Безопасный интернет

Каждый родитель беспокоится о безопасности своего ребенка. Но многие забывают, что защищать детей нужно не только в реальной жизни, но и в интернете.

Несмотря на то, что современные дети легко осваивают технологии, согласно опросу, проведенному РОЦИТ на интерактивной площадке “Голос Рунета” при поддержке проекта “Школа Новых технологий” в мае 2016 г., большинство взрослых (около 70%) считают, что допускать детей к интернету следует не раньше 6 лет, т.е. с началом учебы в школе.

По словам детей, родители не уступают им в прогрессивности и делают интернет для детей доступным. Более 80% школьников 6-10 класса заявили, что родители разрешают им пользоваться интернетом, где бы они ни находились. Но, что интересно, несмотря на безграничные возможности, чаще всего дети выходят в Сеть из дома. Об этом заявляют 36% детей.

У большинства людей путешествие по всемирной паутине начинается с поисковика, но ни один из них не гарантирует предоставление вашему ребенку только безопасной информации. Что делать в такой ситуации?

1. Установить Безопасный режим.

Для этого необходимо создать отдельную учетную запись на сайте выбранной вами поисковой системы.

2. Использовать детские поисковики

Такие как Гогуль или Спутник.дети. Популярность этих ресурсов, несмотря на их безопасность и ориентированность именно на детскую аудиторию, сегодня крайне низкая. Ими пользуются лишь 2% опрошенных. Самыми востребованными браузерами среди детей являются Google Chrome (42%), Яндекс.Браузер (19%) и Safari (17%).

Оба этих способа имеют один недостаток - ребенок не всегда сможет найти актуальную и важную информацию по своему запросу, поэтому не стоит категорично запрещать ему пользоваться обычными поисковыми системами. В этой ситуации важен постоянный контроль со стороны родителей. Например, множество антивирусов сегодня имеют функцию родительского контроля, позволяющую наблюдать за тем, что ребенок делает в Сети.

Не менее важен вопрос, с каких устройств стоит позволять детям выходить в интернет, а с каких нет. С точки зрения родителей, самыми безопасными являются стационарный компьютер (22%), планшет (21%) и ноутбук (18%). При этом, у детей на первое место в пользовании выходит мобильный телефон или смартфон (38%).

В то же время в топ безопасных интернет-ресурсов, по мнению родителей, входят образовательные сайты (15%), сайты учебных заведений (13%), онлайн-переводчики (12%) и электронная почта (12%), т.е. в основном те ресурсы, которые предназначены для учебы и саморазвития ребенка.

В целях предотвращения проблем, перед тем, как допустить ребенка к Сети, родителям необходимо провести предварительную беседу с юным пользователем о том, что он может повстречать на просторах интернета. Помните, что в защиту Вашего ребенка в первую очередь входит Ваше личное общение с ним на тему кибербезопасности.

Абсолютное большинство родителей согласны с тем, что допускать ребенка в интернет бесконтрольно нельзя, уделять внимание безопасности детей в Сети необходимо вплоть до 18 лет. Об этом заявили около 40% опрошенных.

Для защиты юных пользователей родители применяют специальные средства защиты. В числе популярных - установка антивируса (65%), просмотр истории браузера (32%) и фильтры родительского контроля (30%). Дети стараются обезопасить себя в Сети, не только надеясь на родительскую помощь, но и самостоятельно: устанавливают антивирус (29%), не посещают сомнительные сайты (23%) и не переходят по незнакомым ссылкам (20%).

Как уже отмечалось, в вопросах безопасности детей в интернете важное место занимают доверительные отношения с родителями. Любопытно, что родители сегодня переоценивают

степень честности своих детей. Лишь 6% родителей считают, что не знают ничего о том, чем занимаются их дети в интернете, а по словам детей на деле - их сразу 14%.

Для того, чтобы оградить ребенка от противоправного контента (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы) Вам следует сформировать ряд легко выполнимых правил:

- • Договоритесь, чтобы ребенок сообщал Вам о нахождении нежелательной информации;
- • Расскажите, что не вся информация в интернете достоверная и приучите его советоваться с Вами по любому непонятному вопросу;
- • Расспрашивайте ребенка о том, какие сайты он посещал и какую информацию видел;
- • Включите программы родительского контроля, чтобы оградить ребенка от нежелательного контента;
- • Не будет лишним напоминание правил безопасности в Сети.

Помните, что чрезмерный контроль может усилить желание выйти за рамки дозволенного, поэтому доверительное и открытое общение с детьми зачастую гораздо эффективнее.

Около 80% детей когда-либо сталкивались с опасностями в интернете. Причем самая распространенная угроза - это компьютерные вирусы. О ней заявила сразу четверть опрошенных. Также весьма часто дети сталкиваются с опасностями в социальных сетях. 20% детей отметили, что им приходили сомнительные сообщения от незнакомцев. При этом, 3 из 5 детей сообщают своим родителям о тех опасностях, которые встречаются им в Сети.

Все чаще общению вживую дети предпочитают общение в социальных сетях. Более того, общение с друзьями в интернете является самым популярным занятием (24% опрошенных). Очевидно, что переход общения в виртуальную сеть может оградить ребенка от некоторых опасностей, как, например, уличные драки, но не стоит думать, что общение в Сети абсолютно безопасно и не может причинить никакого морального и физического вреда.

Одной из самых распространенных угроз, связанных с общением в Сети, является кибербулинг. Это форма запугивания, насилия и травли детей с помощью телефонов и интернета. Кибербулинг опасен не меньше, чем издевательства в привычном понимании, ведь “жертва” кибербулинга находится в большом психологическом напряжении, и не каждый ребенок сможет его вынести самостоятельно.

Кибербулинг включает в себя:

- • Анонимные угрозы – пересылка писем без подписи отправителя, содержащие угрозы, оскорбления, часто с использованием ненормативной лексики;
- • Преследование – рассылка “неприятных” писем своей “жертве” продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами ее жизни;
- • Использование личной информации – взлом электронной почты или страниц в социальных сетях для получения личной информации для шантажа или издевательств;
- • Флейминг – обмен эмоциональными репликами между агрессором (иногда их может быть несколько) и “жертвой” с целью получения удовольствия от нанесения оскорблений;
- • Хипплейпинг – видеозаписи с издевательствами, которые “заливают” на ресурсы, где их сможет увидеть большое количество пользователей. Такие ролики, естественно, “заливаются” без согласия “потенциальной жертвы”.

Для того, чтобы понять, попал ли Ваш ребенок под тяжелую руку кибер-хулиганов, следует обращать внимание на следующее:

- • Изменилось ли настроение ребенка в худшую сторону
- • Избегает ли он общественных мероприятий
- • Поменял ли он отношение к интернету
- • Сократилась ли частота использования мобильного телефона
- • Какова реакция на приходящие сообщения

- • Не удалял ли он свою страницу в социальной сети

Что делать если ребенок подвергся троллингу?

Спорить с таким кибер-хулиганом бесполезно, как и пытаться доказать ему, что он не прав. Помните, его задача – вывести ребенка из себя, так что молчание принесет ему больше разочарования, чем обидные ответы. Вернее всего просто “забанить” тролля, внеся его в черный список или написав модератору сайта. Важно также объяснить ребенку, что любые нападки и оскорбления тролля не стоит воспринимать всерьез.

Не оставляйте ребенка с его проблемами в сети в одиночку, ведь виртуальная проблема несет за собой реальные переживания.

Мошенники не отстают от хулиганов и также активно разворачивают свою деятельность в Сети. Зачастую “жертвами” кибер-мошенников становятся и дети. Целью кибер-мошенничества является причинение материального или другого ущерба, путем похищения личной информации (номера банковских счетов, логинов и паролей, кодов, паспортных данных и др.).

Объясните ребенку, что сайты, запрашивающие слишком много информации о пользователе при совершении покупок в Интернете (данные счетов, пароли, домашние адреса и номера телефонов), могут оказаться мошенническими. Расскажите, что администратор или модератор сайта никогда не станет требовать полные данные счетов, пароли или пинкоды. Проинформируйте ребенка об основных методах мошенничества, расскажите ему, как можно отличить официальный и надежный сайт от мошеннического, и приучите его советоваться с вами при желании совершить покупку в Сети.

Лучшим вариантом будет взять процесс совершения покупки на себя, или сделать так, чтобы он шел в Вашем присутствии и под Вашим контролем. Так Вы будете в курсе того, на что и как Ваш ребенок тратит деньги, и сможете предостеречь его от кибер-преступников.

Не стоит упускать из виду и смартфон ребенка. Современные гаджеты помимо неоспоримой пользы могут принести и большой вред. Кибер-преступники с радостью взламывают и запускают вирусы на смартфонах (например, они могу украсть деньги с телефонного счета).

Вот несколько правил, которым стоит следовать, чтобы сохранить безопасность своего смартфона и смартфона Вашего ребенка:

- • Установите пароль, чтобы личная информация не попала к посторонним лицам;
- • Не стоит подключаться к непроверенным wi-fi точкам, особенно открытым, так как их легко могут использовать для сбора отправляемых данных, в том числе и паролей;
- • С помощью специального приложения Вы можете контролировать устройство удаленно, даже если оно украдено;
- • Не стоит скачивать неизвестные приложения: пользуйтесь только официальными магазинами AppStore, GooglePlay и Windows Market, проверяйте запрашиваемые приложением разрешения.
- • Не обязательно создавать отдельный аккаунт для Вашего ребенка в магазине приложений. Разные производители дают возможность подключить одного и более членов семьи к одной банковской карте – так Вы сможете контролировать, что собирается купить Ваше чадо.

Теперь поговорим о пользе смартфонов для Вас, как заботливого родителя. Например, с помощью смартфона можно найти потерявшегося ребенка или помочь ему найти дорогу домой, если он заблудился. Есть и другие преимущества, которые Вы получаете, покупая ребенку смартфон:

Картографические сервисы.

Установите приложения с картами на телефон ребенка, с их помощью он сможет определить свое местоположение. Не редко картографические сервисы снабжены дополнительной информацией, например, расположением различных организаций, в том числе постов милиции и поликлиник, остановок, железнодорожных станций, торговых центров. Но самым

важным свойством, которым обладают электронные карты, - это способность проложить маршрут от пункта А в пункт Б. Не забудьте также убедиться, что ребенок знает адрес дома.

Поисковые сервисы.

Обычный поисковик также способен помочь потерявшемуся ребенку, с его помощью можно найти организации, которые находятся поблизости, расписание общественного транспорта и другую важную информацию. Еще поисковик нужен для нахождения специализированных сайтов, на которых люди помогают с поиском детей. Ребенок может найти форум поискового отряда и дать знать, что он потерялся.

Программы по поиску телефона.

Вы можете сами найти пропавшего ребенка, если установите ему на телефон программу, которая будет показывать Вам его местоположение;

Коммуникационные сервисы.

Коммуникационных сервисов в Интернете сейчас очень много – от чатов и онлайн мессенджеров до социальных сетей, они могут оказаться ценным альтернативным средством коммуникации. Родителям следует самим быть, что называется «в тренде», чтобы иметь возможность контактировать со своими детьми по разным каналам. С помощью мессенджеров Вы можете передавать фотографии, геопозицию и другие данные – все это упростит для ребенка процесс поиска дома в случае, если он потеряется.

Специализированные площадки волонтеров-поисковиков.

Это площадки интернет-объединений «Поиск пропавших детей» и «Лиза Алерт», чьи отделения или партнеры функционируют по всей стране. В некоторых регионах существуют свои собственные поисковые отряды, обладающие развитой сетью волонтеров и отличным техническим оснащением (например, в Ярославле). Дать о себе знать через такие площадки имеет смысл, если ребенок находится в критической ситуации или не может связаться с родителями или родственниками.

Смартфон, покупаемый ребенку, должен обеспечивать максимальную безотказность и возможность поддерживать все технологические функции, необходимые для обеспечения безопасности ребенка. «Укомплектовать» смартфон сервисами, которые понадобятся детской безопасности, необходимо самому родителю, не забыв при этом научить ребенка пользоваться всем, что вы установили.

При выборе смартфона для ребенка рекомендуется обратить внимание на следующий функционал:

- • Телефон не должен быть рассчитан на работу только с одним оператором (может возникнуть такая ситуация, что придется поменять Сим-карту);
- • Не следует полагаться только на сенсорный экран смартфона, лучше выбрать телефон, где основные функции – приема и сброса звонков и вызова меню – продублированы «обычными» кнопками;
- • Телефон должен обладать большим объемом памяти или возможностью установки дополнительной карты памяти, для того чтоб на нем свободно могли загрузиться все необходимые приложения;
- • Проблемой современный смартфонов является быстрый разряд аккумуляторной батареи поэтому стоит рассматривать модели с большим объемом батареи или носить с собой зарядное устройство либо дополнительный блок питания.

Для Безопасности ребенка в Сети стоит следовать нескольким простым правилам:

1. 1. Говорите с ребенком об интернете. Расскажите основные правила и о последствиях их нарушения. Самое главное: добиться того, что бы ребенок в любой непонятной ситуации обращался за помощью к родителям;
2. 2. Пользуйтесь интернетом и смартфоном вместе с ребенком. Это хороший способ показать, что возникающие вопросы лучше всего решать вместе;

3. 3. Рассказывайте больше о сайтах и сервисах в интернете, поговорите об его интересах и о том какие страницы можно посещать.
4. 4. Научите бережно относиться к паролям. Донесите до детей, что их нельзя передавать другим людям, за исключением родителей. Убедитесь, что у ребенка вошло в привычку выходить из своих аккаунтов, если он пользовался чужим устройством;
5. 5. Научите использовать настройки конфиденциальности, объясните, что следует рассказывать, а, что нет;
6. 6. Обращайте внимания на возрастные ограничения сайтов. Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи старше 13 лет;
7. Расскажите о том, что за слова. сказанные в интернете, ребенок несет такую же ответственность, как и в реальной жизни;
8. Привлекайте к обсуждению этой темы других взрослых, знакомых и коллег, компетентных в этом вопросе.
9. Используйте антивирус и регулярно обновляйте его;
10. Научите ребенка не открывать вложения и не принимать файлы от неизвестных людей в электронной почте.