

Памятки кибербуллинг. Кибербезопасность

Ребенок может обхитрить кибермошенника. Но для этого он должен знать как минимум 10 правил о том, что можно и чего нельзя делать, когда ты онлайн.

- 1. Если ваш компьютер “говорит”, что сайт небезопасный, послушайте его.** Иногда может появиться всплывающее окно с предупреждением, а порой в строке браузера отображается знак “красный замок”. Это значит, что сайт, на который вы переходите, сомнительный. Лучше закрыть окно.
- 2. Иногда в сети лучше промолчать.** Не стоит писать пост о том, что вы одни дома, рассказывать, чем занимаются родители. Ни в коем случае не объявляйте всему миру, что дом останется без хозяина на две недели. Никогда не знаете, кто может воспользоваться этой информацией.
- 3. Следите за личной информацией, которая попадает в сеть.** Лучше выложить селфи с друзьями со вчерашней прогулки, чем фото своего дома, дачи, характеризующие уровень достатка. Также избегайте провокационных фотографий. Такой контент притягивает неадекватных граждан.
- 4. Встречайтесь с реальными друзьями.** Если пришло сообщение от виртуального друга, которого вы знаете только по переписке, лучше отказать во встрече. “Развиртуализация” бывает крайне опасна.
- 5. У каждого аккаунта должен быть свой пароль.** Чтобы не получилось так, что добыв логин и пароль от вашей страницы в соцсети, мошенники получили доступ в мобильный банк. А такие истории не редкость.
- 6. Придумайте сложный пароль.** Не нужно использовать слова из словаря, сочетание “имя+мобильный телефон”. Транслитерация — тоже не лучший вариант. Вводите буквы, цифры, символы. Пусть лучше это будет больше похоже на сумбур, чем “12345”. Но даже самый сложный пароль надо менять хотя бы раз в полгода. А хранить их можно в фотографиях или заметках среди длинного текста.
- 7. Обновляйте приложения и программное обеспечение.** Как только система предлагает вам установить обновление, делайте это. Причем самые уязвимые для вирусов — это приложения Office и Adobe, не забывайте про них.
- 8. Не все ссылки ведут туда, куда нужно.** Часто на почту приходят письма с просьбами перейти по той или иной ссылке. А там “зловред” — атакующее программное обеспечение. Он незаметно для пользователя “угоняет” логины и пароли, номера платежных карт, которые когда-либо вводили в браузере, сканы документов и паспортов и превращает гаджет в один из узлов ботсети. Не стоит переходить по таким ссылкам, особенно если они в письме от незнакомых вам отправителей.
- 9. Между LTE и публичным wi-fi выбирайте LTE.** Не стоит подключаться к публичным wi-fi в кафе, транспорте, музеях. Вы можете попасть в сеть мошенника,

который будет пропускать весь ваш трафик через свою систему и собирать логины, пароли, номера кредитных карт, личную информацию.

10. Не платите в играх. Когда онлайн игра просит оплатить дополнительные кристаллы, жизни, броню "живыми" деньгами, не делайте этого. Не стоит вводить данные своей карты, иначе вы рискуете стать жертвой обманщиков, которые решили сыграть на вашем азарте.



ПАМЯТКА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

В Интернет ты заходишь через компьютер или мобильное устройство. Любому устройству могут повредить вирусы. Они могут уничтожить важную информацию или украсть деньги через Интернет.

НЕ ЗАХОДИ НА ПОДОЗРИТЕЛЬНЫЙ САЙТ

Если антивирусная защита компьютера или мобильного устройства не рекомендует, не заходи на сайт, который считается «подозрительным».

НЕ СОХРАНЯЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ И НЕ ОТКРЫВАЙ ИХ

Не устанавливай и не загружай программы, музыку, видео или другие файлы, если не уверен, что они безопасны.

НЕ СООБЩАЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Никогда не сообщай свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

НИКОМУ НЕ СООБЩАЙ СВОЙ ЛОГИН С ПАРОЛЕМ

Никому не сообщай свой логин с паролем и не выкладывай их в Интернете - относись к ним так же бережно, как к ключам от квартиры.

НЕ МЕНЯЙ НАСТРОЙКИ ГАДЖЕТА

Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках, если не понимаешь, как это работает и зачем нужно.

ПРИ НЕИСПРАВНОСТИ ГАДЖЕТА ВЫКЛЮЧИ ЕГО

Если тебя что-то пугает в работе компьютера или мобильного устройства, немедленно выключи его. Обратись в службу ремонта.

Рекомендации

для родителей по использованию сети Интернет их детям

Для детей от 7 до 10 лет.

Оптимальной формой ознакомления ребенка в таком возрасте с сетью Интернет будет совместная работа с ребенком за компьютером.

Приучите детей:

- посещать только те сайты, которые Вы разрешили;
- советоваться с Вами, прежде чем совершить какие-либо новые действия, раскрыть личную информацию;
- сообщать Вам, если ребенка что-то встревожило либо было непонятно при посещении того, либо иного сайта.

Запретите:

- скачивать файлы из Интернета без Вашего разрешения;
- общаться в Интернете с незнакомыми Вам людьми;
- использовать средства мгновенного обмена сообщениями без Вашего контроля.

Постоянно беседуйте с детьми на тему использования ими сети Интернет: о действиях, посещенных сайтах, возможных новых знакомых.

Для детей от 10 до 13 лет.

В данном возрасте ребенок уже обладает определенными навыками и познаниями о работе в сети, не готов к постоянному личному контролю со стороны взрослых, однако все еще требует контроля.

Рекомендации:

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- напоминайте о конфиденциальности личной информации;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета, при скачивании и установке программного обеспечения;

поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;

- настаивайте на том, чтобы ребенок позволял Вам знакомиться с содержимым его электронной почты, учетных записей в социальных сетях, перепиской в средствах мгновенного обмена сообщениями;
- расскажите об ответственности за недостойное поведение в сети Интернет.

На данном этапе могут активно использоваться программные средства родительского контроля, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающая услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;
- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);
- функции родительского контроля, встроенные в некоторые антивирусы (например Kaspersky Internet Security, Norton Internet Security), позволяющие контролировать использование компьютера, запуск различных программ

- (попытки запуска запрещенных программ блокируются), использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, загрузку файлов из Интернета, переписку с определенными контактами через Интернет мессенджеры и социальные сети, пересылку персональных данных, употребление определенных слов и словосочетаний в переписке через мессенджеры;
- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.

Подростки в возрасте 14-17 лет.

Рекомендации:

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;
- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета без Вашего ведома;
- напоминайте детям о необходимости обеспечения конфиденциальности личной информации;
- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности;
- обсудите с ребенком возможные риски при осуществлении покупок в сети.

В сети Интернет на сайтах провайдеров, производителей антивирусного программного обеспечения, а также на специализированных ресурсах можно найти рекомендации по обеспечению защиты детей от различных типов киберугроз. Также значимой для родителей может быть размещенная в сети информация о действиях, если ребенок уже столкнулся с какой-либо интернет-угрозой.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, педагогу социальному учреждения образования, правоохранительные органы по месту жительства.

Советы родителям по безопасности в сети Интернет

Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Какие угрозы встречаются наиболее часто? Прежде всего:

Угроза заражения вредоносным ПО. Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко

попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

Доступ к нежелательному содержимому. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера.

Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

Неконтролируемые покупки. Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

Приведем **несколько рекомендаций**, с помощью которых **посещение Интернет** может стать менее опасным для ваших детей:

Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;

Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.; Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;

Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;

Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены;

Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Советы родителям, дети которых издеваются онлайн

- **Обратитесь к специалистам.**

Если ваш ребенок сталкивается с проблемой совладания с сильными эмоциями, такими как злость, ранимость или фрустрированность, то поговорите с психологом о том, как помочь ребенку научиться совладать с этими чувствами здоровыми способами.

- **Проведите образовательные беседы о кибербуллинге и травле онлайн.**

Ребенок вполне может не понимать, насколько болезненным и ранящим является такое поведение. Усильте эмпатию, сочувствие и сопереживание ребенка, а также его осведомленность, поощрив его посмотреть на происходящее со стороны жертвы.

- **Управление стрессом.** Научите ребенка позитивным способамправляться со стрессом. Тренировки, проведение времени на природе, игры с домашними питомцами — отличные способы как для детей, так и для

взрослых дать выход пару и облегчить стресс.

- **Установливайте ограничения на технологии.** Дайте знать ребенку, что вы будете отслеживать его использование компьютера, планшета, смартфона, электронной почты и сервисов для сообщений. Если нужно, запретите доступ к технологиям, пока поведение не улучшится.

- **Установите согласующиеся правила поведения.** Убедитесь, что ребенок понимает правила и наказания за их нарушения.

- **Травля часто — выученное поведение.** Некоторые хулиганы научаются агрессивному поведению из собственного опыта дома, поэтому важно подавать хороший пример собственным привычкам онлайн.

КАК СОВЛАДАТЬ С КИБЕРБУЛЛИНГОМ И ТРАВЛЕЙ В ИНТЕРНЕТЕ



**СОВЕТЫ РОДИТЕЛЯМ
ПО ПРЕДОТВРАЩЕНИЮ
ТРАВЛИ В ИНТЕРНЕТЕ**

Советы взрослым, как прекратить кибербуллинг и травлю в интернете

Вне зависимости от того, сколько боли причиняет травля, дети часто неохотно рассказывают родителям и учителям о кибербуллинге и травле в интернете, потому что они боятся, что такой поступок приведет к лишению их привилегии сидеть за компьютером и иметь мобильный телефон.

В то время как родители всегда должны отслеживать, как ребенок использует технологии, важно не угрожать потерей доступа или другими наказаниями ребенку, который стал жертвой кибербуллинга и издевательств в интернете.



Ваш ребенок, возможно, — жертва кибербуллинга и издевательств в интернете, если он:

1. Становится грустным, злым или пребывает в стрессе во время или после использования интернета или мобильного телефона.
2. Проявляет тревогу, когда получает сообщение, «быстрое сообщение» или электронное письмо.
3. Избегает обсуждений или проявляет секретность по поводу активности за компьютером или мобильным телефоном.
4. Отчуждается от семьи, друзей и деятельности, которую раньше любил.
5. Стал учиться хуже, оценки снижаются по необъяснимым причинам.
6. Отказывается посещать школу или ходить на конкретные уроки; избегает групповых активностей.
7. Проявляет изменения в настроении, поведении, сне, аппетите или проявляет признаки депрессии или тревоги.

Предотвратите кибербуллинг и травлю в интернете до того, как они произошли

Научите ребенка:

- Отказываться действовать в соответствии с сообщениями хулиганов.
- Говорить с друзьями, чтобы прекратить кибербуллинг и травлю в интернете.
- Блокировать общение с хулиганами; удалять сообщения, не читая их.
- Никогда не публиковать и не делиться личной информацией онлайн.
- Никогда не делиться паролями от интернет-сервисов ни с кем, кроме вас.
- Говорить с вами о жизни онлайн.
- Никогда не выносить онлайн ничего, что не хочется показывать одноклассникам, даже по электронной почте.
- Не посыпать сообщения, когда пребываешь обозлен или расстроен.
- Всегда быть вежливым онлайн, будто говорить лично.



Предотвращение кибербуллинга

- Объясните детям, что личная информация, которую они выкладывают в интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.
- Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаления странички, оскорблений.
- Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете.
- Убедитесь, что оскорблении (буллинг) из сети не перешли в реальную жизнь. Если угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под действие уголовного кодекса.



Рекомендации "Как оградить детей от недостоверной информации в сети интернет"

Рекомендации для родителей

Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в то же время, Сеть таит в себе много опасностей. Обязательно нужно поговорить с детьми, объяснить, что могут возникать различные неприятные ситуации и то, как из них лучшим образом выходить. Помните, что безопасность ваших детей в Интернете, на 90% зависит от вас. Напомните детям, что каждый компьютер,

ноутбук имеет персональный IP- адрес. Поэтому всегда очень легко установить адрес и данные пользователя.

Как защитить детей от негативной информации?

В связи с развитием новых технологий в области виртуального пространства, в том числе с распространением сети Интернет, возникла проблема, связанная с доступом несовершеннолетних к информации сомнительного содержания и противоречащей общепринятой этике. В настоящее время любой человек, в том числе и несовершеннолетний, владеющий знаниями в области компьютерных технологий, может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб - ресурс. Отсутствие контроля со стороны родителей за использованием детьми сети Интернет - одна из причин доступности негативной информации несовершеннолетним. Памятка родителям по безопасному использованию детьми сети Интернет. Основные правила, которые помогут оградить Ваших детей от информации сомнительного содержания и противоречащей общепринятой этике, позволяют избежать детям проблем с законом.

Правило №1 Родители должны знать интересы и цели детей, которые используют сеть Интернет.

Правило №2 Рекомендуется допускать использование сети Интернет детьми в присутствии взрослых. Доступ к данному информационному ресурсу должен быть эффективным и безопасным.

Правило №3 Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Республики Беларусь, может оказывать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.).

Правило №4 В случае самостоятельного доступа детей к сети Интернет, родители должны контролировать использование информации несовершеннолетними. О характере и объеме информации, полученной детьми в интернет – ресурсах, необходимо узнавать в «Журнале обозревателя» программы "Internet Explorer". Как ограничить доступ детей к негативной информации в сети Интернет? С целью ограничения доступа детей к «вредным» материалам родители и другие члены семьи могут установить на компьютеры программу

«Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков.

Правила №5 Расскажите детям о порнографии в Интернете. Каждый, кто пользуется социальными сетями, должен помнить, что информация о комментариях, отметках «лайк», нажатии кнопки «Поделиться с друзьями» становится достоянием друзей пользователя, а то и друзей его друзей. То есть определённый круг людей сможет увидеть, какая фотография, видеоролик, картинка или текст заинтересовали того или иного пользователя. Более того, многие приложения сети работают таким образом, что комментарии отображаются на личных страницах со ссылкой на ресурс самих комментаторов

автоматически. А за всё, что размещено на их личных страницах, пользователи несут полную ответственность. Напомните детям, что размещая к себе какой-либо контент, они фактически его рекламируют, делают доступным широкому кругу пользователей. В случае с порнороликами - рекламируете порнографию, то есть занимаетесь её распространением. А это преступление!

Советы по безопасности для детей разного возраста

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.

Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Что можно посоветовать в плане безопасности в таком возрасте?

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее.

- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
- Научите детей не загружать файлы, программы или музыку без вашего согласия.
- Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями.
- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
- Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых».
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

9-12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Не забывайте беседовать с детьми об их друзьях в Интернет.
- Наставайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
- Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
- Расскажите детям о порнографии в Интернет.
- Наставайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
- Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).
- Компьютер с подключением к Интернет должен находиться в общей комнате.
- Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет.
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
- Расскажите детям о порнографии в Интернете. Каждый, кто пользуется социальными сетями, должен помнить, что информация о комментариях, отметках «лайк», нажатии кнопки «Поделиться с друзьями» становится достоянием друзей пользователя, а то и друзей его друзей. То есть определенный круг людей сможет увидеть, какая фотография, видеоролик, картинка или текст заинтересовали того или иного пользователя. Более того, многие приложения сети работают таким образом, что комментарии отображаются на личных страницах со ссылкой на ресурс самих комментаторов автоматически. А за всё, что размещено на их личных страницах, пользователи несут полную ответственность. Напомните детям, что размещая к себе

какой-либо контент, они фактически его рекламируют, делают доступным широкому кругу пользователей. В случае с порнороликами - рекламируете порнографию, то есть занимаетесь её распространением. А это преступление.

- Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- Приучите себя знакомиться с сайтами, которые посещают подростки.
- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закона.

Вот на что следует обратить внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- Беспокойное поведение.

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- Неприязнь к Интернету

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- Нервозность при получении новых сообщений

Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.

2. Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности.

- Ознакомьтесь с отзывами покупателей:
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах.
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить

Как распознать интернет и игровую зависимость

Сегодня все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также

могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
- Периодически старайтесь полностью проверять свои домашние компьютеры.
- Делайте резервную копию важных данных.
- Страйтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Что делать, если ребенок все же столкнулся с какими-либо рисками?

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать.

- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете.
- Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.

- Сберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы).
- Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций.

Семейное соглашение о работе в Интернет

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:

- Какие сайты могут посещать ваши дети и что они могут там делать.
- Сколько времени дети могут проводить в Интернет.
- Что делать, если ваших детей что-то беспокоит при посещении Интернет.;
- Как защитить личные данные.
- Как следить за безопасностью.
- Как вести себя вежливо.
- Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

Научите вашего ребенка использовать службу мгновенных сообщений

При использовании службы мгновенных сообщений напомните вашему ребенку некоторые несложные правила безопасности:

- Никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их может каждый.
- Никогда не разговаривайте в Интернет с незнакомыми людьми.
- Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем общаются.
- Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает.

- Не следует использовать систему мгновенных сообщений для распространения слухов или сплетен.

Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения с вашими детьми.

Может ли ваш ребенок стать интернет-зависимым?

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать?

Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.