Советы для родителей

Детская безопасность – ответственность взрослых.

Не забывайте про периодический контроль виртуальных друзей и сообществ, в которых ребенок ведёт деятельность. Если тематика сообщества не понятна, попросите ребенка ее прояснить, поищите информацию в Интернете – даже картинки и символику сообществ можно проверить через сервис "Поиск по картинке", предоставляемый компаниями "Яндекс" и "Google". Также внимания заслуживают сервисы, позволяющие искать скрытых и скрывающихся друзей. Если ребенок что-то скрывает, то именно это должно заинтересовать родителей.

Займитесь саморазвитием. Особенности виртуальной жизни детей и подростков родителям нужно постоянно познавать и быть в курсе актуальных интернет-угроз.

Постоянно наблюдайте за поведением детей и ведите с ними открытый диалог. Ключевую роль в обеспечении безопасности детей играет общение. Разговоры о безопасности, страхах и проблемах намного эффективнее наказаний. Доброжелательная атмосфера в семье и открытый диалог способствуют успешному развитию ребенка.

Станьте другом своему ребенка. В прямом и переносном смысле. Добавьтесь в друзья к своему ребенку в социальной сети, где у него есть аккаунт. В случае успешного добавления (а для этой операции лучше завести дополнительный анонимный аккаунт) вы сможете видеть, что он публикует, с кем общается, кому симпатизирует. Круг знакомств в виртуальном пространстве не менее значим, чем дворовая компания.

Рекомендации по техническому контролю:

- Регулярно обновляйте антивирус и программу родительского контроля;

- Используйте инструменты родительского контроля. Функции родительского контроля есть как в браузерах, так и в антивирусных программах. Например, в ESET NOD32 Smart Security и Kaspersky Internet Security предусмотрен модуль «Родительский контроль». Кроме того, вы можете выбрать специальное мобильное приложение – ESET NOD32 Parental Control для Android. Существуют подобные инструменты для игровых приставок, таких как NintendoWii, Playstation и Xbox 360. 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);

- Настройте использование https. Убедитесь, что ваш ребенок открывает сайты с защищенным протоколом https (наименование протокола отображается в адресной строке браузера). Это позволит избежать перехвата информации – данные передаются в зашифрованном формате, который не распознают вредоносные программы. Посоветуйте детям-подросткам использовать эти настройки и при доступе к соцсетям через публичный Wi-Fi;

- Проверьте настройки веб-камеры и убедитесь, что она отключена или закрыта, если в данный момент не используется;

- Создайте для ребенка учетную запись с правами пользователя – это позволит вам эффективно контролировать его онлайн-активность. Учетная запись с правами администратора должна использоваться только взрослым;

- Настройте параметры безопасности для социальных сетей. Параметры безопасности в соцсетях, установленные по умолчанию, не гарантируют безопасность. Рекомендуется посвятить немного времени их правильной настройке и проверить, какая информация находится под угрозой утечки;

- Используйте надежные пароли. Напомните детям, что пароли нельзя передавать даже лучшим друзьям;

- Скачивайте программы и мобильные приложения только из проверенных источников;

- Не разрешайте детям публиковать в интернете личную информацию. Запомните и объясните детям, что конфиденциальная информация никогда не запрашивается по электронной почте или в чате;

- При оскорблении ребенка в сети не удаляйте сообщения агрессора, история сообщений послужит доказательством акта воздействия;

- Объясните ребенку, что далеко не вся информация в интернете достойна доверия. Просматривайте историю посещения им сайтов. Если вы обнаружите, что история подчищена, найдите повод, чтобы с ребенком поговорить;

Все, что попало в интернет, останется там навсегда. Объясните детям, что информация, проиндексированная поисковыми системами, навсегда останется в сети. Хуже того, после публикации пользователь теряет контроль над своими данными, любой может использовать и распространять эту информацию. Пусть дети возьмут за правило никогда не публиковать фотографии, статусы и другой контент, который они не хотели бы показывать родителям или родственникам. Это распространяется на соцсети, мессенджеры, блоги и другие сервисы.

Несколько полезных советов для обеспечения родительского контроля и надзора, создающего безопасность детей в Интернете:

Совместное времяпрепровождение в Интернете побудит ваших детей обращаться к вам с любыми вопросами и дилеммами, но, что более важно, позволит вам регулярно обучать их правильному и безопасному поведению в Интернете;

Здравый смысл и логика подсказывают нам — расположение компьютера, которым пользуется ваш ребенок в зоне общего доступа, в зоне видимости взрослых, позволяет родителям контролировать время пользования устройством, а также сферу онлайн-интересов ребенка. Может быть, такое расположение компьютера не очень нравится всей семье, но это все же лучше, и, главное, безопаснее, чем установка устройства в детской комнате за закрытой дверью. Этот совет также актуален для любого другого устройства, имеющего доступ к Интернету. Главный совет — не оставляйте детей наедине с Интернетом без должного присмотра взрослыми членами семьи и без возможности визуального контроля контента;

Используйте закладки, чтобы позволить вашим детям иметь простой и легкий доступ к любимым сайтам;

Если дети часто самостоятельно посещают игровые сайты или некоторые образовательные сайты, отключите функцию покупки и регулярно проверяйте счета вашей кредитной карты и телефона на предмет неизвестных расходов по счету;

Будьте внимательны, моментально реагируйте на любое изменение поведения ваших детей, выходите на разговор о том, что они видели и слышали в Интернете, что их удивило или напугало;

Будьте бдительны в отношении любых признаков, которые могут указывать на то, что ваш ребенок подвергается нападению со стороны онлайн-злоумышленника, найдите ответы на следующие типы вопросов:

- проводит ли ребенок слишком много времени в Интернете, особенно ночью?

- получает ли ребенок звонки по телефону от людей, которых вы не знаете?

- не приходят ли по почте нежданные подарки?

- часто ли ваш ребенок моментально выключает компьютер или звук, когда вы входите в комнату?

- не заметили ли вы отчужденности в отношениях с ребенком и/или нежелание говорить о его онлайн-деятельности?

Что делать, когда дети становятся старше?

Родители уже не могут поддерживать тот же уровень контроля и надзора, что практиковали прежде, дети все чаще находятся за пределами досягаемости взрослых.

Естественно, с возрастом детям хочется получить больше конфиденциальности и независимости. Это ответственный момент для родителей. Нужно найти способ и возможность поговорить с ребенком, чтобы предостеречь от пользования теми сайтами и приложениями,

которые не подходят ему по возрасту и могут ухудшить безопасность детей в Интернете.

Предупредите своих детей, если вы не сделали этого раньше, о рисках и угрозах интернет контактов, особенно, если речь идет о людях, которых дети раньше не знали. Объясните ребенку, что в виртуальном мире интернета все не совсем так, как кажется на первый взгляд, и в сети людям намного проще обмануть, чем в реальной жизни, когда приходится смотреть глаза в глаза.

Объясните ребенку необходимость применения паролей для защиты личных данных от кражи.

Поощряйте критическое мышление.

Заложите долю здоровой критики и неоспоримой логики, здравого смысла и взаимного уважения к мнению другого в ваши разговоры с детьми, но не забывайте об осторожности и такте.

Научите ваших детей распознавать и блокировать нежелательные контакты, возникающие по телефону, электронной почте, в текстовых сообщениях, в социальных сетях или онлайн-играх. Объясните своим детям, что они должны понимать, что то, чем они делятся в сети, могут увидеть и прочитать совершенно другие люди, о существовании которых дети даже не подозревали.

Вы также можете рассказать детям о пользе цифрового следа, который может сохраниться в интернете вечно. Хороший цифровой след может сослужить добрую службу в будущем, когда дети станут взрослыми. Он будет свидетельствовать об их талантах, достижениях и творческом потенциале.

Настройте свой интернет так, чтобы обеспечить безопасность детей в Интернете

Мы уже упоминали об использовании фильтров и мониторинге взрослыми использования Интернета детьми. Вы также можете

рассмотреть другую возможность — включить безопасный поиск Google на всех устройствах, которые использует ваша семья.

Что вы можете сделать в самом браузере, так это включить родительский контроль в таких службах потоковой передачи, как YouTube, Netflix и AppleTV, а также установить программное обеспечение, которое фильтрует контент или позволяет выбирать, в какое время устройства можно использовать, а в какое – нельзя. Это действие аналогично правилу Стива Джобса об ограничении времени, проведенного нашими детьми в виртуальном мире.

Используйте в своем браузере уже установленные опции, такие как история поиска, узнайте их адреса электронной почты и пароли, чтобы вы могли отслеживать активность. Многие устройства используют облачное хранилище, например Google Drive или Apple iCloud, для хранения таких данных, как документы, фотографии или видео. Доступ к ним также можно контролировать.

Ознакомьте детей с функциями GPS и регистрации, поскольку именно они определяют местонахождение вашего ребенка, когда те находятся на улице, их лучше ограничить или навсегда отключить.

Учитывайте риски пользования социальными сетями

Иметь друзей и общаться с другими людьми очень важно для детей и молодежи. В наши дни коммуникации могут быть разными и для разных целей: для поддержания связи с семьей, для ведения блога в Instagram… Многие используют WhatsApp, Snapchat или Viber для общения с друзьями. Конечно, приложений, которые включают моментальный обмен сообщениями между людьми, очень много, но все они представляют определенную степень опасности, особенно в ситуациях, когда дети обмениваются сообщениями с людьми, которых они не знают в реальной жизни и которым не стоит доверять.

Опять же, используйте здравый смысл, логику, предупреждайте детей о том, что сообщения и фотографии, которыми люди обмениваются, могут быть просмотрены и получены не теми, кому адресованы, а совсем другими людьми. Научите их использовать и настраивать параметры конфиденциальности, чтобы их профиль могли видеть только знакомые, и почаще сами проверяйте эти параметры.

Научите детей, как сообщать о злоупотреблениях или недопустимом контенте в службу социальных сетей или другое агентство, особенно когда речь идет о недопустимом контенте. Убедитесь, что дети и подростки понимают риски, связанные с отправкой или пересылкой сексуальных текстов, изображений или видеороликов (по признаку пола), и вред, который это может причинить им и другим.

Правда в том, что, нравится нам это или не нравится, но дети должны это знать. Им нужно учитывать ваши взгляды на вещи и вашу точку зрения, а также их аргументированное обоснование. Это обеспечит безопасность детей в Интернете и придаст уверенности родителям в том, что, даже без родительского контроля, дети не наделают катастрофических

ошибок. Родителям необходимо объяснить своему ребенку, что отправка сексуальных или обнаженных фотографий людей моложе 18 лет, как своих, так и чужих, может быть классифицирована как хранение и распространении детской порнографии. А вот это уже будет иметь более серьезные последствия.

Игры и приложения

Игры и приложения изначально предназначены для саморазвития и самообразования. Как правило, они развивают различные полезные навыки, стремление к победе, при этом доставляя массу удовольствия. Их можно скачать из интернета, причем, многие из них совершенно бесплатно. Даже маленькие дети могут проводить много времени, играя в них.

Лучшие приложения – это те, в которых дети могут экспериментировать и испытывать свои собственные идеи, создавая рисунки или музыку. Некоторые приложения не столько развивают, сколько занимают свободное время ребенка. В бесплатных приложениях часто размещено много рекламы и внедрена возможность покупок внутри приложений. Это могут быть как настоящие покупки, так и виртуальные, но любые могут стать «шоком» для родителей. Маленьким детям очень сложно отличить рекламу от игры.

Первое, что должен сделать родитель, это убедиться, что в игровом приложении нет неприемлемого содержания, насилия, сексуальных образов, грубых выражений или азартных игр.

Большинство родителей никогда не будут поощрять своих детей к азартным играм. Однако симуляция азартных игр может быть встроена в детские игры, и некоторые родители даже не замечают этого.

Воздействие симулированных азартных игр в детском возрасте может повысить вероятность того, что дети будут играть в азартные игры в старшем возрасте. Они могут думать, что азартные игры основаны на навыках, а не на случайности. Они часто верят, что чем больше они играют, тем лучше результат они получат, как и в других играх. Это усиливается, когда в виртуальных играх легче выиграть, чем в реальной игре.

Что можно сделать с этим? Только снова объяснять, обсуждать, включать здравый смысл и логику и не жалеть времени на это. Помогите детям осознать риски азартных игр и понять, как это работает. Еще один совет: избегайте играть в азартные игры на виду у детей, не устраивайте азартных игр в кругу семьи.

Не позволяйте детям играть в жестокие игры с насилием

Родители должны уметь поддерживать связь со своими детьми, не позволять им отдаляться, стараться убеждать собственным примером, например, никогда не играть в жестокие игры в присутствии ребенка. Дети быстро распознают двойные стандарты. Возможно, вам нужно проявить твердость, ограничивая доступ к жестоким играм, так как некоторым детям они нравятся больше всего.

Хотя связь между игрой в жестокие игры и проявлением насилия в реальной жизни зачастую не прослеживается, недопустимая графика и темы для взрослых могут по-прежнему находить у вашего ребенка эмоциональный отклик, вызывая ночные кошмары, страхи и беспокойство.

Подростки часто увлекаются многопользовательскими онлайн-играми. Они могут играть с друзьями и знакомиться с новыми людьми со схожими интересами в любой точке мира. В этих случаях родители должны напоминать своим детям об осторожности при обмене личной информацией, следить за тем, в какое время они играют. Некоторые игры происходят в разных часовых поясах, что может означать, что подросток играет в то время, когда он должен спать. А ведь школу никто не отменял,

Когда дети и подростки проводят много времени за играми, они тратят меньше времени на выполнение более медленных и более трудоемких задач, таких как чтение книг или выполнение домашних заданий.

Дружите со своими детьми, тратьте на них свое время, обучайте их и контролируйте

Не ведите себя, как заезженная пластинка, повторяя одно и то же каждый день. Найдите подходящее время, располагающее к беседе с вашими детьми. Лучшим вознаграждением за потраченное вами время станет уверенность в том, что ваши объяснения помогут обеспечить безопасность детей в Интернете, что ваши дети не совершат непоправимых поступков, которые могут повлиять на их жизнь или на жизнь членов вашей семьи.

Выполняйте сами то, к чему призываете детей. Дети понимают столько же, а в данном случае (использование современных коммуникационных технологий) иногда больше, чем взрослые. Если дети увидят, что вы не следуете своим собственным правилам, тому, чему вы их учили, например: используете свое настоящее имя в социальных сетях, играете в азартные онлайн игры, что вы не осторожны со своей личной информацией и IP, то это заставит их потерять веру в вас и перестать следовать вашим наставлениям.