Безопасный интернет детям!

Памятка для детей и родителей

Интернет – это мир интересных и полезных возможностей, но в то же время это источник угроз, особенно для ребенка. Агрессия, преследования, мошенничество, психологическое давление, встречи с онлайн незнакомцами – это лишь некоторый перечень угроз, которые поджидают ребенка в глобальной сети каждый день. Как же оградить от них ребенка?



В России почти 12 млн. несовершеннолетних пользователей интернета, при этом большинство родителей не знают, что делает их ребенок во Всемирной сети, какую информацию ищет, с кем общается. Чтобы сделать интернет безопасным, «Билайн» совместно с экспертами выработали простые рекомендации для заботливых родителей и их детей, которые помогут предупредить угрозы и сделать работу в Интернете полезной.

Самый главный совет для родителей – будьте в курсе деятельности ребенка. Говорите с ним об Интернете: спрашивайте, что он сегодня делал, с кем познакомился, что интересного узнал. Старайтесь регулярно просматривать ресурсы, которые посещает Ваш ребенок, и проверяйте список его контактов, чтобы убедиться, что он знает всех, с кем общается. Попросите ребенка сообщать Вам или близким людям о любых угрозах или тревогах, связанных с Интернет, и не ругайте за неприятные случаи, иначе он все будет скрывать.

Второе важное правило – станьте проводником ребенка в Интернет. То, чему не научите ребенка Вы, научат другие или ребенок сам научится, не подозревая об угрозах. Поэтому Вам следует хорошо разбираться в Интернет и помогать ребенку его осваивать. Научите ребенка правильно искать нужную информацию, сформируйте список полезных, интересных, безопасных для детей ресурсов и посоветуйте правильно их использовать. С самого начала объясните ребенку, почему ни в коем случае не стоит выдавать данные о себе и своейсемье, публиковать фотографии, где изображен сам ребенок, семья, школа и прочие данные.

Научите вашего ребенка уважению и этикету в Интернете. По статистике, более 80% российских детей имеют профиль в социальных сетях, а 23% сталкиваются в Сети с агрессией и унижением. Попросите ребенка его не провоцировать конфликтные ситуации и относиться к другим так же, как он хотел бы, чтобы относились к нему самому. Объясните, что ни при каких обстоятельствах не стоит размещать провокационный материал и не распространять по чьей-либо просьбе информационные и агрессивно-настроенные сообщения. Информация, выложенная в Интернет – доступна всем и может быть использована в любых, в том числе, мошеннических целях.

Всегда помните старую поговорку «предупрежден – значит вооружен». Расскажите ребенку, что в Интернете встречаются и «хорошие», и «плохие» люди. Объясните, почему не стоит добавлять «в друзья» незнакомых людей - они могут быть не теми, за кого себя выдают. Предупредите ребенка, чтобы он ни в коем случае не соглашался на «живые» встречи с Интернет-незнакомцами, прежде чем не поставит в курс вас или близких родственников. Посоветуйте ему общаться в Интернете с теми, с кем он лично знаком. Предостерегите от скачивания платной информации, особенно через sms. Объясните, почему не стоит обращать внимания на яркие баннеры с сообщениями о выигрышах или призах. Выдайте ему инструкцию по правильному поведению в глобальной паутине.

И наконец, последний, но не менее важный совет – используйте технические возможности Вашего компьютера и Оператора. Для предотвращения нежелательного контента и вирусов необходимо установить антивирус, настроить антиспам фильтры в почте. С помощью средств Родительского контроля или соответствующих услуг Оператора можно создавать «белый» список Интернет-сайтов, ограничить время пребывания ребенка в Интернет, настроить возрастной фильтр.

Правила безопасного интернета для детей

-  Никому и никогда не разглашай свои пароли. Они – твой главный секрет. Придумай свой уникальный пароль, о котором никто не сможет догадаться. Не записывай пароли на бумажках, не храни их в открытом доступе. Не отправляй свои пароли по электронной почте.

- При регистрации на сайтах и в социальных сетях старайся не указывать личную информацию (номер телефона, адрес места жительства, школы, место работы родителей и другое) – она может быть доступна всем, даже тем, кого ты не знаешь!

- Помни, что фотография, размещенная в Интернете доступна для просмотра всем. Старайся не размещать фото, на которых изображена твоя семья, школа, дом и другие личные данные.

- Старайся не встречаться с теми, с кем ты знакомишься в Интернете.

- Помни, что многие люди рассказывают о себе в Интернете неправду.

- В Интернете и социальных сетях старайся общаться только с теми, с кем ты лично знаком. Подумай и посоветуйся с родителями, прежде чем добавить незнакомого человека к себе в список «друзей».

- Не используй веб-камеру при общении с незнакомыми людьми, помни о необходимости сохранять дистанцию с незнакомыми людьми.

- Уважай собеседников в Интернете. Никогда и ни при каких обстоятельствах не угрожай другим, не размещай агрессивный и провокационный материал. Будь дружелюбен. Не груби.

- Помни, что даже в Интернете существует «сетевой этикет». Если ты пишешь сообщение заглавными буквами, то собеседник может подумать, что ты кричишь на него.

- Не вступай в незнакомые сообщества и не распространяй по чей-либо просьбе информационные, провокационные и агрессивно-настроенные материалы и сообщения.

- Не все, что ты можешь прочесть или увидеть в интернете - правда. Не ленись и перепроверяй информацию в других поисковиках или спроси у родителей.

- Помни, что существуют сайты, непредназначенные для детей, не заходи на сайты «для тех, кто старше 18 лет», на неприличные и агрессивно настроенные сайты. Если ты попал на такой сайт по ссылке, закрой свой браузер, используя клавиши “ctrl+alt+delete”.

- Расскажи все, что ты увидел, выучил или узнал нового взрослому.

- Ни в коем случае не указывай свой номер телефона или электронный адрес, не отправляй с него смс на незнакомые номера в Интернете.

- Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать.

- Если тебе показалось, что твои друзья отправляют тебе «странную» информацию или программы, переспроси у них, отправляли ли они тебе какие-либо файлы. Иногда мошенники могут действовать от имени чужих людей.

- Если ты хочешь купить в Интернете какую-либо услугу или игру, обратись к взрослому. Он подскажет тебе, как избежать мошенничества.

- Не загружай файлы, программы или музыку без согласия взрослых – они могут содержать вирусы и причинят вред компьютеру.

- Попроси родителей установить на компьютер антивирус и специальное программное обеспечение, которое будет блокировать распространение вирусов.

Берегите детей от социальных сетей

По данным «Лаборатории Касперского», самыми распространенными угрозами для детей в социальных сетях являются порнографический контент, педофилия и кибербуллинг — подростковый виртуальный террор. Общение в соцсетях также опасно мошенничеством, в том числе и от лица «друзей», и потенциальным пересечением с преступниками. На сегодняшний день опасными социальными сетями являются  — Вконтакте (самая опасная),  «Одноклассники»,  Интернет-магазины, сайты с порнографией и эротикой, веб-почта и нелегальный софт. Эти ресурсы могут нести опасность не только для психики ребенка, безопасности компьютера, но и для вашего кошелька.

О том, что социальные сети опасны для детей, написано и пишется не мало.  У детей, выросших в  социальных сетях, утрачиваются навыки межличностного общения,  развивается синдром гиперактивности, отмечается подъем психотических проявлений, таких как  бред, беспокойство, спутанность сознания, тревога, повышенная уязвимость, формируется ощущение безнаказанности, отсутствуют знания о добре и зле, о моральных законах социума, о границах поведения и т.д. Часть информации, которую дети публикуют на своих страницах, может сделать их уязвимыми для фишинговых сообщений, киберугроз и интернет-похитителей.
Понятно, что нельзя полностью оградить ребенка от интернета, да это было бы неправильным. К тому же опасности настигнут ребенка лишь тогда, когда он будет в социальных сетях находиться больше, чем в реальном мире.

Если ребенок находится в социальной сети более 4 часов в день, он в два раза чаще страдает от депрессии, и в три раза от расстройства сна, нежели тот, кто проводит в социальных сетях ограниченное количество времени.

Что же делать? Вот несколько советов по защите детей от угроз социальных сетей, предложенных на сайте «Microsoft Центр безопасности»:

- Поговорите с детьми об их опыте общения в социальных сетях. Дайте им понять, что вы вместе с ними постараетесь найти удачный выход из сложившейся ситуации, если она возникнет.

- Установите собственные правила пользования Интернетом у вас дома.   В них должно быть указано, могут ли дети использовать сайты социальных сетей и каким образом.
Проследите за тем, чтобы дети соблюдали возрастные ограничения на сайте. Не разрешайте пользоваться сайтами социальных сетей детям, не достигшим 13 — летнего возраста.

- Научитесь пользоваться сайтом. Узнайте, существует ли на сайте контроль над публикуемым содержимым,  установите его при необходимости, периодически просматривайте страницу вашего ребенка.

- Настаивайте на том, чтобы дети никогда лично не встречались с тем, с кем они общались только по Интернету, и попросите их общаться только с теми, кого они знают лично.  Иногда бывает недостаточно просто сказать детям, чтобы они не разговаривали с незнакомыми людьми.

- Проследите за тем, чтобы ваши дети не указывали  свои полные имена. Не разрешайте им  публиковать полные имена своих друзей.

- Опасайтесь наличия в профиле ребенка информации, по которой можно идентифицировать его личность. В противном случае, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных. Будьте бдительны, если дети разглашают эту и другую информацию, которую можно использовать для их идентификации, например школьный талисман, рабочие места и название города проживания.

- Посоветуйте выбрать сайт, который не столь широко используется. Некоторые сайты позволяют обеспечить защиту с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ребенок.

- Следите за деталями на фотографиях. 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, которые могут раскрывать много личной информации.

- Предостерегите своего ребенка относительно выражения собственных эмоций перед незнакомцами. Объясните детям, что многое из публикуемого сможет прочесть любой пользователь, имеющий доступ в Интернет, а также, что похитители часто ищут эмоционально уязвимых детей.

- Расскажите детям об интернет-угрозах. Если у них возникнет ощущение, что им угрожают через Интернет, то они должны немедленно сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют.

- Удаление страницы. Если ваши дети откажутся следовать установленным правилам, которые предназначены для их безопасности и вы безуспешно пытались их убедить следовать им, то вы можете обратиться на сайт социальной сети, который использует ваш ребенок, и попросить удалить его страницу. Можно также обратить внимание на средства фильтрации интернет-содержимого.

И ещё, как это ни банально, читайте с детьми книги, смотрите вместе фильмы, ходите в музеи, играйте в совместные игры, разговаривайте и объясняйте.

Программное обеспечение для обеспечения безопасности детей в Интернете

«Лаборатория Касперского» представила новое кроссплатформенное решение для обеспечения безопасности детей в Интернете – Kaspersky Kids (http://www.kaspersky.ru/safe-kids-np)

Kaspersky Safe Kids позволит получать информацию о звонках, смс и местоположении ребенка, отслеживать посты и список друзей в социальных сетях, ограничить время использования интернета и устройств.

Kaspersky Safe Kids — мультиплатформенное решение Лаборатории Касперского для защиты детей.

С помощью него вы сможете:

Защитить ребенка от нежелательной информации в интернете.
- Контролировать время ребенка за компьютером и другими устройствами.
- Ограничивать время на игры и социальные сети.
- Контролировать скачивание приложений.
- Получать подробные отчеты о действиях ребенка в интернете.
- Получать информацию о местоположении ребенка и статистику звонков и смс.
- Отслеживать посты с упоминанием ребенка и изменений списка друзей на Facebook.

Вы можете установить Kaspersky Safe Kids на устройства с операционными системами Windows, Android, iOS, и Mac.

Kaspersky Internet Security (http://support.kaspersky.ru/kis2016)

Родительский контроль – это компонент программы Kaspersky Internet Security, позволяющий установить для каждой учетной записи на компьютере ограничения доступа использования компьютера и интернета.

С помощью Родительского контроля вы можете оградить детей и подростков от негативного влияния при работе на компьютере и в интернете, например, обезопасить от длительного нахождения за компьютером и в интернете, от потери времени и денег при посещении некоторых веб-сайтов, ограничить доступ к веб-ресурсам, предназначенным для взрослой аудитории, и т. д.

С помощью Родительского контроля вы можете контролировать:

- Использование компьютера. Вы можете контролировать использование компьютера каждым пользователем. Каждое включение компьютера будет отражено в отчете.
- Запуск различных программ. При включенном контроле время запуска и завершения работы программ будет отражено в отчете, а попытки запуска запрещенных программ будут блокироваться.
- Использование интернета (ограничение использование интернета по времени). Вы можете определить общее суточное количество часов для работы в интернете (например, 6 часов) и задать временной диапозон в течение суток для каждого дня недели (например, с 15 о 20 часов с понедельника по пятницу и с 17 до 23 часов в субботу и воскресенье).
- Посещение веб-сайтов в зависимости от их содержимого.
- Загрузка файлов из интернета в зависимости от их категории. Вы можете определить типы файлов, доступных и запрещенных для скачивания (например, файлы из категории Музыка разрешены к скачиванию, а файлы из категории Архивы – запрещены.)
- Переписка с определенными контактами через интернет-пейджеры (ICQ, Miranda, mIRC и т. д. ). При включенном контроле текст, время и адресаты будут отражены в отчете. (Для включения контроля в программах, использующих защищенное соединение, установите Проверять защищенные соединения, если включен Родительский контроль в окне Настройка – закладка Дополнительные параметры – раздел Сеть.)
- Переписка с определенным контактами в социальных сетях (Facebook, MySpace, Twitter). Вы можете контролировать и ограничивать переписку с конкретными пользователями в социальных сетях. При включенном контроле текст, время и адресаты будут отражены в отчете.
- Пересылка персональных данных. Вы можете контролировать и ограничивать пересылку персональной информации через интернет-пейджеры. При включенном контроле сообщения, содержащие персональные данные, будут блокироваться, а попытка пересылки будет отражена в отчете.
- Употребление определенных слов и словосочетаний в переписке через интернет-пейджеры. При включенном контроле каждое ключевое слово, обнаруженное в переписке, будет отражено в отчете.
- Вы можете указать для учетной записи пользователя псевдоним и выбрать изображение, которое будет отображаться в интерфейсе программы.

Использованы материалы сайтов:
http://www.mamainfo.ru/
http://eduinspector.ru/
http://ocompah.ru/
http://kaspersky.ru/