

Памятка для родителей

Безопасность детей в социальных сетях. Родительский контроль.

Нынешние дети начинают учиться считать, писать и читать практически одновременно с работой за компьютером. Хорошо это или плохо — вопрос спорный. Но несомненно, что освоение компьютера с юных лет открывает широкие возможности в плане развития и образования, которые чаще всего реализуются при активном подключении родителей в качестве направляющей и контролирующей стороны.

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

Как правило, родителям требуется организовать контроль за временем работы на компьютере (время приходится ограничивать), регулировать доступ к «вредным» программам (в частности, к играм), а также наблюдать за использованием Интернета и блокировать доступ к неподходящим для ребенка ресурсам.

С 2004 года в первый вторник февраля празднуется Всемирный день безопасного Интернета. В условиях быстрых темпов развития информационных технологий необходимость контроля Интернета становится вопросом первостепенной важности. Рискам, таящимся в киберпространстве, особенно подвержены дети. Глобальная сеть ничуть не безопаснее игровой площадки. Это понимают во всем мире.

- Сегодня не нужно работать в ФСБ, чтобы узнать о человеке все, достаточно залезть в Интернет, и Вы найдете фамилию, возраст, адрес, место учебы, материальное положение. Практика показывает, что дети в поисках друзей размещают о себе в Сетях только голую правду. А опытным мошенникам не остается ничего кроме как воспользоваться их наивностью и недостатком родительского контроля. Преступники в Интернете действуют по принципу волка в овечьей шкуре. Они пользуются тем, что дети не могут распознать взрослого, умело маскирующегося под их сверстника. Только контролируя Интернет, отслеживая переписку ребенка, родители могут обнаружить тех, кто отправляет подозрительные сообщения их детям, пытается втереться к ним в доверие, договориться о встрече, задает наводящие вопросы и забрасывает просьбами выслать откровенные фотографии

- Глобальная Сеть содержит большое количество информации взрослого содержания. Интернет насчитывает сотни миллионов порнографических

страниц. Порнография считается одной из самых прибыльных отраслей. Эта индустрия в Интернете приносит около 2,5 миллиардов долларов в год. А количество порнографических страниц с каждым годом растет в десятки раз быстрее, чем грибы после дождя.

- Другая серьезная проблема - распространение наркотиков через Глобальную Сеть. Достаточно набрать в поисковике название наркотического средства, чтобы узнать всё, начиная от того, как его приготовить до того, где взять.

- В Интернете легко найти информацию суицидального характера, видеоматериалы по дракам, вскрытиям. Здесь же дети, оставшись без надлежащего контроля родителей, могут свободно познакомиться с любыми формами экстремизма.

- Интернет – реальный пожиратель времени. В поисках развлечений, играя или просто зависая в чате, можно проводить часы драгоценной жизни. В последние годы набирает обороты болезнь под названием «Интернет-зависимость». Дети начинают пропускать уроки, хуже учиться, становятся раздражительными. По мнению врачей, родителям следует контролировать, чтобы младший школьник проводил за компьютером не больше четверти часа. Бесконтрольное сидение в Интернете ведет к тому, что дети теряют зрение, перестают заниматься спортом, теряют навыки общения вне Сети. В Китае несколько подростков умерли за компьютером не в силах оторваться от экрана, чтобы поесть.

- Кроме того, через Интернет легко проникают вредоносные программы в виде вложенных файлов электронных писем, троянских коней, HTML и Java-вирусов и могут привести в поломку компьютера.

С 2008 года в России существует Национальный узел Интернет-безопасности - Центр безопасного Интернета. Он посвящен проблеме безопасной, корректной и комфортной работы в Глобальной сети. Создатели проекта уверены, что в условиях ускоренных темпов внедрения Интернета в повседневную жизнь граждан защита наших детей от рисков, скрытых в недрах всемирной паутины, требует активной позиции каждого.

Родительский контроль компьютера.

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра веб-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как

осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

Довольно часто применяется более жесткий способ контроля – создание белого списка. Ребенок может посещать только те веб-сайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребенок даже не в курсе, о чем вообще сверстники ведут разговор, Интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержанию. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на веб-странице, то она не открывается. Родителям, возможно, придется отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к веб-сайтам. Есть еще одна, если так можно выразиться, группа риска – это программы обмена мгновенными сообщениями. Ребенок наивен, он можно нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. Напрашивается и вторая опасность – собеседники ребенка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьезных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

В вашей семье один ребенок или несколько детей, есть компьютер, подключенный к Интернету. Как обезопасить младшее поколение от негативных последствий пребывания в Сети? Первое, что сразу напрашивается – компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь родителей сможет постоянно

следить за тем, чем занимается ребенок. В противном случае, он запрется в комнате, и вы даже, возможно, не догадаетесь, что чадом скачано несколько фильмов эротического содержания, а в местном чате ему рассказали, как самому делать петарды.

Ребенку надо показать Интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя. Нельзя соглашаться на встречи с незнакомыми людьми, нельзя сообщать личные данные, нельзя самостоятельно совершать покупки в сетевых магазинах. Ну а вместо нравоучений сыну «не смотри на голых женщин», уместней воспользоваться специальными программными продуктами, которые закроют ему доступ к взрослым ресурсам.

Идеального рецепта настройки родительского контроля не существует, поскольку тут всё зависит от целого ряда факторов: уровня компьютерной подготовки ребенка и его родителей, компьютерных предпочтений и степени сознательности подрастающего поколения и, наконец, от отношения самих родителей к данной проблеме. Вариантов организации родительского контроля несколько. Можно ограничиться встроенными средствами Windows, задействовать модули родительского контроля в решениях класса Internet Security, подключиться к сервисам для фильтрации нежелательных сайтов либо установить специализированные программы родительского контроля.

Обучение детей основам безопасности при работе с Интернетом

1. Научите детей никому не сообщать пароли

Дети создают имена пользователей и пароли для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций.

Согласно исследованиям 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, 66 процентов девочек в возрасте 7-12 признались, что сообщали свой пароль другим лицам.

Первое правило безопасности при работе в Интернете: пароли следует держать в секрете. Научите детей хранить свои пароли столь же бережно, как информацию, которую они хотя защитить.

Правила, которые дети должны знать и соблюдать:

- Никогда не сообщайте свои пароли другим. Не показывайте никому свои пароли, даже друзьям.

- Обеспечьте защиту для записанных паролей. Будьте внимательны к тому, где вы храните или записываете пароли. Не храните пароли в рюкзаке или бумажнике. Не оставляйте данные о паролях в местах, где вы бы не хотели оставить информацию, защищенную с их помощью. Не храните пароли в файле на компьютере. Преступники ищут там в первую очередь.

- Никогда не предоставляйте свой пароль по электронной почте или в ответ на запрос по электронной почте. Любое сообщение электронной почты, в котором вас просят указать пароль или перейти на веб-сайт, чтобы проверить пароль, может представлять собой разновидность мошенничества, которая называется фишингом. К ним относятся запросы с сайтов, вызывающих доверие, которые вы можете постоянно посещать. Мошенники часто создают поддельные сообщения электронной почты, содержащие такие же логотипы как и на реальных сайтах и написанных таким языком, чтобы не вызывать сомнения в своей достоверности.

- Не вводите пароли на компьютерах, которые вы не контролируете. Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете.

Не используйте эти компьютеры с учетными записями, где требуется вводить имя пользователя и пароль. Преступники могут за очень небольшие деньги приобрести устройства, регистрирующие нажатия клавиш, которые устанавливаются в течение нескольких секунд. С помощью подобных устройств злоумышленники могут собирать информацию, вводимую на компьютере, через Интернет.

2. Помощь детям в безопасном использовании социальных сетей.

Ваши дети могут пользоваться сайтами социальных сетей, которые предназначены для детей, такими как Webkinz или Club Penguin, или сайтами, предназначенными для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие.

Дети используют социальные сети для общения с лицами, которые могут проживать на другом конце земного шара, или со своими знакомыми, с которыми они каждый день видятся в школе.

Дети должны понимать, что многие из этих сайтов социальных сетей могут просматриваться всеми, кто имеет доступ в Интернет. В результате публикации ими некоторой информации они могут стать уязвимыми для фишинговых сообщений, киберугроз и похитителей в Интернете.

Далее приведены некоторые советы, которые помогут детям безопасно пользоваться сайтами социальных сетей:

1. Беседуйте с детьми по поводу их общения в социальных сетях. Просите детей рассказывать вам, если им встретится в Интернете то, что вызывает у них беспокойство, неудобство или страх. Сохраняйте спокойствие и убедите детей, что вам можно рассказывать о таких вещах. Дайте детям понять, что вы поможете им успешно разрешить сложившуюся ситуацию.

2. Определите правила работы в Интернете. Как только ваши дети станут самостоятельно пользоваться Интернетом, установите правила пользования Интернетом. В этих правилах должно быть определено, могут ли ваши дети использовать сайты социальных сетей и каким образом.

3. Убедитесь в том, что ваши дети соблюдают возрастные ограничения. Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 и более лет. Если ваши дети не достигли этого возраста, не разрешайте им пользоваться данными сайтами. Вы не должны полностью полагаться на сами службы, чтобы не допустить регистрацию ваших детей на этих сайтах.

4. Учитесь. Оцените сайты, которые планирует использовать ваш ребенок, и убедитесь, что вы и ваш ребенок понимают политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль над публикуемым содержимым. Кроме того, периодически просматривайте страницу вашего ребенка.

5. Научите своих детей никогда лично не встречаться с теми, с кем они общались только по сети. Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети. Иногда бывает недостаточно просто сказать детям, чтобы они не разговаривали с незнакомыми людьми, поскольку дети могут не считать незнакомым человека, с которым они «встречались» в сети.

6. Попросите детей общаться только с теми людьми, которых они уже знают. Вы можете помочь защитить ваших детей, попросив их использовать данные сайты для общения с друзьями и никогда не общаться с теми, с кем они лично не встречались.

7. Убедитесь в том, что ваши дети не указывают свои полные имена. Научите своего ребенка указывать только свое имя или псевдоним и ни в коем случае не использовать псевдонимы, которые могли бы привлечь нежелательное внимание. Кроме того, не разрешайте своим детям публиковать полные имена своих друзей.

8. Относитесь с осторожностью к идентифицирующей информации в профиле вашего ребенка. На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающих учеников определенной школы.

9. Будьте осторожны, если ваши дети предоставляют информацию, по которой их можно идентифицировать, например школьное животное - талисман, рабочее место или город проживания. Если указано слишком много информации, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных.

10. Постарайтесь выбрать сайт, который не столь широко используется. Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ваш ребенок. Например, с помощью Windows Live Spaces вы можете настроить разрешения, указав тех, кто может посещать ваш сайт. При этом возможны самые различные настройки – от всех пользователей Интернета до ограниченного списка людей.

11. Следите за деталями на фотографиях. Объясните детям, что фотографии могут раскрывать много личной информации. Попросите детей не публиковать фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.

12. Предостерегите своего ребенка относительно выражения своих эмоций перед незнакомцами. Вероятно, вы уже предупреждали своих детей не общаться с незнакомыми людьми напрямую по сети. Однако дети используют сайты социальных сетей для написания журналов и стихотворений, в которых часто выражают сильные чувства.

Объясните детям, что написанное ими сможет прочесть любой, кто имеет доступ в Интернет, и похитители часто ищут эмоционально уязвимых детей.

13. Расскажите детям об интернет-угрозах. Как только ваши дети станут достаточно взрослыми для использования сайтов социальных сетей, расскажите им о них киберугрозы. Расскажите детям, что если у них возникнет ощущение, что им угрожают через Интернет, то им сразу же следует сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют. Кроме того, очень важно научить детей общаться по сети точно так же, как они общаются лично. Попросите детей относиться к другим людям так же, как они хотели бы, чтобы относились к ним самим.

14. Удаление страницы вашего ребенка. Если ваши дети отказываются соблюдать установленные вами правила для защиты их безопасности, и вы безуспешно пытались помочь им изменить свое поведение, можно обратиться на веб-сайт социальной сети, которую использует ваш ребенок, с просьбой удалить его страницу. Можно также обратить внимание на средства фильтрации интернет-содержимого (например, Функции семейной безопасности Windows Live) в качестве дополнения и ни в коем случае не замены для контроля со стороны родителей.

3. Если ваши дети пишут блоги, убедитесь в том, что они не рассказывают слишком много о себе.

Практика написания блогов (сокращение от англ. "web log" – дневник в сети) или личного интерактивного журнала очень быстро стала популярной среди подростков, многие из которых ведут свои блоги без ведома родителей или опекунов.

Социальные сети сейчас обошли по популярности блоги среди большинства подростков, однако многие дети по-прежнему ведут свой блог на своем сайте социальной сети. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском.

Несмотря на то, что ведение блога дает возможные преимущества, включая развитие навыков письма и общения, очень важно рассказать детям об Интернете и научить их писать блоги еще до того, как они начнут этим заниматься аналогично тому, как все сначала оканчивают курсы по вождению, прежде чем самостоятельно садятся за руль автомобиля.

Начальные советы:

1. Определите правила пользования Интернетом с детьми и проявите настойчивость.

2. Просматривайте то, что дети планируют опубликовать в Интернете, прежде чем они опубликуют эти материалы. Внешне безобидную информацию, например школьное животное-талисман и фотография города, можно собрать воедино и понять, в какую школу ходит автор.

3. Спросите себя (и проинструктируйте детей делать то же самое), насколько комфортно вы будете чувствовать себя, показывая эти материалы незнакомцу. Если имеются сомнения, исключите такие материалы.

4. Проведите оценку службы блогов и выясните, обеспечивает ли она возможность написания личных блогов, защищенных с помощью паролей.

5. Сохраните интернет-адрес блога вашего ребенка и регулярно проверяйте его.

6. Просматривайте другие блоги, отыскивая положительные примеры для подражания для ваших детей.

4. Помните об интернет-мошенниках

Согласно данным Федеральной торговой комиссии США, 31 процент жертв похищения личных данных составляют молодежь. Подростки становятся привлекательными объектами для мошенников, поскольку у них хорошие кредитные оценки и малый долг, по сравнению со взрослыми они меньше заботятся о безопасном хранении информации.

Некоторые моменты, о которых должны знать ваши дети, чтобы стать разумными потребителями и избежать интернет-мошенничества:

1) Никогда не разглашайте личную информацию. Никогда не указывайте свою личную информацию, например полное имя или город проживания во время общения с помощью мгновенных сообщений или в чатах, если вы полностью не уверены в личности человека, с которым вы общаетесь.

2) Обязательно завершайте сеанс с выходом из системы при работе на общедоступном компьютере. Если вы используете компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью завершите все сеансы с выходом из системы. Вы не знаете, какое программное обеспечение установлено на этих компьютерах, а также что оно выполняет. Кроме того, может быть установлено программное обеспечение, фиксирующее нажатие клавиш.

3) Придумывайте безопасные пароли и держите их в секрете.

4) Используйте только безопасные сайты. Если ваши дети совершают покупки в Интернете, то им следует каждый раз убеждаться в том, что URL-адрес сайта, на котором они вводят финансовую информацию, начинается с префикса `https://`, в правом нижнем углу имеется желтый значок замка или адресная строка отображается зеленым цветом. Они могут щелкнуть по значку замка или в адресной строке, чтобы проверить сертификат безопасности данного сайта.

5) Распознавание мошенников и сообщение о фактах мошенничества. Расскажите своим детям о признаках подделки идентификационных данных: предложение утвержденных кредитных карт, звонки из агентств по сбору информации или незнакомые финансовые документы. Если у вашего ребенка возникнет подозрение на подделку личных данных, немедленно предпримите соответствующие действия, чтобы ограничить ущерб. Обратитесь в свою кредитную компанию, банки или все три организации по кредитной отчетности, а также в полицию. Закройте все счета, которые подвергались фальсификации, и попросите детей поменять пароли для всех своих учетных записей в Интернете. Ведите журнал всех выполняемых действий.

Для детей и их неравнодушных родителей существует бесплатная линия помощи «Дети онл@йн» <http://detionline.com>

Если ребенка оскорбляют и преследуют в интернете или ребенок стал жертвой сетевых мошенников, столкнулся с опасностью во время пользования сетью Интернет, если вы обеспокоены безопасностью ребенка при его работе в интернете, обратитесь на бесплатную линию помощи «Дети онл@йн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и интернета. Консультации проводят психологи и технические специалисты МГУ имени М.В. Ломоносова, Федерального института развития образования МОН РФ и МГТУ им. Баумана.