Как уберечь своих детей от деструктивных сайтов в интернете.

(руководство для родителей)

Наши дети - главная ценность в жизни. В наше время защищать детей от различных неприятностей становится непростой задачей. Современные телефоны и планшеты становятся все сложнее. В связи с этим родителям необходимо постоянно совершенствовать свои знания технологий, чтобы помогать детям правильно использовать гаджеты. Данное руководство призвано помочь родителям обеспечить безопасное использование детьми мобильных устройств и интернета.

Чем старше становятся дети, тем больше новых проблем появляется. Родители учат своих детей и учатся сами. Вам кажется, что дети знают о компьютерных технологиях больше, чем вы? Вы не одиноки, многие родители думают точно так же. Нынешние подростки родились буквально со смартфоном в руках, в то время как многие взрослые познакомились с мобильными устройствами уже в сознательном возрасте. Но это не делает ребенка главным техническим специалистом в доме. Даже если ребенок умеет пользоваться интернетом, это не означает, что он осознает последствия каждого действия в Глобальной компьютерной сети Интернет. Родителям нет необходимости разбираться в цифровом мире лучше ребенка. Но вы должны быть всегда готовы к моменту, когда ваш ребенок найдет в Сети что-то незнакомое и будет нуждаться в разговоре с кем-то более опытным. Важно вовлечь ребенка в диалог. Поэтому в семье так важна доверительная атмосфера, где дети могут свободно задавать вопросы и получать исчерпывающую информацию в доступной форме.

Сегодня полный запрет доступа детей к технологиям не решает проблему безопасности. Современные технологии - важная часть повседневной жизни, необходимая для развития. Вместо того чтобы устанавливать ограничения, поговорите с детьми о безопасности и организуйте взаимодействие ребенка с гаджетами. Многие вышеупомянутые риски актуальны и для взрослых, поэтому рекомендованные меры предосторожности стоит применять в любом возрасте.

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 это пояснить, 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 нам, родителям, нужно постоянно познавать и быть в курсе актуальных интернет-угроз Кроме этого, в регионе создан удобный и бесплатный инструмент для саморазвития и консультаций -«Родительский форум».

Целесообразно обращаться к специалистам-психологам, а зачастую и к психиатрам. Уже первый неправильный тактический шаг может навредить: после этого усиливается воздействие на ребенка, создается агрессивный настрой против родителей, появляются угрозы и попытки склонять к совершению побега из дома или к самоубийству.

Постоянно наблюдайте за поведением детей.

Не забывайте, что любые попытки приблизиться к ребенку он будет обсуждать со своими идеологами в соцсетях. Ему будут пояснять примерно так: «не слушай родителей, слушай нас».

Постарайтесь вернуть ребенка в семью. Родительская любовь и тепло могут в этом помочь.

Рекомендации по техническому контролю.

1. Используйте инструменты родительского контроля. Функции родительского контроля можно использовать как в браузерах, так и в антивирусных программах. Например, в ESET NOD32 SmartSecurity, KasperskylntemetSecurity предусмотрен модуль «Родительский контроль». Кроме того, вы можете выбрать специальное мобильное приложение — ESET NOD32 ParentalControl 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:\Usere\User\AppData\Local\Microsoft\Windows\Temporary IntemetFiles в операционной системе).

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

3. Не удаляйте сообщения агрессора, история сообщений послужит доказательством акта воздействия.

4. Объясните ребенку, что далеко не вся информация в интернете достойна доверия.

5. Ведите с ребенком открытый диалог. Ключевую роль в обеспечении безопасности детей играет общение с ними. Разговоры о безопасности, страхах и проблемах намного эффективнее наказаний. Доброжелательная атмосфера в семье и открытый диалог способствуют успешному развитию ребенка.

6. 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.

7. Не рекомендуется создавать для ребенка учетную запись с правами администратора.

8. Настройте использование https. Убедитесь в том, 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-подроспсам использовать эти настройки и при доступе к соцсетям через публичный Wi-Fi.

9. Используйте надежные пароли. Напомните детям, что пароли нельзя передавать или давать на время даже лучшим друзьям.

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

Тактические подсказки для родителей

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

2. Не забывайте регулярно обновлять антивирус и программу родительского контроля.

3. Просматривайте историю посещения сайтов ребенком. Если вы обнаружите, что история подчищена, найдите повод, чтобы с ребенком поговорить.

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

5. Проверьте настройки профиля ребенка в соцсетях. Открытый доступ к профилю может подвергнуть ребенка риску.

6. Не переходите по подозрительным ссылкам

7. Скачивайте программы и мобильные приложения только из официальных источников

8. Используйте комплексные антивирусные продукты и решения.

9. Избегайте заполнения сомнительных форм с персональными данными в Сети.

10. Не открывайте файлы от неизвестных отправителей.