**Лекция об информационной безопасности для детей.**

В соответствии с Конституцией Российской Федерации человек, его права и свободы имеют приоритетное значение. Права человека могут быть реализованы тогда, когда люди информированы о своих правах и знают, как их использовать. Дети каждый день смотрят телевизор часами, но все больше и больше времени они проводят в Интернете, используя навыки, которым они быстро обучаются у своих сверстников. Дети используют интерактивные средства для игры, общения, написания блогов в Интернете, прослушивания музыки, размещения собственных фотографий и поиска других людей для общения в интерактивном режиме. Использование электронных, цифровых и интерактивных информационных средств оказывает значительное положительное воздействие на развитие детей: это увлекательно, это обучает и социализирует. Однако это также несет потенциальную возможность вреда для детей и сообществ, в зависимости от того, как осуществляется использование.

Рассмотрим основные интернет-угрозы:

**Электронная безопасность:** Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

**Вредоносные программы -** это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное программное обеспечение и различные формы вредоносных кодов.

**Спам** - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

**Кибермошенничество** - это один из видов киберпреступлений, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль.

**Коммуникационные риски** связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

**Контентные риски** связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

**Неподобающий контент.** В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

**Киберпреследование** - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Чтоб обойти вышеперечисленные риски, не нужно размещать на своих страницах следующую информацию:

* Информация о вашем местоположении
* Информация о планах на длительные поездки
* Фотографии дорогих вещей и подарков
* Фотографии квартиры или дома
* Свой домашний адрес
* Фотографии личных документов

Во избежание рисков, связанных с нарушением безопасности в интернете и жизни, рекомендуем соблюдать следующие правила:

1. Если у вас появились страхи при общении или посещении незнакомого сайта в интернете – не бойтесь просить помощь у родителей.
2. Не оставляйте в общем доступе и личной переписке информацию о банковских картах, личных документах, местоположении и др., а так же не отправляйте эту информацию незнакомцам.
3. Не переходите по ссылкам, присланным незнакомыми людьми, спам-сообщениям.
4. Не выкладывайте фото/видео или информативные материалы о себе и своих знакомых, которые смогут скомпрометировать вас в будущем.
5. Не встречайтесь в реальной жизни с людьми, с которыми познакомились в интернете. Сообщите родителям, если незнакомцы настаивают на встрече.
6. Помните, что совершая покупки в интернете, вы тратите реальные деньги.
7. Не поддавайтесь на заманчивые предложения в интернете. Не стоит переходить на сайты, связанные с розыгрышами техники, огромными скидками и прочими предложениями.

Рекомендуемые к изучению медиа-файлы:





