работы на компьютере, иначе все ваши усилия будут сведены на нет.

Защита от вирусов также имеет огромное значение для семейной онлайн-безопасности. Веб-сайты, которые кажутся безобидными, на самом деле могут содержать вредоносный код. В других случаях с такого сайта ребенок может быть перенаправлен на поддельный сайт, который выглядит так же, как и настоящий, но в действительности заражен клавиатурным шпионом или вирусом.

Чтобы убедиться, что персональные данные вашего ребенка не передаются злоумышленникам, запланируйте регулярную автоматическую проверку компьютера на вирусы и проводите полную проверку системы раз в месяц. Так вы будете уверены, что на вашем жестком диске не поселился незваный гость.

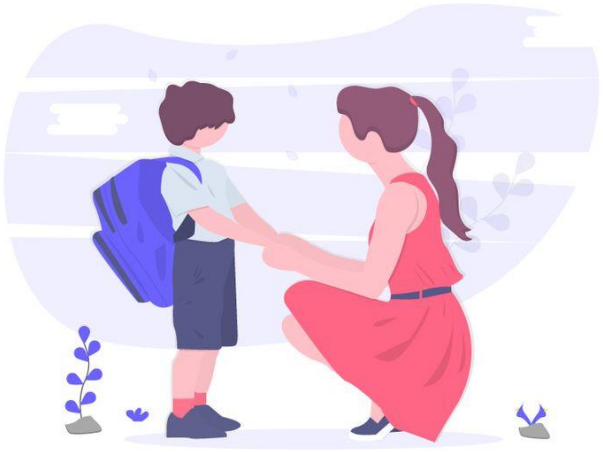
Доверяйте своему ребенку и уважайте его

Ребенку нужна определенная степень свободы, чтобы расти и развиваться самостоятельно. Деспотичный родительский контроль с этим никак не согласуется, и ребенок может начать бунтовать.

В результате родители получат войну на двух фронтах:

1. пытаясь ограничить использование интернета ребенком;
2. сталкиваясь со стремлением ребенка получить бóльшую независимость.

Чтобы не проиграть сражение, надо разбираться в технических аспектах онлайн-контроля и трезво оценивать способность детей обходить неэффективные меры защиты.



Дети вступают в мир планшетов и смартфонов с самого рождения и в интернете чувствуют себя совершенно комфортно, в отличие от многих взрослых. Однако этот комфорт часто оборачивается неспособностью оценить потенциальные риски. Что нужно понимать родителям: использование инструментов интернет-безопасности не должно обернуться неуважением к вашему ребенку. Безопасность ребенка в интернете начинается с использования действенных и гибких инструментов родительского контроля и дополняется надежным антивирусным ПО. Эта комбинация работает еще лучше, если родители уважают права и свободы своих технически продвинутых детей. С помощью правильных инструментов и правильного отношения можно избежать многих проблем, поджидающих ребенка в Сети.

Как выбрать самое надежное защитное ПО для дома:

Выбирая ПО для родительского контроля, необходимо убедиться, что оно осуществляет комплексную защиту от интернет-угроз.

Инструменты родительского контроля – это лишь часть защиты вашей семьи от опасностей, подстерегающих в Сети. Защита детей в интернете должна включать следующее:

- блокировку нежелательного контента;
- защиту устройств от вирусов, вредоносных программ, спама и мобильных угроз.

Чтобы создать надежный страховочный барьер, защитное ПО должно решать обе эти задачи.

К счастью, многие современные решения интернет-безопасности обеспечивают комплексную защиту от всех онлайн-угроз из единого центрального узла.

На рынке представлено множество защитных продуктов, поэтому выбор правильного решения может показаться крайне сложной задачей. К счастью, можно протестировать эти продукты, установив бесплатную пробную версию. Во время

тестового периода вы можете оценить программу и убедиться, что она подходит для нужд вашей семьи.

Что нужно знать детям о безопасности в интернете:

Если вы объясните детям, с какими рисками они могут столкнуться в Сети, это будет еще один важный шаг к тому, чтобы сделать их общение с интернетом безопасным и увлекательным. Но обеспечивать их безопасность на этой виртуальной игровой площадке может быть непростой задачей. Ведь рядом нет учителей, которые бы следили за ними, да и вы не можете контролировать их каждую минуту.

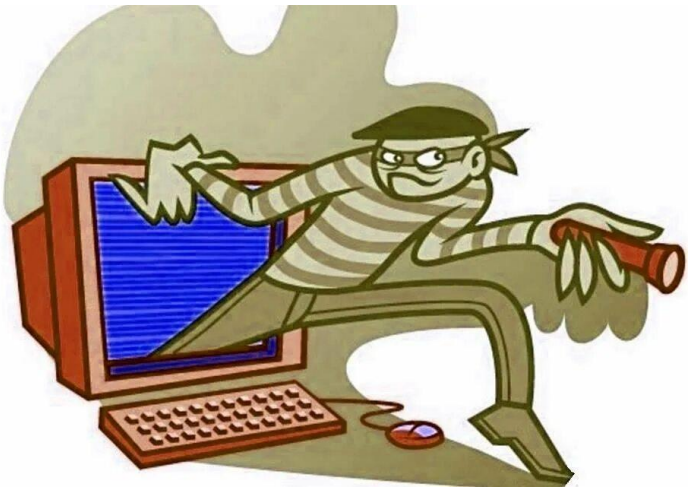
Так как же защитить детей в интернете? Давайте разберемся, что нужно объяснить детям, чтобы уберечь их от повседневных угроз.

1. Нельзя вступать в общение с незнакомцами

Играя в онлайн-игры с друзьями или общаясь в социальных сетях, дети постоянно вступают в контакт с посторонними людьми.

Но в цепочках комментариев, чатах и мессенджерах их могут поджидать киберпреступники. Они прячутся за аватарами, пытаясь обманом вынудить детей раскрыть личную информацию, которая потом может быть использована для кражи идентификационных данных и денег. С помощью фишинга мошенники атакуют самые уязвимые группы, например, детей и пенсионеров.

Что должен знать ваш ребенок? Он должен знать, что люди в интернете могут оказаться совсем не теми, за кого себя выдают. Даже если кто-то выглядит, говорит и ведет себя как ровесник, это может оказаться неправдой. Поэтому ребенку следует быть осторожным и не сообщать виртуальным друзьям никакую личную информацию, в том числе свой возраст, местоположение, логины и пароли и даже дома ли сейчас его родители.



Как вы можете помочь своему ребенку? Разрешайте ему играть только в хорошо известные игры и посещать только доверенные социальные платформы. Но даже в этом случае вам будет сложно обеспечить его безопасность, если вы не знаете, с кем и о чем он разговаривает онлайн. Комплексные решения в области интернет-безопасности, такие как Kaspersky Premium, могут в этом помочь. Они не позволят ребенку отправлять через чаты и мессенджеры личную информацию, например, реквизиты банковского счета, имена и адреса.

Вдобавок в подобных чатах обитают не только киберпреступники. К сожалению, как и в реальной жизни, в Сети ребенок может подвергнуться буллингу.

2. Блокируйте кибербуллеров и сообщайте о них

Некоторые люди регистрируются на игровых сайтах и в соцсетях специально для того, чтобы преследовать и травить остальных участников. Их называют кибербуллерами.

Контролировать и предотвращать кибербуллинг сложно. Как правило, модераторы онлайн-игр пытаются блокировать таких игроков, но при большом количестве участников невозможно уследить за каждым. В социальных сетях сделать это тоже непросто, поскольку каждая платформа имеет собственные правила реагирования на кибербуллинг. Даже определение травли может быть различным на разных платформах.

Что должен знать ваш ребенок? Если чьи-либо действия кажутся ему агрессивными или вызывают дискомфорт, ему следует сообщить вам об этом. По возможности вы или ваш ребенок должны зафиксировать нежелательное поведение и сообщить о нем в службу поддержки. Главное – убедитесь в том, что ребенок больше не подвергается агрессии. Если необходимо, служба поддержки может заблокировать агрессора. Иногда травля в интернете является продолжением травли в реальной жизни. В таком случае необходимо дополнительное вмешательство.

Как вы можете помочь своему ребенку? И здесь функции родительского контроля в защитном решении помогут обезопасить ребенка от травли на онлайн-площадке. Защитное ПО следит за тем, с кем общается ребенок в Сети, и дает родителям возможность заблокировать любые нежелательные контакты. Можно настроить отправку уведомлений, если в онлайн-переписке ребенка появляются определенные слова.

Но даже с такой защитой все же невозможно следить за ребенком 24 часа в сутки. Безобидные на первый взгляд сайты могут содержать вредоносные ссылки, способные поставить под угрозу безопасность вашей домашней сети.

3. Из-за некоторых ссылок, загрузок и веб-сайтов компьютер может заболеть

Киберпреступники в курсе, что дети часто ищут бесплатные программы, музыку и игры в Сети. А еще они знают, что дети склонны доверять ссылкам и вложениям в электронных письмах больше, чем взрослые.

Что должен знать ваш ребенок? Если перейти по одной из таких ссылок, можно нечаянно загрузить вирус, который поставит под угрозу безопасность не только компьютера, но и всей домашней сети. Ребенок не хотел ничего плохого, он просто нажал на рекламный баннер, а вредоносное ПО уже загружается на компьютер и угрожает его безопасности.

Как вы можете помочь своему ребенку? Лучшая защита – это качественное решение для интернет-безопасности, которое блокирует небезопасные ссылки и проверяет каждую скачиваемую программу на признаки вредоносного ПО. Комплексный защитный продукт, такой как **Kaspersky Total Security**, обеспечит безопасность всех членов семьи и всех компьютерных и мобильных устройств в доме. Вы можете контролировать всю домашнюю сеть с вашего компьютера и настраивать параметры безопасности для каждого устройства по отдельности.

Однако ничто не заменит направляющую роль родителей. Просто разговаривайте с вашими детьми, научите их не нажимать автоматически кнопку «да» и держаться подальше от кибербуллеров или потенциальных киберпреступников. Защитное решение со встроенными инструментами родительского контроля – это лишь дополнение, которое позволяет наблюдать за поведением ребенка в интернете.

4. Все, что попадает в интернет, остается там навсегда

Никакую информацию нельзя удалить из интернета полностью, даже если она не была размещена в публичном доступе. Дети не понимают, что все тексты и фотографии, которыми они делятся в интернете, останутся там навсегда. Нужно объяснить им, что есть много причин, почему информация не исчезает из интернета.

Сама архитектура интернета не предполагает того, что какие-то элементы можно удалить бесследно. После удаления всегда останутся цифровые следы, похожие на хлебные крошки. Люди не задумываются о том, что их персональная информация будет храниться в Сети дольше, чем они планировали. Если ребенок отправляет кому-либо изображение, сообщение или другие данные, этот человек всегда может сохранить их. Устройства вашего ребенка могут прослушиваться с помощью программ-шпионов или атак типа man-in-the-middle («человек посередине»).

Что должен знать ваш ребенок? Нельзя делиться в интернете *никакой информацией*, если ты не готов к тому, что она останется в публичном доступе до конца твоей жизни. И не важно, общается ли ребенок с незнакомцем или с человеком, которого он знает в реальной жизни. Риск всегда остается. Даже исчезающие сообщения в таких приложениях как Snapchat никогда полностью не исчезают из интернета.

Как вы можете помочь своему ребенку? Убедитесь в том, что в случае любой сомнительной ситуации он вам о ней расскажет. Объясните ребенку, что он

обязательно должен посоветоваться с вами, если захочет приобрести приложение или получит сообщение с обещанием бесплатного подарка или письмо с просьбой рассказать подробности о личной жизни. Откровенный разговор может поставить барьер на пути любых нежелательных действий по отношению к вашему ребенку.

Итак, вы сделали все необходимые шаги по установке ПО для интернет-безопасности. Вы уже знакомы с потенциальными интернет-угрозами. Теперь пришло время поговорить с ребенком о кибербезопасности.

6 способов поговорить с ребенком о безопасности в интернете:

Самое главное – говорить с ребенком об онлайн-угрозах на понятном для него языке. Интернет таит в себе реальные риски для детей и подростков, но родители могут научить их принимать осознанные решения, чтобы обеспечить их безопасность.

1. Установите базовые правила

Прежде чем дать ребенку компьютер или мобильное устройство, нужно обсудить с ним, с учетом его возраста, что он может, а что не может делать.

Во-первых, установите временные ограничения на пользование интернетом. Если ребенок не просто проводит время в интернете, а решает с его помощью какую-либо задачу, меньше шансов, что он окажется где-нибудь в нежелательной части Сети.

Объясните ребенку, что он должен спросить разрешения, прежде чем делиться такой информацией, как имена и адреса, или вступать в контакт с виртуальными знакомыми. Ребенок должен сразу же обратиться к вам, если он увидел что-то, что его расстроило или напугало.

Научите ребенка **относиться к другим в Сети так, как он хотел бы, чтобы относились к нему**. Это ценное умение. Сознание анонимности в Сети нередко позволяет говорить жестокие вещи даже тем, кто обычно этого не делает, и дети не исключение. Если ребенок поможет сделать интернет добрее, ему самому будет приятнее там находиться.

2. Поговорите с ребенком о том, как и, главное, зачем вы будете следить за его действиями в Сети

Все дети растут, и однажды ваш ребенок зарегистрируется в соцсетях. Предупредите его сразу, что вы будете следить за его публикациями, и объясните зачем. Даже подростки могут не понимать до конца долговременные последствия своих действий, как и то, что интернет ничего не забывает. Они должны знать, что вы заботитесь о них, стараясь оградить их от беды.

Это сложная эквилибристика – следить за безопасностью вашего ребенка и при этом не дать ему почувствовать, что вы ему не доверяете. Обозначьте границы и обсудите, в каких ситуациях вам может понадобиться перейти эти границы.

Если вы увидите, что ваш способ наблюдения вызывает конфликты, будьте готовы попробовать что-то другое. Напоминайте ребенку, что ваша главная забота – это его безопасность. По мере взросления не бойтесь давать ему больше свободы.

Программные продукты родительского контроля, такие как Kaspersky Safe Kids, предлагают легкое решение для мониторинга и управления онлайн-активностью ваших детей.

3. Говорите с ребенком о том, что происходит в его жизни

Открытость и доверие принципиально важны в отношениях с ребенком вообще и при обеспечении его онлайн-безопасности в частности. Кибербуллинг мало чем отличается от буллинга в реальной жизни. Дети часто не говорят о нем родителям, потому что боятся неприятностей или полагают, что их лишат доступа в интернет.

Дайте понять, что вам интересны все сферы жизни ваших детей. Ребенок должен знать, что он может прийти к вам с любой своей проблемой. Регулярно беседуйте с детьми и внимательно слушайте их – они должны чувствовать, что вам важно и интересно все, что с ними происходит.

4. Научите ребенка действовать самостоятельно

Объясните ребенку, что он может сам активно защищать себя: покажите, как использовать настройки конфиденциальности, функции блокировки и отправки жалоб на тех сайтах, которые он посещает.

Дети постарше могут знать об онлайн-мире больше вас. Попробуйте обратиться к ним за советом, чтобы они сами показали вам функции безопасности на тех сайтах, где они часто бывают.

5. Вовлекайте ребенка в принятие решений

Как и любые беседы родителей с детьми, разговоры об онлайн-безопасности должны быть для ребенка опытом познания, а не скучными нотациями.

Спрашивайте его мнение о том, с чем он сталкивается в интернете и не кажется ли это ему потенциально опасным. Если ребенок не согласен с вами, узнайте почему и будьте готовы аргументировать свою позицию. Даже если ребенку не нравятся ваши правила, он с большей вероятностью будет выполнять их, если участвовал в их выработке.

6. Не забывайте о позитиве

Важно, чтобы у ребенка не сложилось впечатление, что весь интернет – это страшное место, которого стоит избегать любой ценой.

Подготовьте почву для воспитания ответственного поведения онлайн: поговорите о том, как интернет может помочь с учебой и с другими интересами ребенка. Дети следуют примеру родителей, хотя иногда мы этого и не видим. Если вы будете подавать пример ответственного поведения в интернете, это может иметь гораздо более сильный эффект, чем правила и ограничения.

Важные выводы для родителей о защите детей в интернете:

Сегодня дети взрослеют в мире, который киберцентричен. Рано или поздно ребенок познакомится с интернетом и другими цифровыми технологиями – мы не сможем этого избежать. Но мы можем научить его навыкам безопасного поведения в интернете, чтобы минимизировать риски. Родителям нужно выбрать правильную стратегию, и здесь пригодятся наши советы.

Подводя итоги, перечислим самые важные выводы.

- Говорите с детьми о потенциальных опасностях, поджидающих их в интернете.
- По возможности установите компьютер ребенка в общей комнате.
- Постарайтесь сделать так, чтобы компьютером пользовались все члены семьи.
- Приучите детей рассказывать вам, если они встретятся в Сети с чем-то, что их расстроит или причинит им дискомфорт.
- Ограничьте контент, доступ к которому можно получить через компьютер.
- В этом вам помогут многие решения в области интернет-безопасности.
- Например, браузер Internet Explorer имеет функцию ограничения доступа Content Advisor, которая тоже может оказаться полезной.
- Установите правила, которые укажут вашим детям, что они могут и что не могут делать в Сети. Например, вы можете оговорить, разрешено ли им:
- регистрироваться в социальных сетях и на веб-сайтах;
- совершать онлайн-покупки;
- скачивать музыку, видео или программные файлы;
- использовать мессенджеры;
- посещать чаты.
- Если вы разрешаете ребенку пользоваться мессенджерами или заходить в чаты, ему следует объяснить, что общение и переписка с незнакомцами могут быть опасны.
- Загружайте и устанавливайте на все свои устройства свежие обновления и патчи безопасности, как только они появляются. Это касается операционных систем, приложений и другого ПО.
- Установите надежное антивирусное ПО, которое сможет защитить все семейные компьютеры и мобильные устройства от вредоносного ПО и хакеров. Многие защитные решения сочетают антивирусные возможности с продвинутыми

функциями родительского контроля, что облегчает задачу по защите детей в интернете. Вот какие функции должно иметь ваше защитное решение:

- защита от вредоносного ПО;
- фильтрация спама;
- защита от фишинга;
- родительский контроль;
- мониторинг просмотра веб-страниц в режиме реального времени.

Защита детей в Интернете: что могут сделать взрослые?

- Объясните детям и установите четкие правила – какие сайты они не должны посещать.
- Помогите детям выбрать правильное регистрационное имя и пароль, если это необходимо для общения детей посредством программ мгновенного обмена сообщениями или сетевых игр. Убедитесь в том, что они не содержат никакой личной информации.
- Объясните вашим детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.
- Объясните детям, что люди в Интернете не всегда являются теми, за кого они себя выдают. Не позволяйте детям встречаться лично с их «знакомыми» по Интернету без вашего наблюдения.
- Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
- Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.
- Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости.
- Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.
- Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет-дневник, регулярно посещайте его.

Будьте внимательны к вашим детям!

Возрастные особенности детей и Интернет

Ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при пользовании Интернетом. Родителям важно понимать особенности формирования их характера и интересы в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

Более подробную информацию по повышению безопасности детей различного возраста в Интернете см. на веб-сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/children/parentsguide.mspx

Повышение уровня безопасности детей в Интернете при помощи программных средств

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. Пожалуйста, примите необходимые меры, чтобы защитить ваших детей при помощи программных средств. Но помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

- Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам (например, с помощью Internet Explorer®)
- Увеличьте уровень защиты и конфиденциальности:
  - используя возможности Microsoft® Windows XP, создайте отдельные учетные записи для разных пользователей
  - настройте параметры безопасности Internet Explorer®
- Следите за тем, какие сайты посещают ваши дети (например, с помощью Internet Explorer®)
- Напоминайте детям, чтобы они не общались в Интернете с незнакомцами. Помогите им оградить себя от неизвестных контактов (например, с помощью Microsoft Windows Messenger)

Более подробную информацию по повышению безопасности в Интернете с помощью технологических средств см. на веб-сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/children/childrenonline.mspx