Памятка для родительского контроля

Моему ребенку **7-8 лет** Как защитить его от опасностей в интернете

1. Запустите программу лаунчер на свой телефон. Лаунчер спросит у вас, какие программы можно ребенку показывать, а какие нельзя, и сработает защитной оболочкой.

2. Используйте детские поисковые машины. Они помогут увидеть список просмотренных ссылок.

3. Блокируйте нежелательные контенты. Установите бесплатные фильтры нежелательных запросов и сайтов, поисковых запросов в YouTube, контроль используемых игр и приложений, контроль продолжительности работы. Дополнительные возможности платных версий – история поисковых запросов и гаджета по расписанию, контроль заряда батареи и активности «ВКонтакте» и Facebook, отчет об интернет-активности ребенка, немедленные уведомления при вероятных опасностях, GPS-трекеры.

4. Требуйте от ребенка соблюдения временных норм нахождения за гаджетами. Всегда говорите о том, что вы наблюдаете за ним не потому, что вам этого хочется, а потому, что вы беспокоитесь о его безопасности и готовы прийти ему на помощь в любую минуту.

5. По возможности установите компьютер в общей комнате. Так легче контролировать ребенка и ненавязчиво присматривать за ним. У ребенка не будет ощущения, что за ним ведется постоянный контроль, а родители будут знать, какие сайты их дитя посещает.

6. Помните о том, что в возрасте 7-8 лет дети обладают очень сильным чувством семьи, родители являются авторитетом для них, они доверяют им и не сомневаются в любви и поддержке с их стороны. И в то же время дети очень заинтересованы игрой в сети, посещают разные сайты, постоянно ищут какую-то информацию.

Памятка для родительского контроля

Моему ребенку **9-12 лет** Как защитить его от опасностей в интернете

1. Поставьте компьютер в ту комнату, где чаще всего бывает ваша семья.
2. Создайте совместно с ребенком домашнее правило пользования интернетом и требуйте его выполнения.
3. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
4. Определите временные нормы нахождения за компьютером и требуйте их соблюдения. Создайте ограниченную учетную запись для работы на компьютере.
5. Имейте доступ к почте, чтобы предостеречь детей от общения с незнакомцами.
6. Не ленитесь наблюдать за своим ребенком, когда он пребывает за компьютером. Рассказывайте отом, что вы готовы ему помогать при возникновении любой опасности и всегда беспокоитесь о нем.
7. Договоритесь с ребенком о том, что он не будет загружать программы без вашего разрешения. Создайте список сайтов и позволяйте заходить только на те, которые вы обговорили с ним.
8. Предупредите ребенка, чтобы он не соглашался на личные встречи со своими друзьями поинтернету. Всегда интересуйтесь о друзьях ребенка в сети.
9. Приучите никогда не выдавать любую личную информацию через электронную почту, регистрационные формы, чаты.
10. Проведите беседу о порнографии, сплетнях, угрозах и различных хулиганствах в сети Интернет. О любых угрозах попросите его сообщать вам.
11. Дети в этом возрасте получают много информации из интернета и хотят еще больше прочесть, усль шать, увидеть, посешая разные сайты. Доступ к нежелательной информации легко блокируется при помощи средств родительского контроля.

Моему ребенку **13-18 лет** Как защитить его от опасностей в интернете

1. Пользуйтесь фильтрами контента.
2. Спросите, какими чатами и сайтами пользуется подросток.
3. Настраивайте своего ребенка не общаться в приватном режиме и советуйте использовать чат, в котором есть модератор. Он может запретить нецензурные слова, спам, сообщения.
4. Без вашего разрешения ребенок не должен загружать программы, так как может случайно появиться вирус, нежелательные сайты или чаты.
5. Скажите ребенку, что вы обязательно должны знать о любых угрозах или тревогах, связанных с интернетом.
6. Объясняйте постоянно, что нельзя использовать интернет для хулиганства, распространения угроз, порнографии, сплетен.
7. Предупредите о недопустимости выдавать в интернет свой электронный адрес, использовать почтовые фильтры и отвечать на письма от незнакомцев.
8. Спрашивайте, с кем подросток общается через мессенджеры – приложения для мгновенного обмена текстовыми сообщениями, фотографиями и аудиозаписями.
9. Учите уважать других пользователей в интернете, так как даже в виртуальном мире действуют правила хорошего поведения.
10. Расскажите о том, что по закону дети не могут играть в азартные игры. С сетевыми азартными играми связано много проблем и возможных рисков.
11. Воспитывая детей-подростков, не забывайте о том, что интернет-безопасность – это кибербезопасность и компьютерная безопасность браузера и сети, а также правильное поведение в сети.

Памятка для педагогов и родителей

«АКТИОН» Образование

Виды кибераггрессии

Кибersталкинг - использование интернета для домогательства или бесконечного преследования человека, группы или организации. Например, похищение личности, вандализм, вымогательство, секс или сбор информации, которая используется для запугивания или домогательств. Этим занимаются знакомые и незнакомые люди. Они анонимно вовлекают незнакомых людей онлайн.

Троллинг - нагнетание участником общения через компьютерную сеть гнева путем скрытого или явного принижения, оскорбления или явного задирания, нарушая правила сайта. Человек, который нарушает этику онлайн-взаимодействия, называется тролль. Он размещает в сети провокационные сообщения, чтобы вызвать негативную эмоциональную реакцию или конфликты между участниками.

Хейтинг - полноценная травля, которая часто происходит с публичными людьми. Массовые негативные комментарии и оскорбления от группы людей идут в адрес одного человека.

Диссинг - в сети распространяется информация, которая может опорочить человека. Начинается травля в соцсетях: оскорбительные посты, создаются фотожабы, сфабрикованные скриншоты, придуманные тексты сообщений с недостоверной информацией.

Флейминг - «спор ради спора». Поводом могут стать неудачные шутки, насмешки, необоснованная критика. В сети флеймеры будут писать вульгарные сообщения, оскорбления, комментарии унизительного содержания. Провокация с их стороны намеренная, спокойная, продолжительная, чтобы вывести жертву из себя. Например, вначале предлагается сыграть в какую-либо психологическую игру, а потом специально высмеивают, подлавливая на мелочах.

Аутинг - выкачивание любой личной информации. Публикуются и разглашаются персональные данные: публикации о доходах, расходах, сведения об отдыхе, местонахождении членов семьи, интимные фотографии. Информация ворується из личных гаджетов, которую могут опубликовать без разрешения и с угрозами.

Хеппислепинг - в переводе с англ. «счастливое хлопанье, радостное избиение». Это название закрепилось за видеороликами реальных сцен насилия.

Бойкот – социальная изоляция. Поводом может служить любая мелочь, например, человек, общающийся в сети, не знает сленга, слушает «не ту музыку», не так говорит, не то пишет. Начинается игнорирование, исключение жертвы из всех деловых или неформальных бесед, общих переписок.

Харассмент – домогательства от реальных знакомых и от фейков (фейк, от англ. слова fake – фальшивка, любая недостоверная информация, размещенная в интернете, СМИ, медиа). Выражается в кибератаках или целенаправленных домогательствах с сексуальным подтекстом. Злоумышленник прибегает к шантажу и вымогательству, угрожает отправить переписку или снимки всем контактам, требует денег.

Домогательство – очень опасный вид травли в интернете. Детям рассылают личные сообщения, в которых вь смеивают их жизнь, внешний вид, семью, угрожают и оскорбляют. Могут предложить поиграть в психологическую игру, например, спрашивают о чем-либо, а потом подлавливают на ответах, говорят, что они глупые и неправильные.

Груминг – появляется незнакомый человек в сети, втирается в доверие к ребенку, долго доброжелательно с ним общается, пытается всеми силами подружиться. Этот человек просит выслать фото, личные истории определенного характера, а потом начинается шантаж – грозится рассказать обо всем родителям и опубликовать все фото.

Секстинг – в сети пересылаются личные фотографии, сообщения интимного содержания, видео. Существуют два вида: добровольный, по обоюдному согласию, и недобровольный, когда адресат получает нежелательное сообщение.

Фишинг – вь манивание паролей от личных страниц с различных сервисов, чтобы получить доступ к персональной информации и сделать спам-рассылки. Например, крадут аккаунты игровой платформы Steam, где распространяются игры и есть социальная сеть. Пользователь перешел случайно по какой-то ссылке, и компьютер заблокировался. Приходит сообщение с предложением разблокировать компьютер за деньги, но никакой гарантии на восстановление нет.

Остракизм – «отчуждение, изоляция». Многие дети хотят быть включенными в какую-либо группу. Исключение из группы воспринимается впоследствии ими как социальная смерть.