

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ**

В России около 8 миллионов пользователей глобальной сети — дети. Они играют, знакомятся, познают новое о мире... и при этом встречаются с целым рядом угроз, о которых даже и не подозревают. Наша обязанность — предупредить и защитить их от негативного контента (информации, расположенной на страницах сайта).

### **УГРОЗЫ, ВСТРЕЧАЮЩИЕСЯ НАИБОЛЕЕ ЧАСТО:**

**Контакты с незнакомыми людьми** - ими могут быть преступники и злоумышленники.

**Заражение вредоносными и нежелательными программами.** К вредоносным программам относятся вирусы, черви и «троянские кони» — это компьютерные программы, которые могут нанести вред компьютеру и хранящимся на нем данным. Под «нежелательным программным обеспечением» понимаются программы, которые выполняют на компьютере некие задачи без согласия на то пользователя. Они могут показывать рекламные сообщения, объявления или собирать личные данные о человеке, его окружении.

**Доступ к нежелательному содержанию.** Сегодня в Интернете очень много информации о таких понятиях как: насилие, наркотики, порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и пр. Часто просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера.

**Неправильное формирование нравственных ценностей.** Возникает в результате доступа к нежелательному содержанию. Существуют средства фильтрации нежелательного материала, но фильтры могут помочь в блокировании только некоторых материалов. Поэтому взрослым важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались за советом и помощью.

**Раскрытие личных данных.** Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Подробное раскрытие личных данных потенциально опасно.

**Интернет-мошенничество и хищение данных кредитной карты.** Осуществляется с помощью фальшивых электронных писем, в которые включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом будет использована с ущербом для пользователя.

**Азартные игры.** Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем как игровых, так и настоящих денег.

### **РЕКОМЕНДАЦИИ, С ПОМОЩЬЮ КОТОРЫХ ПОСЕЩЕНИЕ ИНТЕРНЕТА МОЖЕТ СТАТЬ МЕНЕЕ ОПАСНЫМ ДЛЯ ВАШИХ ДЕТЕЙ:**

1. Посещайте Интернет вместе с детьми. Поощряйте их делиться с вами успехами и неудачами в деле освоения Интернет.
2. Объясните детям, что если в Интернете что-либо беспокоит их, то следует не скрывать этого, а поделиться с вами своим беспокойством.
3. Объясните ребенку, что при общении в чатах, использовании он-лайн игр и др. ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.
4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес,

номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.

**5.** Объясните своему ребенку, что в реальной жизни и в Интернете нет разницы между неправильными и правильными поступками.

**6.** Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни.

**7.** Скажите им, что никогда не стоит встречаться с друзьями из Интернета без контроля взрослых. Люди могут оказаться совсем не теми, за кого себя выдают.

**8.** Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены.

**9.** Не забывайте контролировать детей в Интернете с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

**Будьте внимательны к вашим детям!!!**

Материал подготовила

В.А. Осипова, специалист по соц. работе