

Защити своих детей в сети «Интернет»

Нежелательный контент. Интернет - хищники. Опасные вирусы и вредоносное ПО. Это лишь малая часть причин, по которым родители во всем мире озабочены безопасностью детей в интернете. Безопасность в киберпространстве ставится во главе угла, когда речь заходит о знакомстве детей с цифровыми устройствами: смартфонами, планшетами и компьютерами.

Всем известно, что интернет полон пугающей информацией, и некоторые родители, чтобы оградить детей от подобного контента, запрещают им пользоваться интернетом, до тех пор, пока они не достигнут определенного возраста. Однако существует целый ряд различных программ, установив которые, можно обеспечить безопасность несовершеннолетних в сети. Сейчас, когда информационные технологии общедоступны, со стороны правительства принимаются серьёзные меры по обеспечению безопасности всех граждан, обращающихся к ресурсам всемирной паутины - включая несовершеннолетних.



Законодательство в сфере интернет - безопасности в разных странах мира может незначительно отличаться, но проблемы, с которыми оно борется, имеют сходное происхождение. Наряду с тем, что интернет предоставляет детям быстрый и удобный доступ к полезной информации, а также к развлекательным материалам, все же пользование интернетом сопряжено с огромными рисками.

Ниже представлены некоторые из опасностей, которые подстерегают ребёнка онлайн.

Нежелательный контент

Сидя в интернете, ребёнок может с легкостью натолкнуться на нежелательный контент - особенно если на устройстве не установлены специальные, ограничивающие данные материалы, программы. Нежелательный контент, такой как, например, сцены насилия, порнографии и другие материалы, вызывающие страх, ужас, панику и т.д. у ребёнка, может нанести вред здоровью и развитию. Если ребёнок продолжительное время подвергается воздействию таких материалов, его психическое здоровье серьёзно страдает.



Интернет - Хищники

Одной из самых больших опасностей в сети является встреча ребёнка с интернет - хищником. В качестве своих жертв эти преступники намеренно выбирают наиболее уязвимые слои населения - в том числе детей. Особая опасность состоит в том, что преступники способны без особого труда скрыть свою подлинную личность - это затрудняет их поиски в реальной жизни. Спрятавшись за фальшивым лицом, интернет - хищники, с помощью онлайн платформ - особенно часто это происходит в социальных сетях - склоняют детей к незаконным действиям, в том числе и сексуального характера.



Киберпреступность

За годы существования интернета проблема киберпреступности становится только острее. Находясь в сети, ребёнок может стать жертвой преступника, даже не догадываясь об этом. Все это может привести к краже личной информации пользователя, включая имя, адрес, дату рождения, текущее местоположение и т. д. Но самое страшное, если для выхода в интернет ребёнок использует одно из устройств родителей, например, ноутбук - в этом случае может произойти похищение личных данных, которые в дальнейшем могут быть легко скомпрометированы.

Кибербуллинг (киберзапугивание)



Кибербуллинг - остро - социальная проблема. Исследования показывают, что в настоящее время более половины подростков становятся жертвами травли в интернете; еще столько же выступает в качестве преследователей. Социальные сети образуют благоприятную среду для киберхулиганов, чье онлайн поведение несет в себе опасность. Риск подвергнуться травле в интернете сейчас очень высок, поэтому родителям нужно следить за тем, что происходит с их ребёнком в социальных сетях, а также объяснять, что он может поделиться с родителями любой проблемой, какой бы она ни была, особенно если ребёнок становится жертвой кибербуллинга.

Инструменты защиты в интернете

Для обеспечения безопасности детей в интернете существует множество разнообразных инструментов: антивирусное программное обеспечение, VPNs (виртуальные частные сети) и приложения для реализации родительского

контроля. Благодаря этим инструментам родители получают возможность контролировать деятельность их детей в сети, что обеспечивает разумное использование интернета ребёнком.

Антивирусное программное обеспечение



Пренебрегая антивирусными программами, вы подвергаете устройство вашего ребёнка риску. Данные программы предназначены для предотвращения совершаемыми киберпреступниками попыток взлома цифровых устройств - ноутбуков, планшетов, смартфонов и т. д.

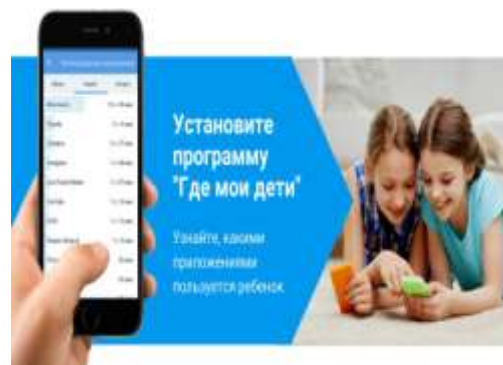


Большинство платформ антивирусного программного обеспечения предоставляют собой эффективные инструменты, блокирующие доступ ребёнка к сайтам,

содержащим вредоносное ПО. Используя антивирус ESET NOD32 SmartSecurity родители сами выбирают те категории сайтов, к которым несовершеннолетний будет иметь доступ. Переход на все остальные ресурсы, не попадающие под данные категории, будет заблокирован.

Приложения для реализации родительского контроля

Приложения родительского контроля - это незаменимый инструмент, позволяющий родителям отслеживать активность ребёнка в Интернете. Используя данные сервисы, можно узнать, какие веб - сайты посещал ребёнок, какой контент он просматривал и какие приложения использовал. Приложения, реализующие родительский контроль, становятся действительным залогом безопасности для всех, кто стремится обеспечить благополучие своих детей в эпоху Интернета. С их помощью можно ограничить время нахождения ребёнка в интернете, что увеличит количество времени для общения с друзьями и семьей, прогулок на свежем воздухе и занятий спортом. Кроме того, данные программы предоставляют родителям возможность блокировки определенных веб - сайтов, еще до того, как ребёнок обратится к ним - в том числе сайтов с играми и сайтов, содержащих порнографические материалы.



Советы для родителей по детской интернет - безопасности

Расскажите ребёнку об опасностях, с которыми он может столкнуться в сети

Это исключительно важный момент. Родители не только должны досконально изучить вопрос безопасности детей в интернете, но и обучить самих детей

правильному поведению в сети, чтобы исключить возможность возникновения опасных ситуаций. Обязательно обсудите с ребёнком все проблемы, затронутые в этой статье, расскажите о существовании онлайн - хищников, киберпреступности, вредоносных программ, кибербуллинга. Мало того, что нужно научить ребёнка правильно переходить улицу и не разговаривать с незнакомцами, также требуется объяснить, что при неправильном использовании интернет может быть очень опасен.

Покажите ребёнку, что Вы готовы всегда его выслушать

Чрезвычайно важно, чтобы ребёнок понимал - родители открыты для разговора, когда речь идет о безопасности в интернете. Если у ребёнка появляются проблемы, связанные со всемирной паутиной, он должен осознавать, что любой момент может поделиться ими с родителями.



В

Научите ребёнка, что общение в сети с незнакомцем, так же опасно, как и в реальности

Всем известное правило «Не говорите с незнакомцем на улице» актуально и в эпоху интернета. Обязательно донесите до своего ребёнка, что встречи с людьми, с которыми он знакомится в интернете, сопряжены с риском для его безопасности. Незнакомцы в Интернете могут и, скорее всего, будут опасны.



Мошенничество в Интернете

Многие люди, в том числе дети, становятся жертвами безопасных на первый взгляд всплывающих окон и спам - сообщений, созданных и рассылаемых киберпреступниками. Эти всплывающие окна и спам - сообщения могут быть очень опасными и, вероятнее всего, приведут к заражению устройства компьютерным вирусом.

Дети и социальные сети



Социальная сеть, без сомнения, является одной из самых революционных технологий XXI века. Миллионы пользователей по всему миру выбирают социальные сети, такие как Facebook, ВКонтакте, Instagram. Эти ресурсы показали себя эффективным инструментом для общения, создания онлайн - сообществ и продвижения бизнеса. Тем не менее, когда речь заходит о

детях в социальных сетях, особенно если они только начинают знакомиться с ними, данные технологии таят в себе ловушки, о которых следует знать заранее.

Проблемы в социальных сетях

Как уже говорилось ранее, кибербуллинг получил широкое распространение в эру развития социальных сетей. Так как число случаев кибербуллинга в сети продолжает расти, нужно быть готовым, что любой ребёнок в Интернете может столкнуться с угрозой психологического насилия.

Помимо этого, нахождение ребёнка в социальных сетях в разы увеличивает риск атаки интернет - хищника. Преступные личности в целях маскировки очень часто используют фальшивые профили, напоминающие профиль ребёнка. Именно поэтому в момент знакомства с социальными сетями ребёнок должен быть предупрежден об опасности встречи с интернет - хищниками.

Контролируйте деятельность ребёнка онлайн



Если ребёнок пользуется социальными сетями, родители должны следить, чем он занимается в сети: какую информацию выкладывает в своём профиле, с кем общается, какие материалы читает и т.д. Отличным инструментом для этих целей могут стать приложения, реализующие родительский контроль - например, сервис «Где мои дети», позволяющий узнать, сколько времени ребёнок проводит, общаясь

в социальных сетях и мессенджерах.

Интернет и дети подросткового возраста

Когда дети достигают определённого возраста - в частности речь идёт о подростках - их интересы довольно часто вступают в противоречие с установленными родителями правилами безопасности. Подростки стремятся быть более независимыми от родителей. Тем не менее, неограниченный доступ к сети интернет может стать настоящей проблемой. Такой нежелательный контент, как видео со сценами насилия, жестокие компьютерные игры, материалы с рейтингом 18+, порнографические изображения - притягивает подростков как

магнит. Поэтому, даже предоставляя несовершеннолетним свободу действия в интернете, родители все равно могут и дальше использовать приложения, ограждающие их ребёнка от материалов нежелательного содержания. В этом случае по-прежнему уместно использование различных инструментов, о которых говорилось ранее - в частности приложений и сервисов, реализующих родительский контроль. Данная мера позволит родителям обеспечить детям ту приватность в сети интернет, к которой они стремятся, и одновременно с этим избавит их от страха, что ребёнок натолкнется на нежелательный контент.

