Опасности в Интернете. Сайты, таящие в себе опасность негативного отношения к жизни, подталкивающие к самоубийствам. Родительский контроль в интернете.

Опасность в интернет-пространстве можно разделить на три вида:

1. Доступная для детей негативная информация.
2. Противоправные и социально-опасные действия самого ребенка.
3. Целенаправленные действия третьих лиц в отношении ребенка.

Какие опасности существуют в интернете?

Опасность: проблемы конфиденциальности. Размещая информацию о себе в социальных сетях, вы должны быть готовы к тому, что ее может увидеть большое количество людей. В итоге, ваша частная жизнь становится достоянием общественности. Подумайте о том, что опираясь на ваши раскрытые сведения, нетрудно узнать ваши привычки, фамилии и имена друзей, ваш маршрут движения. А наличие этого делает вас простой целью для атак киберхулиганов.

Опасность: хакерство и взлом паролей. Даже если вы принимаете все меры для того, чтобы оградить информацию о себе от незнакомых вам людей, эти попытки, в конечном итоге, могут оказаться бесполезными. Есть множество хакерских программ, которые помогают подбирать пароли к популярным веб-сайтам и взламывать их. Поэтому задавайте сложные пароли (от 10 символов) к личным данным и тогда вероятность подбора будет пропорциональна длине пароля (чем больше, тем сложнее).

Опасность: виртуальные двойники. Время от времени вы раскрываете информацию о себе: вашу дату рождения, информацию о вашей семье, ваших занятиях, предпочтениях в области литературы и кинематографа, поездках, где вы живете и пр. Кто-то может украсть эти данные, собрать их воедино и создать вашего виртуального двойника. Остается лишь дополнить профиль вашей фотографией, которую несложно взять из вашего блога, дневника или даже вашего аккаунта в той же самой социальной сети и собрать воедино кое-какие факты вашей биографии, которые так же без труда берутся из тех же источников.

Опасность: вымогательство и шантаж. Сетевое вымогательство уже существует. И вам могут предложить купить порочащую вас страницу за совсем небольшую сумму, в виде кодов карточек экспресс оплаты той или иной сотовой сети или одним из множеств видов сетевой оплаты услуг. Также в социальных сетях мы рискуем подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать установление дружеских отношений с целью личной встречи, вступления с ним в отношения, шантажа и эксплуатации. Общаясь лично, злоумышленник, чаще всего представляясь сверстником, входит в доверие к вам, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече.

Опасность: интернет-зависимость. Сайты социальных сетей могут вызвать зависимость: ими очень просто пользоваться, они открывают вам целый мир информации, непознанной до сих пор. Социальные сети дают вам возможность заявить о себе на весь мир. Вы можете много раз в день заходить на свои страницы «В контакте», «Одноклассниках», Facebook и проводить много времени, просто читая о том, что происходит в жизни ваших друзей. Вы можете тратить на это учебное или рабочее время и уделять меньше времени учебе, работе, друзьям, себе и своей семье.

Опасность: экстремизм, национализм, фашизм. Все широкие возможности интернета используются представителями экстремистских течений для того, чтобы заманить в свои ряды новичков.

Опасность: секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам «проникнуть в мысли» и повлиять на взгляды на мир.

Опасность: Наркотики. Интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья».

Опасность: интернет-знакомства. Ещё одна опасность – интернет- знакомства. Существует немало обманутых людей, познакомившихся в социальных сетях.

Опасность: вред здоровью. Проведение большого количества времени в интернете вредит здоровью и оказывает влияние на психику человека.

И другие…

Сайты, таящие в себе опасность негативного отношения к жизни, подталкивающие к самоубийствам.

«Группы смерти» – это группы в социальной сети: «Вконтакте», которые прямо или косвенно склоняют подростков к суициду.

Признаки участия подростка в «группах смерти»:

- ребенок участник групп: «F57», «Тихий дом», «Море китов»;
- упоминает, пишет имя Рина;
- на личной странице в соц. сетях есть видеозаписи, фото, тексты, связанные с суицидом;
- рисует, имеет в электронном или бумажном виде оккультную символику (пентаграммы, сатанинские знаки и т.п.);
- стихи, цитаты на тему смерти или с мистическим уклоном;
- рисует, есть изображения на странице в социальных сетях: китов, бабочек, бритв, ножей, крови и т.п.;
- появление на теле следов порезов, ожогов и иных признаков членовредительства;
- ребёнок упоминает о каких-то оставшихся днях: «Осталось 35 дней»;
- нарушение режима сна, ранний подъем утром или невозможность разбудить ребёнка утром и т.д.

Родительский контроль в интернете.

Понятие родительские контроль обозначает комплекс мер, позволяющих установить ограничение на пользование определенными ресурсами в Интернете. В операционных системах это могут быть как встроенные функции, так и специально скаченные программы. Это один из основных способов, как как сделать детский интернет безопасным.

У контроля есть три функции:

1. Ограничение нахождения ребенка в сети. Компьютер будет самостоятельно выключаться при достижении установленного администратором периода. Повторно включить его можно будет только в разрешенное системой время.
2. Блокировка для детей в интернете определенных программ.

3. Ограничение запуска игровых приложений.

Эти мероприятия позволят снизить нагрузку как на зрение, так и на детскую психику.

Установив стандартные опции, родители получают возможности:

1. Отследить все действия своего отпрыска в компьютере. Они смогут увидеть, какие программы он запускал, сколько по времени они работали. Система дает возможность получать подробные отчеты с детской учетной записи.

2. Функционал позволяет установить ограничения по использованию игр в зависимости от возраста.

Обеспечивается тотальное слежение за работой с браузером. Взрослые могут ограничить использование определенных сайтов по ключевым словам. У них есть возможность отслеживать активность ребенка в интернете, посещение сайтов, просмотр видео.

Рекомендации для родителей по организации безопасной работы в Интернет

1) Внимательно относитесь к действиям ваших детей в «мировой паутине»:

Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернет, особенно на этапе освоения.

Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернет и как вовремя предупредить угрозы.

2) Информируйте ребенка о возможностях и опасностях, которые несет в себе сеть:

Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием от другого пользователя Интернет, ему нужно сообщить об этом близким людям.

Научите ребенка искать нужную ему информацию и проверять ее, в том числе с Вашей помощью.

Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернета, особенно путём отправки sms, – во избежание потери денег.

Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться Ваш ребенок, и посоветуйте их использовать.

3) Выберите удобную форму контроля пребывания вашего ребенка в Сети:

Установите на Ваш компьютер необходимое программное обеспечение – решение

родительского контроля, антивирус Касперского или Doctor Web.

Если Ваш ребенок – учащийся младших классов и остается часто дома один, ограничьте время пребывания Вашего ребенка в Интернете.

Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка.

Создавайте разные учетные записи на Вашем компьютере для взрослых и детей. Это поможет не только обезопасить ребенка, но и сохранить Ваши личные данные.

Регулярно отслеживайте ресурсы, которые посещает Ваш ребенок. Простые настройки компьютера позволят Вам быть в курсе того, какую информацию просматривал Ваш ребенок.

4) Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей:

Используйте удобные возможности повышения уровня компьютерной и Интернет грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.

Знакомьте всех членов Вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.