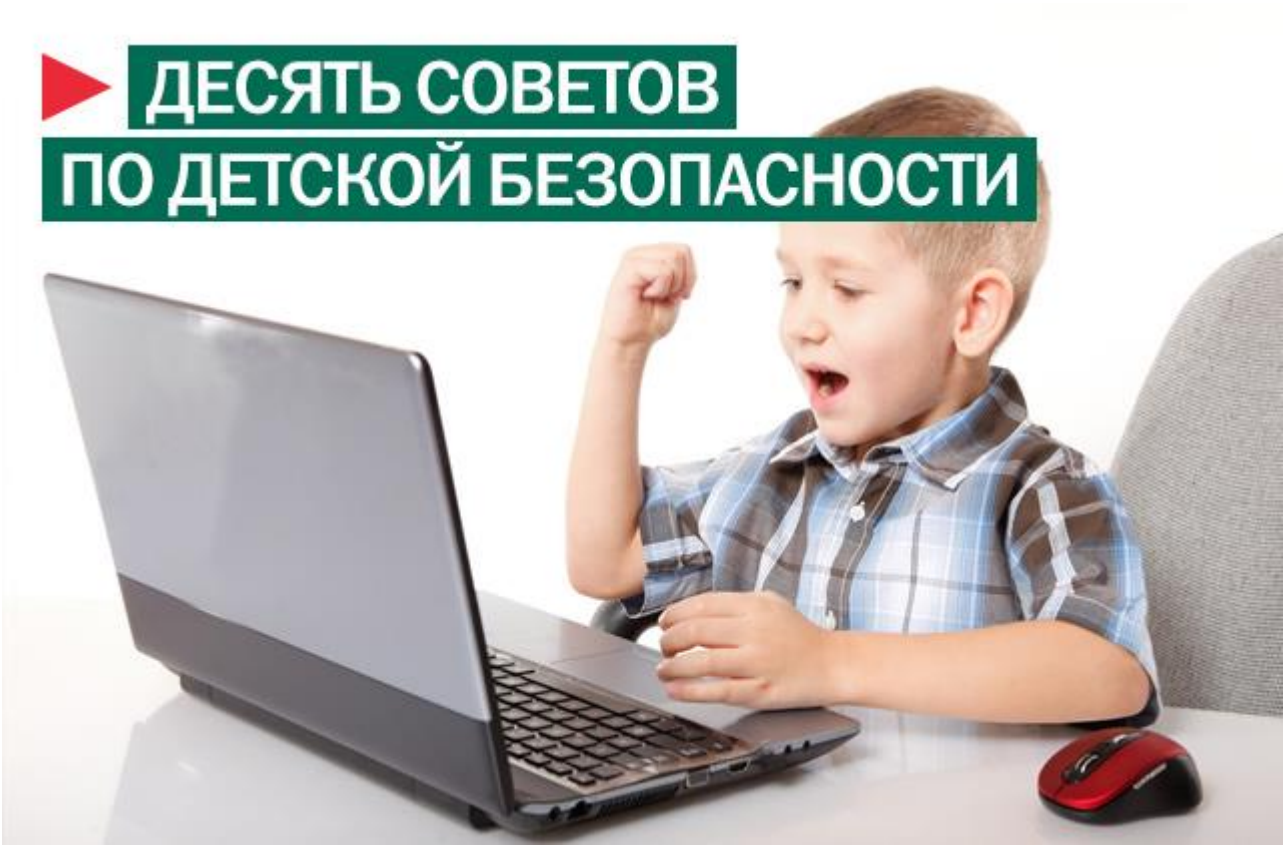
Десять советов детской безопасности

Существуют потенциальные риски, с которыми все мы сталкиваемся в Интернете. К ним относятся вредоносные программы, фишинг-атаки и нежелательная почта. Но есть дополнительное измерение, где речь идет о детях. Они не такие опытные, как мы, поэтому, как правило, менее осторожны при обмене информацией и иначе воспринимают мошеннические сообщения, в которых предлагается переход по ссылкам.



Есть также совершенно определенные опасности, с которыми сталкиваются дети. К ним относятся ресурсы, посвященные порнографии, насилию и наркотикам, а также направленные на нанесение себе умышленного вреда или даже доведение до самоубийства. К сожалению, такой опасный материал доступен всего лишь парой кликов мышкой: нежелательное содержание может отображаться вместе с остальными результатами порой совершено безобидного поиска — например, «маленькая киска», «сладости» или что-то другое, что может интересовать наших детей.

Помимо этого дети могут подвергаться влиянию баннерной рекламы на страницах, которые посещают. Вы можете удивиться, когда узнаете, что мошенники очень часто рассчитывают именно на детские наивность и непосредственность, размещая контекстную рекламу. Дело в том, что многие дети пользуются кредитными картами родителей, что делает их мишенью. Не меньшая проблема от того, что мошенники часто торгуют поддельными продуктами и услугами, за которые дети расплачиваются онлайн. Например, компьютерные игры, книги, фильмы, покупки внутри каких-то приложений в ноутбуках, смартфонах и планшетах.

Ничего не скрываю, делюсь всем

Родители более опытны, но нередко менее технически подкованы. Дети же технически более продвинуты, но зачастую беспечны и не знают о грозящих опасностях.

Это совсем иной аспект безопасности в Интернете. Наши дети растут в культуре, когда принято делиться любой информацией. Социальные сети превратили Интернет в доску объявлений на семейной кухне, чем они и пользуются. Они размещают информацию о том, кто они такие, где находятся, что покупают и с кем дружат. И все — с картинками. Но в то время как та кухонная доска объявлений доступна только для семьи и друзей, подобная информация в социальных сетях становится достоянием всего света. Личная информация может быть использована нечистоплотным негодяем, который затем вотрется в доверие к ребенку, чтобы затем встретиться с ним в реальном мире. Общие фотографии могут быть использованы сверстниками для запугивания и шантажа. Взрослые часто считают, что все дело в некоей культуре «делиться всем», дети тоже, пока не понимают, что что-то идет не так.

Технологический разрыв поколений

К сожалению, мы столкнулись с тем, что у нас большой технологический разрыв между поколениями. Родители более опытны, но нередко менее технически подкованы. Они даже не всегда осознают всех возможностей современных технологий. Дети же технически более продвинуты, но зачастую беспечны и не знают о грозящих опасностях.

Наблюдатель и Учитель

Дети должны знать, что такое хорошо, а что такое плохо в Интернете так же, как они должны знать правила дорожного движения и важность быть рядом с нами.

Именно потому, что родителям важно вовлекать себя в онлайновую деятельность своих детей с самого раннего возраста, они являются учителями для своих детей, делятся с ними опытом. Конечно, безопасность переписки должна присутствовать исходя из возраста ребенка. Мы не можем ожидать от маленького человечка, что он самостоятельно разберется в тонкостях интернет-угроз. Но дети должны знать, что такое хорошо, а что такое плохо в Интернете так же, как они должны знать правила дорожного движения и важность быть рядом с нами. Важно также просто и доступно объяснить необходимость использования защитных программ, защищающих от вредоносного кода, защиты личной информации и тому подобных вещей. По мере взросления ребенка такие разъяснения должны становиться все более подробными и частыми. И чем раньше такие разъяснения начнутся, тем менее обременительными и необязательными они будут казаться детям.

Вот наш список лучших советов для поддержания безопасности ваших детей в Интернете:

1. Поговорите с ними о потенциальной опасности.
2. Вовлекайте себя в интернет-деятельность ваших детей с самого раннего возраста, давая понять, что это норма, потому что вы для них главный Наставник.
3. Подталкивайте их на разговоры, в которых дети будут делиться с вами своей сетевой деятельностью, в частности могут рассказать, если чувствуют какой-то дискомфорт или ощущают явную угрозу.
4. Сегодня культура «делиться всем» является широко распространенной. Дети, конечно, маловероятно, но все же инстинктивно часто признают опасности, присущие бездумному распространению информации о себе, поэтому очень важно понятным языком изложить им потенциальные проблемы.
5. Установите четкие нормы и правила поведения детей в Интернете. Обязательно объясните, почему вы это делаете. Вы должны пересматривать эти правила с взрослением ребенка.
6. Используйте программное обеспечение для родительского контроля, чтобы установить приемлемые рамки, отводимые на время в Интернете, получаемый контент, определенные виды деятельности (например, заблокировать чаты и форумы). Родительский контроль можно настроить для нескольких учетных записей в компьютере, применяя различные правила для разных детей.
7. Приучите детей проявлять бдительность в отношении их личной жизни и информации о ней в социальных сетях. Убедите их настроить свой профиль таким образом, чтобы вся подобная информация была видна только ограниченному кругу друзей и членам семьи.
8. Опыт против технической продвинутости. Вы можете быть более осведомленными о потенциальных опасностях Интернета, но, скорее всего, ваши дети будут более продвинуты в техническом плане. Поощряйте взаимный обмен информацией, учитесь друг у друга.
9. Защитите компьютер с помощью программного обеспечения интернет-безопасности.
10. Не забывайте о своих смартфонах — это сложные компьютеры, а не только телефоны. Большинство смартфонов поставляются с функцией родительского контроля, а производители программного обеспечения могут предложить приложения для фильтрации нежелательного контента, нежелательных SMS и прочих неприятностей.