

ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

10 правил безопасной работы в Интернете для детей

Прежде чем позволять своим детям выходить в Интернет без вашего контроля, составьте вместе с ними правила, которых они должны будут придерживаться.

Если вы не знаете с чего начать, ознакомьтесь с приведенными ниже советами, которые помогут вам научить детей принципам безопасной работы в Интернете.

1. Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Путешествуйте в Интернете вместе с детьми.
2. Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.
3. Если ваши дети общаются в чатах, пользуются программами мгновенной передачи сообщений, играют в сетевые игры или занимаются в Интернете чем-то другим, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.
4. Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.
5. Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.
6. Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения несколько не изменяются.
7. Добейтесь от детей уважения к собственности других пользователей Интернета. Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.
8. Убедите детей в том, что они не должны встречаться с интернет-друзьями лично. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого они себя выдают.
9. Объясните детям, что верить всему, что они видят или читают в Интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации им следует обратиться за советом к вам.
10. Контролируйте действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают.

Научите детей отличать факты от домыслов

Интернет предоставляет доступ к огромным объемам информации и обеспечивает широчайшие возможности для обучения, но вместе с тем в нем часто встречаются бесполезные и недостоверные сведения.

Публиковать информацию в Интернете может кто угодно, и для оценки её правдивости необходимы навыки критического мышления.

В первую очередь это относится к детям, которые склонны верить всему, что им встречается в Интернете.

Печатные материалы в этом смысле более надежны, потому что редакторы и корректоры тщательно проверяют их, устраняя ошибки, ложные и неточные сведения и т.д. Информация, публикуемая в Интернете, во многих случаях не подвергается никакой проверке.

Объясните детям базовые принципы устройства Интернета и укажите, что любой человек может легко создать свой веб-узел без какого-либо контроля. Научите детей использовать разные источники информации, а также подвергать сомнению и проверять то, что они узнают в Интернете.

Как помочь детям научиться отличать правду от лжи и дезинформации в Интернете

1. Начните учить детей работе в Интернете с малых лет. В наше время даже дошкольники пользуются Интернетом для поиска информации, поэтому детей надо с малых лет учить отличать факты от мнений и распознавать предрассудки, пропаганду и стереотипы.
2. Расспрашивайте детей о том, что они находят в Интернете. Спросите у них, например, каково предназначение того или иного веб-узла. Развлечения? Продажа каких-либо товаров? Есть ли на веб-узле контактная информация автора или раздел с информацией о проекте?
3. Финансирует ли поддержку веб-узла какая-то конкретная компания или человек? Может быть, его поддержка осуществляется на общественных началах? Действительно ли Интернет является лучшим местом поиска определенных сведений?
4. Убедитесь в том, что дети проверяют сведения, найденные в Интернете, по другим источникам. Обнаруженную в Интернете информацию следует проверять по другим веб-узлам и источникам, таким как газеты, журналы и книги. Поощряйте детей обращаться к вам за помощью.
5. Объясните детям, что важно использовать разные источники информации, а не только Интернет. Сводите детей в библиотеку, купите им хорошую энциклопедию на компакт-диске, такую как Microsoft Encarta. Так вы предоставите детям доступ к альтернативным источникам сведений.
6. Обучите детей способам эффективного поиска сведений в Интернете. Благодаря этому они смогут получать надежную качественную информацию.
7. Обсудите с детьми проблемы нетерпимости и расизма. Программные фильтры позволяют блокировать некоторые материалы, разжигающие ненависть.

8. Однако ваши дети должны знать о расизме и событиях в мире, чтобы уметь распознавать проявления нетерпимости.

Четыре действия для повышения безопасности семьи при работе в Интернете

Хотя никакая технология не может заменить участия родителей, программное обеспечение корпорации Microsoft позволяет защитить детей от неприемлемого содержимого несколькими способами.

Ниже приведено несколько советов по защите конфиденциальности и безопасности детей при использовании компьютера.

Действие 1. Решите, на какие веб-узлы ребенку можно заходить, а на какие нельзя.

Имеет смысл проверить некоторые веб-узлы для детей. Обращайте особое внимание на веб-узлы, которые собирают личные данные.

Если вы не согласны с заявлением о конфиденциальности определенного веб-узла или не желаете разглашать какие-либо личные данные о своем ребенке, немного поискав, вы можете найти подобный веб-узел, который не запрашивает никаких сведений.

Заблокируйте неприемлемое содержимое. Одним из лучших видов защиты от неприемлемого содержимого является его блокировка до того, как оно попадет на компьютер. С помощью программного обеспечения корпорации Microsoft это можно сделать несколькими способами.

Родительский контроль в Windows Vista. Как родитель вы принимаете решение о том, какое содержимое является приемлемым для вашего ребенка в зависимости от его возраста, развития и ваших личных убеждений. Система Windows Vista предоставляет широкий спектр мощных средств родительского контроля, помогающих наблюдать за тем, как дети пользуются компьютером, контролировать этот процесс и обеспечивать их безопасность. Дополнительные сведения см. в статье Родительский контроль в Windows Vista.

Служба семейной безопасности Windows Live OneCare. Программное обеспечение, помогающее фильтровать данные с учетом возраста каждого ребенка, чтобы защитить его от содержимого, нежелательного для просмотра. Можно также ограничить поиск, заблокировать или разрешить определенные веб-узлы и наблюдать за тем, чем ваши дети занимаются в Интернете. Кроме того, имеется возможность доступа к рекомендациям по обеспечению безопасной работы ребенка в Интернете и о том, как родителям следует разговаривать с детьми о ненадлежащей работе в Интернете. Дополнительные сведения см. в документе Семейная безопасность Windows Live OneCare (EN).

Родительский контроль для игровой приставки Xbox. Игровая приставка Xbox содержит подобные средства родительского контроля, помогающие ограничить возможность ребенка играть в ненадлежащие игры и просматривать ненадлежащие

DVD-фильмы. Дополнительные сведения об обеспечении безопасности ваших детей при игре по Интернету см. в документе Советы по безопасности, касающиеся детей и игр.

Действие 2. Повысьте уровень безопасности и конфиденциальности.

Помимо блокировки неприемлемого содержимого рекомендуется заблокировать доступ к веб-узлам и загрузку файлов, которые могут представлять угрозу безопасности и конфиденциальности.

Создайте различные учетные записи пользователей. Windows Vista и Windows XP позволяют создавать на компьютере несколько учетных записей. Каждый пользователь может отдельно входить в систему и имеет уникальный профиль с собственными папками "Рабочий стол" и "Мои документы".

Как родитель вы можете назначить себе учетную запись администратора, которая обеспечивает полный контроль над компьютером, а детям предоставить ограниченные учетные записи с ограниченными полномочиями.

Пользователи с ограниченными полномочиями не могут изменять системные параметры либо устанавливать новое оборудование или программное обеспечение, включая большинство игр, программ для воспроизведения файлов мультимедиа и программ для общения по Интернету.

Установите параметры безопасности веб-обозревателя. Вы можете защитить своего ребенка с помощью веб-обозревателя. Обзорщик Internet Explorer позволяет контролировать параметры безопасности и конфиденциальности путем назначения веб-узлам уровней безопасности.

Обзорщик Internet Explorer 6 также позволяет защитить конфиденциальность при работе в Интернете с помощью функций, позволяющих контролировать то, каким образом веб-узлы отслеживают ваши действия.

Действие 3. Следите за тем, какие веб-узлы посещают ваши дети

У родителей не всегда есть возможность лично присутствовать, когда ваши дети работают в Интернете. Однако можно впоследствии проверить, что дети делали в Интернете.

Просматривая список журнала обозревателя Internet Explorer, можно узнать, какие веб-узлы посещали ваши дети. Чтобы просмотреть список журнала, нажмите кнопку "Журнал" на панели инструментов обозревателя.

Щелкните папку, чтобы раскрыть её и просмотреть отдельные страницы, посещенные вашим ребенком на определенном веб-узле.

С помощью средств родительского контроля MSN 9 можно получать по электронной почте еженедельные отчеты с подробными сведениями о работе ребенка в Интернете за последнее время, включая общее время, проведенное в Интернете, веб-узлы, которые ребенок посетил или пытался посетить, адреса электронной почты и

идентификаторы MSN Messenger тех людей, с которыми общался ребенок, а также загруженные файлы.

Действие 4. Напомните детям о том, что им не следует общаться с незнакомцами в Интернете

Общение в режиме реального времени и обмен мгновенными сообщениями — прекрасный способ для детей обсудить свои интересы и найти друзей. Но анонимность Интернета может привести к тому, что ребенок станет жертвой самозванцев и преступников. Чтобы свести угрозу к минимуму, научите детей следующим мерам предосторожности:

- Использовать для своей идентификации только имя или псевдоним.
- Никогда никому не сообщать номер телефона или адрес.
- Никогда никому не отправлять свои фотографии.
- Никогда не соглашаться на встречу со знакомыми по Интернету без сопровождения.

Чтобы защитить своих детей от контактов с незнакомыми людьми при обмене мгновенными сообщениями, настройте программное обеспечение таким образом, чтобы разрешать использовать только проверенные контакты.

Чтобы заблокировать неизвестных лиц в Windows Messenger, выполните следующие действия.

1. Откройте меню Сервис.
2. Выберите пункт Параметры.
3. Выберите вкладку Конфиденциальность.
4. Добавьте известных вам людей в список Разрешить и заблокируйте остальных пользователей.

Список проверенных контактов, помогающий родителям ограничить возможности своих детей по обмену электронной почтой, также является одной из возможностей MSN 9.

Выработка семейных правил пользования Интернетом

Хотя программное обеспечение позволяет защитить вашу семью от неприемлемого интернет-содержимого, оно не может заменить обучение детей ряду основных правил. Поговорите с детьми об угрозах при работе в Интернете и научите их, как действовать в сложной ситуации. Наконец, установите ограничения и обсудите их с детьми. Вместе вы сможете создать комфортную и безопасную среду для работы детей в Интернете.

Двенадцать советов по безопасности при ведении блогов для детей и родителей

Привычка вести блог, или персональный веб-дневник, распространилась со скоростью пожара, особенно среди подростков, которые иногда ведут блоги без ведома родителей или опекунов.

Последние исследования показывают, что сегодня примерно половину всех блогов ведут подростки. При этом двое из трех раскрывают свой возраст, трое из пяти публикуют сведения о месте проживания и контактные данные, а каждый пятый сообщает свое полное имя. Само собой разумеется, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей сети создают блоги, и каждый стремится привлечь как можно больше внимания аудитории. Иногда это приводит к тому, что дети размещают в них такой неуместный материал, как провокационные фотографии себя или своих друзей.

Хотя ведение блога имеет потенциальные преимущества, например улучшение навыков письменной речи и общения, важно обучить детей работе в Интернете и ведению блогов до того, как они начнут это делать — подобно тому, что перед тем, как ездить на машине самостоятельно, необходимо окончить автошколу. Ниже приведены несколько советов для начала.

1. Установите правила работы в Интернете для детей и будьте настойчивы.
2. Просматривайте то, что дети планируют отправить, перед отправкой. По сведениям, которые могут казаться безобидными, например символу школы или фотографии города, можно определить, какую школу посещает автор.
3. Спросите себя (и попросите детей сделать то же самое), чувствуете ли вы себя комфортно, показывая содержимое веб-журнала постороннему. В случае сомнений удалите соответствующие сведения.
4. Оцените качество работы службы веб-журналов и выясните, предлагает ли она личные, защищенные паролем веб-журналы.
5. Сохраните веб-адрес блога своего ребенка и регулярно его просматривайте.
6. Посещайте другие блоги и ищите положительные примеры для подражания для своих детей.

Основные рекомендации для владельцев блогов

Приведенные ниже советы могут помочь детям, заинтересованным в ведении блога, хотя эти советы никоим образом не являются исчерпывающими. В зависимости от потребностей семьи можно дать детям еще несколько советов. Начните с объяснения детям приведенных ниже правил.

1. Никогда не публикуйте никакие личные данные, в том числе фамилию, контактные данные, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей и родственников, имена в системе мгновенного обмена сообщениями, возраст или дату рождения.

2. Никогда не публикуйте провокационные фотографии, свои или чьи-либо ещё, и всегда проверяйте, что публикуемые фотографии не раскрывают каких-либо упомянутых выше сведений. Всегда внимательно рассматривать задний план на фотографиях.

3. Принимать во внимание то, что публикуемая в Интернете информация остается там надолго и Кто угодно может легко распечатать блог или сохранить его на компьютере.

4. Пользоваться только службами веб-журналов с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя (но даже если это так, лучше полагать, что доступ к блогу может получить кто угодно).

5. Не стремиться к соревнованию с другими детьми, ведущими веб-журналы;

6. Вести веб-журналы в положительном ключе и не использовать их для злословия или нападок в адрес других детей.

Повышение уровня безопасности детей при посещении ими веб-узлов социальных сетей

При взгляде на ребенка, делающего домашнее задание за семейным компьютером в гостиной или общающегося и просматривающего страницы в Интернете через сотовый телефон на заднем сиденье машины, может показаться, что он постоянно находится в Сети.

Социальные веб-узлы крайне популярны у подростков и набирают все большую популярность среди детей младшего возраста. Дети используют веб-узлы социальных сетей для общения как с детьми из других частей мира, так и с теми, кого каждый день встречают в школе. На веб-узлах социальных сетей дети выражают свои чувства, а иногда даже ищут сведения о ком-то, кого им довелось повстречать на вечеринке или в школе. Например, после личной встречи ребенок может посетить веб-узел своего нового знакомого, чтобы лучше понять, хочет ли он с ним подружиться.

Сегодня многие дети не видят большой разницы между жизнью в реальном мире и в Интернете. Они посещают как социальные веб-узлы, созданные специально для детей (например, Webkinz или Club Penguin), так и веб-узлы, предназначенные для взрослых (например, Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие). Что бы они ни делали, они должны понимать, что многие такие веб-страницы может увидеть любой человек, имеющий доступ в Интернет.

На этих веб-узлах дети:

- общаются;
- играют в игры;
- размещают свои фотографии и видеоролики и смотрят чужие;
- ведут блоги;

- публикуют данные о себе.

К сожалению, некоторые сведения, размещаемые детьми на своих страницах, могут сделать их объектом фишинг-афер, запугивания и действий интернет-преступников. Ниже описано несколько способов, которые позволяют сделать использование веб-узлов социальных сетей более безопасным для ребенка.

1. Обсуждайте с детьми их опыт использования веб-узлов. Просите детей рассказывать вам, если что-либо, с чем они столкнулись на этих веб-узлах, пугает их или вызывает у них дискомфорт. Ведите себя спокойно и напоминайте детям, что они могут без опасений рассказывать вам обо всем. Объясните, что готовы помочь им разрешить любую ситуацию благоприятным образом.

2. Установите правила пользования Интернетом дома. По мере того как дети начинают самостоятельно пользоваться Интернетом, имеет смысл составить список правил его использования, который бы их устроил. В этих правилах должно быть указано, разрешается ли ребенку посещать веб-узлы социальных сетей и на каких условиях.

3. Убедитесь, что ваши дети следуют ограничениям по возрасту, установленным на веб-узле. Рекомендуемый возраст регистрации на веб-узлах социальных сетей — 13 лет и старше. Если ваши дети младше рекомендуемого возраста, не позволяйте им посещать эти веб-узлы. Помните, что сами службы могут не препятствовать регистрации малолетних детей на веб-узле.

4. Изучите веб-узел сами. Просмотрите сайты, которые собирается посещать ваш ребенок, и убедитесь, что и вы, и ребенок понимаете суть политики конфиденциальности и кодекса поведения. Выясните, отслеживается ли на сайте размещаемое его пользователями содержимое. Кроме того, периодически просматривайте страницу своего ребенка. Другие советы см. в статье [Советы по безопасному ведению блога для родителей и детей](#).

Запретите детям лично встречаться с теми, с кем они общались исключительно в Сети, убедите их общаться только с людьми, которых они знают лично. Дети могут подвергнуться серьезной опасности при личной встрече с людьми, с которыми они общались исключительно в Интернете. Чтобы защитить своих детей от этой опасности, убедите их использовать такие веб-узлы для общения только со своими друзьями, а не с незнакомыми людьми.

Может оказаться недостаточным просто запретить ребенку общаться с незнакомыми людьми, потому что он может не считать незнакомым человека, с которым «познакомился» в Сети:

1. Убедитесь в том, что ваши дети не используют полные имена. Пусть ребенок использует только имя или псевдоним, который не будет привлекать излишнего внимания. Также запретите детям использовать полные имена своих друзей.

2. Контролируйте размещение любых других личных данных в профиле ребенка. Многие веб-узлы социальных сетей позволяют детям входить в общие группы, которые объединяют учащихся одной школы.

3. Внимательно относитесь к ситуациям, когда дети размещают такие данные или другие сведения о себе, с помощью которых можно выяснить их личность (например, эмблему своей школы, фотографию рабочего места или название города, в котором они живут). Излишняя открытость может сделать ребенка объектом запугивания, мошенничества, действий интернет-преступников или кражи личных сведений.

4. Рассмотрите возможность использования веб-узла с ограничением доступа. Некоторые веб-узлы социальных сетей позволяют защищать свою страницу с помощью пароля или реализуют другие методы защиты, разрешая просмотр сведений о детях только тем, кого они знают. Например, служба MSN Spaces позволяет указать, кому разрешается просматривать веб-узел, начиная от всех пользователей Интернета и заканчивая только выбранными людьми.

5. Обращайте внимание на детали фотографий. Объясните ребенку, что по фотографиям можно многое узнать о человеке. Убедите детей не размещать свои фотографии или фотографии друзей с легко узнаваемыми деталями, такими как названия улиц, номера машин или название школы на одежде.

6. Предупредите ребенка, что нельзя показывать свои чувства незнакомым людям. Наверное, вы уже сказали детям, что не следует общаться с незнакомцами в сети. Однако дети используют веб-узлы социальных сетей, чтобы вести дневники и писать стихотворения, в которых часто весьма открыто выражают свои чувства.

7. Объясните детям, что их записи может прочитать кто угодно, у кого есть доступ к Интернету, и что интернет-преступники охотятся на эмоционально ранимых детей.

8. Расскажите детям о запугивании с помощью Интернета. Как только дети достаточно повзрослеют для посещения веб-узлов социальных сетей, расскажите им о практике запугивания в Интернете. Объясните ребенку, что если ему кажется, что его запугивают, следует сказать об этом родителям, учителю или кому-то из взрослых, кому он доверяет. Кроме того, нужно пояснить ребенку, что общаться с другими людьми в Интернете надо так же, как он общался бы с ними вживую. Попросите детей вести себя с другими людьми так же, как они хотели бы, чтобы себя с ними вели другие.

9. Удаление страницы ребенка. Если ребенок отказывается подчиняться установленным вами правилам, призванным его защитить, то после попытки на него повлиять, можно связаться с администрацией веб-узла социальной сети, которую посещает ребенок, и попросить удалить его страницу. Кроме того, можно попробовать воспользоваться средствами фильтрации содержимого в Интернете (такими как семейная безопасность Windows Live OneCare (EN)) в качестве дополнения (но не замены) родительского контроля.

Рекомендации по использованию Интернета детьми с учетом возраста

До 10 лет: высокий уровень защиты

Контролируйте детей и следите за тем, чтобы у них не было доступа к неприемлемым материалам, пока им не исполнится 10 лет.

Средства обеспечения безопасности в Интернете позволяют ограничить доступ к содержимому, веб-узлам и деятельности и активно контролировать использование Интернета детьми.

Для детей в возрасте от 2 до 10 лет Интернет — это отличное место, где они могут играть и учиться.

Использование компьютера детьми в этом возрасте необходимо контролировать. Также можно порекомендовать применять специальные средства, такие как служба семейной безопасности Windows Live OneCare или функция родительского контроля в Windows Vista.

Ниже приведены некоторые советы, помогающие обезопасить использование Интернета детьми 2-10 лет.

1. Налаживать открытое и дружественное общение с детьми никогда не рано. Говорите с ними о компьютерах и не игнорируйте их вопросы и любопытство.
2. Когда дети этого возраста пользуются Интернетом, родители всегда должны быть рядом с ними.
3. Составьте четкие правила использования Интернета.
4. Настаивайте на том, чтобы дети не раскрывали личные сведения, например: свое настоящее имя, адрес, номер телефона или пароли, — людям, с которыми они познакомились в Интернете.
5. Помогите детям придумать псевдонимы, не раскрывающие никаких личных сведений, если на веб-узле будет запрошено имя для персонализации отображаемых материалов.
6. Ознакомьтесь со средствами фильтрации веб-содержимого (например, функция родительского контроля в Windows (EN) или служба семейной безопасности Windows Live OneCare для Windows XP с пакетом обновления 2), которые помогут найти общий язык с детьми и установить родительский контроль.
7. При использовании средств обеспечения безопасности для всей семьи, создайте профили для каждого члена семьи в зависимости от его возраста.
8. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer (EN).
9. Для блокирования всплывающих окон в автономном режиме можно использовать Защитник Windows. Защитник Windows входит в состав системы Windows Vista. Для системы Windows XP с пакетом обновления 2 (SP2) Защитник Windows можно загрузить бесплатно.

Все члены семьи должны показывать пример поведения детям, которые только начинают использовать Интернет.

От 11 до 14 лет: средний уровень защиты

Несмотря на то, что дети этого возраста лучше разбираются в Интернете, имеет смысл следить за тем, чтобы у них не было доступа к неприемлемым материалам.

С помощью средств обеспечения безопасности в Интернете можно ограничить доступ к содержимому и веб-узлам, а также регистрировать в отчете деятельность в Интернете.

Убедитесь, что дети этого возраста понимают, какие личные данные не следует передавать через Интернет.

Дети 11-14 обычно очень восприимчивы. В этом возрасте дети обладают хорошими способностями к выполнению компьютерных команд, использованию мыши и компьютерным играм.

Однако при восприятии сведений из Интернета они во многом зависят от взрослых или старших братьев и сестер.

Родителям, имеющим детей такого возраста, следует контролировать использование компьютера и применять специальные средства, такие как служба семейной безопасности Windows Live OneCare или функция родительского контроля в Windows Vista.

Ниже приведены некоторые советы, помогающие сделать использование Интернета детьми 11-14 лет более безопасным.

1. Поддерживайте открытые, дружеские отношения с детьми. Говорите с ними о компьютерах и не игнорируйте их вопросы и любопытство.
2. Составьте четкие правила использования Интернета.
3. Настаивайте на том, чтобы дети не раскрывали личные сведения, например свое настоящее имя, адрес, номер телефона или пароли, людям, с которыми они познакомились в Интернете.
4. Помогите детям придумать псевдонимы, не раскрывающие никаких личных сведений, если на веб-узле будет запрошено имя для персонализации отображаемых материалов.
5. Создайте профили для каждого члена семьи с помощью средств обеспечения безопасности для всей семьи.
6. Установите средний уровень для параметров безопасности средства обеспечения безопасности семьи, что позволит применить некоторые ограничения к содержимому, посещаемым веб-узлам и действиям пользователей.
7. Установите компьютеры с подключением к Интернету в общих комнатах, где легко наблюдать за детьми.

8. В качестве дополнения к родительскому контролю используйте средства фильтрации веб-содержимого (например, службу семейной безопасности Windows Live OneCare (EN)).

9. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer.

10. Для блокирования всплывающих окон в автономном режиме можно использовать Защитник Windows. Защитник Windows входит в состав системы Windows Vista. Для системы Windows XP с пакетом обновления 2 (SP2) Защитник Windows можно загрузить бесплатно.

11. Попросите детей сообщать вам, если что-то или кто-то в Интернете угрожает им или доставляет неудобства. Ведите себя спокойно и напоминайте детям, что они могут без опасений рассказывать вам обо всем. Поощряйте их за правильное поведение и просите обращаться к вам снова в подобных ситуациях.

От 15 до 18 лет: низкий уровень защиты

Подростки должны иметь практически неограниченный доступ к содержимому, веб-узлам или деятельности в Интернете. Они хорошо разбираются в Интернете, но все равно нуждаются в напоминаниях родителей о соответствующих мерах предосторожности. Родители должны быть готовы помочь подросткам и объяснить, как распознавать неприемлемые сообщения и избегать небезопасные ситуации.

Имеет смысл, чтобы родители напоминали подросткам о том, какие личные сведения не следует передавать через Интернет.

Подростки должны иметь практически неограниченный доступ к содержимому, веб-узлам или деятельности в Интернете. Несмотря на то, что подростки лучше разбираются в Интернете, родители все же должны снабдить их соответствующими рекомендациями по обеспечению безопасности. Родители должны быть готовы помочь детям и объяснить, как распознавать неприемлемые сообщения и избегать небезопасные ситуации.

Может потребоваться напомнить детям о недопустимости передачи личных сведений через Интернет.

Что подростки делают в Интернете

Юноши этого возраста обычно интересуются юмором, играми или другими веб-узлами с мультимедийным содержимым. Девушки более склонны к созданию социальных сетей и участию в них.

Ниже приведены некоторые советы, помогающие обезопасить использование Интернета подростками.

1. Продолжайте поддерживать открытое и дружественное общение с детьми на тему компьютеров. Обсуждайте с ними их действия в Интернете и найденных там друзей так, будто речь идет о событиях и друзьях из реальной жизни.

2. Попросите детей сообщать вам, если что-то или кто-то в Интернете угрожает им или доставляет неудобства. Если детей что-то или кто-то беспокоит в Интернете, им следует сообщить о своих подозрениях родителям.

3. Установите компьютеры с подключением к Интернету в общих комнатах, а не в комнатах детей.

4. В качестве дополнения к родительскому контролю используйте средства фильтрации веб-содержимого (например, функцию родительского контроля в Windows Vista (EN) или службу семейной безопасности Windows Live OneCare (EN)).

5. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer.

Для блокирования всплывающих окон в автономном режиме можно использовать Защитник Windows. Защитник Windows входит в состав системы Windows Vista. Для системы Windows XP с пакетом обновления 2 (SP2) Защитник Windows можно загрузить бесплатно.

6. Узнавайте у детей, какие чаты и доски объявлений они посещают и с кем общаются. Поощряйте общение в отслеживаемых комнатах бесед (чатах) и настаивайте на том, чтобы дети общались только в общих окнах комнат бесед.

7. Не разрешайте детям встречаться с друзьями из Интернета.

8. Объясните детям, что они не должны загружать из Интернета программы, музыку или файлы без вашего разрешения. Обмениваясь файлами и загружая из Интернета текст, изображения и другие материалы, они могут нарушить законы об авторских правах.

9. Расскажите детям о порнографии и других материалах для взрослых в Интернете и направьте их на веб-узлы с грамотными материалами о здоровье и половой жизни.

10. Помогите своим детям защититься от нежелательной почты. Научите их не сообщать в Интернете свои адреса электронной почты, не отвечать на нежелательную почту и пользоваться фильтрами электронной почты.

11. Расскажите детям об ответственном и порядочном поведении в Интернете. Они не должны использовать Интернет для хулиганства, распространения слухов или угроз.

12. Проследите за тем, чтобы дети советовались с вами перед заказом, покупкой или продажей чего-либо в Интернете.

13. Обсудите с детьми азартные игры в Интернете и связанный с ними риск. Напоминайте им, что играть в азартные игры в Интернете запрещено законом.

То, что дети проводят в интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление Сети, полагая, что она — безграничный источник новых знаний. Вскоре выяснилось, что подростки не пользуются интернетом для выполнения домашних заданий или поиска полезной информации. Вместо этого юное поколение общается в чатах и играет в онлайн-игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей; интернет сделал это еще более трудной задачей. Общение в интернете и интерактивные игры настолько затягивают детей, что они теряют ощущение времени. Несколько советов ниже помогут вашим детям не впасть в интернет-зависимость.

Советы по достижению равновесия между временем, проводимым в интернете и вне его

1. Следите за симптомами проявления интернет-зависимости. Спросите себя: оказывает ли времяпровождение в Сети влияние на школьные успехи ребенка, его здоровье и отношения с семьей и друзьями? Выясните, сколько времени ваш ребенок проводит в интернете.
2. Обратитесь за помощью. Если у вашего ребенка проявляются серьезные признаки интернет-зависимости, проконсультируйтесь с педагогом. Навязчивое использование интернета может быть симптомом других проблем, таких как депрессия, раздражение или низкая самооценка.
3. Не запрещайте интернет. Для большинства детей он является важной частью их общественной жизни. Вместо этого установите внутрисемейные правила использования интернета. В них можно включить следующие ограничения: количество времени, которое ежедневно проводит в интернете ребенок; запрет на Сеть до выполнения домашней работы; ограничение на посещение чатов или просмотр материалов «для взрослых».
4. Держите компьютер в открытом помещении. Установите компьютер в общей комнате вашей квартиры, а не в спальне ребенка.
5. Поддерживайте равновесие. Пусть ребенок почаще играет с другими детьми на свежем воздухе.
6. Помогайте ребенку участвовать в общении вне интернета. Если ваш ребенок застенчив и испытывает неловкость при общении с ровесниками, почему бы не рассмотреть возможность специального тренинга? Поощряйте участие ребенка в тех видах деятельности, которые объединяют детей с одинаковыми интересами, например, моделирование кораблей или литературный кружок.
7. Контролируйте своих детей. Ознакомьтесь с программами, которые ограничивают использование интернета и осуществляют контроль над посещаемыми сайтами, например, MSN Premium. Однако помните, что сообразительный ребенок, если постарается, может и отключить эту службу. Поэтому ваша конечная цель — развитие у детей самоконтроля, дисциплины и ответственности.

8. Предложите альтернативы. Если вам кажется, что ваши дети интересуются только онлайн-развлечениями, попробуйте предложить им автономный аналог одной из их любимых игр. Например, если ваш ребенок получает удовольствие от ролевых игр на тему фэнтези, предложите ему почитать книги соответствующей тематики.