

**ПРАВИЛА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В ИНТЕРНЕТЕ (советы родителям)**

**Интернет опасности для детей** – это комплекс внешних воздействий, который проявляется при посещении всемирной сети и угрожает безопасности ребенка и его окружающим. Опасности могут носить физический, психологический или материальный характер. Стоить помнить, что на данный момент всемирная сеть интернет являет слабо контролируемой средой. Поэтому неконтролируемое нахождение ребенка любого возраста и любого уровня технических знаний в интернете без присмотра взрослых сопряжено с рядом опасностей.

**Физические опасности** при работе в интернете носят опосредственный характер. То есть непосредственно в интернете вашему ребенку никто не может причинить физический урон. Это обусловлено самой технологией вхождения во всемирную паутину. Ведь ребенок работает за сенсорным экраном или мониторов и механизмов физического воздействия на него со стороны злоумышленников нет. Но! Люди, преследующие криминальные цели, могут воздействовать на вашего ребенка путем перенесения отношений в реальный мир, они могут выведать у него физический адрес или назначить встречу. Наиболее распространенными целями являются сексуальные домогательства, похищение ребенка и различного рода аферы. Поэтому очень важно объяснить ребенку опасность разглашения реальной информации о себе, а также назначение свиданий с совершенно незнакомыми людьми. Ребенок должен попытаться понять, что за фотографией красивой тринадцатилетней девочки может прятаться сорокалетний педофил. Поэтому любые попытки назначения подобных свиданий должны четко быть на контроле родителей.

**Психологические опасности** при работе в интернете – это наиболее распространенный тип угрозы для вашего ребенка. Интернет содержит разного рода информацию, которая далеко не всегда полезная и может нанести урон психике ребенка или в корне поменять его мировоззрение, причем в худшую сторону. Тут следует заметить, что доступную информацию в интернете можно разделить на три вида:

* Легальный контент для общего доступа;
* Легальный контент только для взрослых;
* Запрещенный контент.

Легальный контент для общего доступа тоже может быть вреден для ребенка, так как в зависимости от возраста он может быть просто не готов к её восприятию. Например, медицинский учебник по гинекологии нежелателен для ознакомления школьникам младших классов. Хотя, конечно, вред от общедоступного контента несравнимо меньший, чем от информации второго и третьего типа. К легальному контенту только для взрослых относится информация разрешенная к ознакомлению только совершеннолетним. Она, как правило, сексуального характера: фотографии, статьи, фильмы, товары. И тут сложность возникает на уровне разграничения доступа. Если в реальной жизни в секс-шоп ребенка просто не пустят, то в интернете получить доступ к онлайн секс-шопу ему не составит труда. Разного рода вопросы «исполнилось ли вам 18 лет?» представляются нам наивными и сделанными только для отвода глаз. Очень маловероятно, что подросток ответит правдиво на этот вопрос. А глобальных эффективных механизмов разграничения доступа по возрасту пока не существует, поэтому оптимально применять локальное программное обеспечение для защиты ребенка и ограничения ему доступа к нежелательным данным. Такое же программное обеспечение может помочь и с информацией третьего типа: запрещенный контент. Это информация, запрещенная в большинстве стран мира – проповедующая нацизм, терроризм, наркотики, расовую непримиримость, жестокость, сексуальные извращения и любой порнографический контент. Этот тип информации может нанести прямой вред психике ребенка, вызвать у него разного рода расстройства либо озлобить или мотивировать вступить в какую-то запрещенную организацию. Задача родителей проявить бдительность и обеспечить ребенку максимально безопасный серфинг в сети, если у вас самих не хватает технических знаний, то следует нанять специалиста по настройки программного обеспечения для защиты детей в интернете.

**Опасности материального характера**, которые возникают при работе в интернете, связаны с разного рода мошенничествами, а также вредоносным программным обеспечением. С последним призвано бороться антивирусное программное обеспечение, но всё же бывают случаи, когда дети заражают компьютер, слушаясь инструкций мошенников о том, что антивирусное обеспечение надо отключить или внести программу аферистов в список исключений. Часто вредные приложения или подпрограммы вшивают в пиратское программное обеспечение или в комплекте с легальным продуктом пытаются установить и вирусный. Ребенок должен усвоить, что ни одно легальное и безопасное программное обеспечение не должно требовать выключения антивирусной защиты! И что скачивание пиратских программ может нести угрозу не только компьютеру, но и материальному благосостоянию семьи. Ведь вредоносные программы опасны не только вероятностью повреждения данные на компьютере, но и тем, что могут передавать мошенникам пароли, данные кредитных карточек, банковских счетов и так далее. Также ребенок может стать жертвой аферистов и не устанавливая программ на компьютер. Ему просто могут на выдавать в браузере какую-то ложную информацию и попросить отправить SMS сообщение, совершить звонок на платный номер, перечислить деньги и т.д. Иногда такая информация приходит якобы от его друзей, а по факту со взломанных хакерами аккаунтов. Мотивация может быть совершенно разная от «Поздравляем! Вы выиграли миллион!» до «Надо помочь больным детям!» Ребенок должен усвоить, что нельзя никому разглашать пароли или совершать отправку сообщений, звонить куда-то, пересылать деньги на основании информации в интернете. И что даже если он и хочет кому-то помочь, то надо поставить в известность взрослых и выяснить действительно ли этот человек нуждается в помощи или это уловка аферистов.