Памятка для родителей
Безопасность детей в социальных сетях. Родительский контроль

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 апреле 2012 года Президент РФ Дмитрий Медведев на заседании президиума Государственного совета России выступил за контроль Интернета на предмет пропаганды наркотиков.

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.

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.

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.

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.
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.
- 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.

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, киберугро и похитителей в Интернете.

Советы, которые помогут детям безопасно пользоваться сайтами социальных сетей:
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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. 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.
- 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.
- 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.
- 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.
- Расскажите детям об интернет-угрозах. Как только ваши дети станут достаточно взрослыми для использования сайтов социальных сетей, расскажите им о них киберугроз. 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.

- 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.
- 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.

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 к педагогам учебного заведения, где учится ребенок или участковому по месту жительства.