Безопасность детей в интернете. Рекомендации родителям

Сеть Интернет – это огромный мир информации и коммуникаций. Как и многое в мире использовать эти коммуникации и информацию можно во благо или во зло.

Безопасность в сети Интернет достаточно размытое понятие. Давайте попробуем классифицировать угрозы, от которых мы хотим обезопасить наших детей.

Сложность обеспечения безопасности в сети в том, что границы стёрты, и злоумышленники могут находиться за тысячи километров, размытость границ взаимодействия пользователей усложняет их идентификацию, а следственно и возможность наказания за содеянные поступки. Напротив, человек несведущий не скроется за псевдонимом, даже используя «бытовые» методы конспирации, и будет быстро найден соответствующими службами. (Например, при распространении информации запрещённой к распространению законами РФ)

Большинство же пользователей крайне легкомысленно относятся к безопасности в Интернете, а в частности: созданию паролей, хранению информации, защите своих устройств, а так же ответственности за ретрансляцию информации определённых содержаний.

Попробуем составить список угроз для детей, которые потенциально может нести Интернет.

1) Информационная безопасность.

   Запрещенного характера.

   Производство и способы употребления запрещённых веществ.
   Производство и тестирование СВУ (Самодельных взрывных устройств)
   Производство либо модернизация оружия или боеприпасов.

   Неприемлемого содержания.

   Сцены насилия в видео и играх.
   Сексуальной тематики.
   Религиозные и сектантские течения.
   Группы по сомнительным интересам.
   Откровенно экстремистские группы.
   Группы провокаторы. (Синий кит, сайты призывающие к членовредительству или опасным действиям..)

   Потеря личной информации

   Архивы фото и видео
   Рабочая информация
   Конфиденциальная информация
   Личные данные (например медицинские)
   Данные банковских карт

2) Безопасность общения.

   Действия третьих лиц в отношении ребенка
   Склонение к распространению запрещённых веществ.
   Склонение к участию в сомнительных мероприятиях или митингах за вознаграждение.
   Вовлечение в занятие проституцией и занятиями порочащими честь и достоинство.

3) Финансовая безопасность.

   Потеря средств с банковских карт
   Вымогательство
   Оплата за восстановление данных или настройку компьютера.

4) Психологическая безопасность

   Хейтинг, троллинг, кибербуллинг. (Злое обращение, насмешки, унижение, травля, преследование в сети, комментарии и т.п.)

   Психологические манипуляции

5) Программная безопасность

   Заражение устройств вирусами, использование мощностей Вашего компьютера для платного выполнения каких-либо действий или алгоритмов. Например, добыча крипто валюты, написание отзывов от Вашего имени, выманивание средств у Ваших друзей в соцсетях.

Как становиться понятно, виртуальный мир невероятно многогранен. К сожалению, в нём достаточно угроз, и они между собой связаны. Слабое внимание к информационной безопасности, может столкнуть Вас и с другими угрозами, например, с вымогательством или потерей средств с банковской карты.

Понятно становиться и то, что от этих угроз нужно защищаться, и научить этому детей.

Первый шаг это, это, конечно, Ваша заинтересованность и внимание к данной теме. Лишний раз посмотрите настройки ваших устройств, почитайте лицензионные соглашения приложений, которые Вы используете, Поговорите с детьми о безопасности в Интернете. Научите своих детей определять угрозы и проговорите алгоритм их действий при встрече с этими угрозами.

Важным шагом будет защитить свои устройства антивирусным программным продуктом. Желательно, чтоб этот продукт был не пробным вариантом с урезанными возможностями. Взвешенно подойдите к выбору Антивируса, и не пожалейте средств на безопасность. Зачастую это не такие большие средства. Например, Антивирус о котором ниже пойдёт речь стоит 900 руб. в год. Ведь платный Антивирус любого разработчика имеет значительно более широкие возможности, чем бесплатные, или пробные варианты.

Итак, какой же функционал антивирусных продуктов нам предлагают разработчики, как же мы можем обезопасить, себя, детей и их психику, свой кошелёк, свои устройства?

Давайте рассмотрим, что нам предлагает Лаборатория Касперского в сфере Интернет безопасности детей.

На официальном сайте можно скачать, оплатить, а так же бесплатно в течении 7 дней протестировать следующий программный продукт -Kaspersky Safe Kids.

Kaspersky Safe Kids включает в себя приложения для ребенка и родителя, которые взаимодействуют. Приложение на устройстве ребенка помогает контролировать его онлайн-активность, приложение на вашем устройстве позволяет просматривать отчеты и менять настройки, Вы также можете управлять настройками детского приложения.

Блокирование доступа к нежелательным веб-сайтам и контенту

Помогает управлять доступом к играм и нежелательным приложениям

Позволяет контролировать время использования каждого устройства

Отчеты о публикациях ребенка в Facebook и ВКонтакте и изменениях в списке друзей

Советы профессионального психолога относительно онлайн-активности ребенка

Определение местонахождения ребенка на карте в режиме реального времени

Установление безопасного периметра на карте и отправка уведомлений в случае выхода ребенка за его пределы

Отправка уведомлений о низком уровне заряда батареи на устройстве ребенка

Это что касается контроля, для возможности своевременного реагирования.

Напоследок можно привести ряд рекомендаций для работы, поиска информации, общения в Интеренте, которые, во многом, обязательны к выполнению и взрослыми. Внимательно изучите их, и не просто расскажите о них детям, а разработайте ряд правил для пользования Интернетом и не переставайте уделять этому вопросу пристальное внимание!

Итак, простые правила, которые должны появиться в каждой семье.

<u>Правила работы в сети Интернет</u>

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.

3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свои пароли.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)

7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней по возможности не было указано никакой личной информации.

9. Не всей информации, которая размещена в Интернете, можно верить.

10. Не оставляйте без присмотра компьютер с важными сведениям на экране

11. Не сохраняйте важные сведения на общедоступном компьютере.

Советы по безопасности в сети Интернет для детей 7-8 лет

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним, не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

- Используйте специальные детские поисковые машины.

- Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

- Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

- Научите детей не загружать файлы, программы или музыку без вашего согласия.

- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Советы по безопасности для детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы Вы убедились, что они не общаются с незнакомцами.
- Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

А самое главное проведите время с ребёнком в сети, посмотрите, что его интересует и какими ресурсами он пользуется. При совместной работе не забывайте напоминать правила, о которых мы Вам рассказали.

Удачи!