Консультация для родителей
«Как обеспечить информационную безопасность детей в интернете»

Сегодня невозможно представить жизнь без использования интернета, он стал неотъемлемой частью во всех сферах. Развитие технологий приводит к тому, что дети с раннего детства проводят в сети большую часть своего свободного времени. К сожалению, вместе с нужной и полезной информацией маленькие пользователи сталкиваются с нежелательным контентом, который может нанести вред психическому и физическому здоровью, стать угрозой для жизни.

Классификация информационной опасности для детей в интернете

Для маленьких пользователей в сети встречаются разные виды опасности, которые можно классифицировать по различным тематикам. В основном это сайты и форумы:

- Суицидальной направленности;
- Пропагандирующие наркотики;
- Разжигающие расовое неприятие и национальную рознь;
- Связанные с порнографией;
- Знакомства;
- Пропагандирующие насилие, экстремизм, различные виды мошенничества, девиантные формы поведения;
- Секты.

Контент

Чего только сегодня не встретишь во Всемирной паутине. Ребенок может наткнуться на контент, который связан с насилием, жестоким обращением с животными, сексуальными извращениями, убийствами. Взрослым важно позаботиться о безопасности в интернете для детей и воспользоваться функцией «родительский контроль». Далее подробнее расскажем о специальных возможностях, которые помогают ограничивать доступ детей к нежелательным сайтам и контролировать время, проведенное в сети:

- как часто ребенок сидит в соцсетях;
- сколько времени проводит, смотря видеоролики в YouTube или TikTok;
- в какие игры играет (возрастной рейтинг).

Киберпреступность

Киберпреступностью называется деятельность, связанная с неправомерным использованием сети интернет. Здесь можно выделить широкий спектр нарушений. Например, вовлечение детей в торговлю наркотиками, мошенничество, получение личных данных. Задача родителей – рассказать чаду, что нужно быть очень внимательным и остерегаться незнакомцев, которые пытаются вовлечь его в сомнительную деятельность:

- не раскрывать данные документов и карт;
- не рассказывать личные пароли и адреса;
- ни у кого ничего не покупать без ведома взрослых.

Кибербуллинг

Если родители начали замечать, что ребенок стал агрессивным, раздражительным, нервным, тревожным, нужно расспросить его о причинах такого поведения. Зачастую это происходит из-за негативного общения в сети, где оказывается психологическое давление, либо ему угрожают, издеваются.

Взрослым нужно выявить агрессоров и изолировать ребенка от общения с ними. Можно воспользоваться черным списком, а если дело зашло слишком далеко, обратится в правоохранительные органы.

Как распознать злоумышленника?

Зачастую злоумышленнику не составляет труда обмануть ребенка, воспользовавшись детской наивностью и доверчивостью. Поэтому маме и папе нужно объяснить, как распознать первые звоночки опасности:

- это незнакомый человек;
- он намного старше;
- у него на странице нет фото, друзей, личной информации или она фейковая;
- незнакомец обращается со странными просьбами: уточнить личные данные, номера банковских карт, пополнить счет мобильного телефона, выслать фото и т.п.

Основные правила информационной безопасности для детей в интернете

Прежде чем допускать чадо к пользованию интернетом, важно обсудить и закрепить основные правила безопасности для детей.

1. Первое время старайтесь посещать различные интернет ресурсы вместе с детьми. Просите их делиться информацией, которую они узнали.

2. Объясните, как вести себя на просторах сети:

- Не общаться с навязчивыми незнакомцами. Расскажите ребенку, что могут требовать от него незнакомые люди в сети, научите говорить «нет» и отстаивать свое мнение, поясните, что обязательно нужно делиться с вами, если кто-то пытается на него давить, чтобы что-то получить.
- Фото и личную информацию нужно размещать в закрытом аккаунте, чтобы ее могли видеть только близкие друзья. Если страница открыта, то лучше использовать псевдоним в качестве имени (желательно без гендерного определения, чтобы злоумышленники не могли догадаться, кто перед ними), а также не указывать в публикациях геолокацию.
- Никогда не использовать веб-камеру для общения с незнакомыми людьми.
- Проверять сайты на безопасность. Объясните, какие площадки должны вызывать подозрение у ребенка: с обилием рекламы, с заголовками, обещающими получение призов, денег, подарков и т.п.
- Сохранять логины и пароли от своих страниц в надежном месте. Например, в записной книжке, которая хранится дома.
- Не встречаться в реальной жизни с малознакомыми виртуальными друзьями.
- 3. Если у вашего ребенка уже есть аккаунт в системе Google, настройте функцию родительского контроля. С помощью него можно оградить чадо от нежелательного контента и ограничить время его пребывания в сети.

Если у ребенка гаджет с системой Android, зайдите в Play Market и скачайте приложение «Родительский контроль». В настройках можно выбрать ограничения по возрасту для различных программ и приложений.

В устройствах IPhone и IPad также можно установить ограничения на контент, приложения, общее экранное время. Для этого нужно зайти в «Настройки – Основные – Экранное время».

Эту функцию также можно установить на операционной системе Windows в 10 версии. Нужно войти в «Учетные записи – Другие люди – Добавить члена семьи» и добавить учетную запись для ребенка, указав нужные ограничения.

При необходимости дополнительно укажите возраст ребенка, тогда система сама будет ограничивать доступ согласно допустимому возрасту.

4. Самостоятельно зарегистрируйте ребенка в программах, которые не требуют использования личной информации, а только регистрационное имя и адрес электронной почты. Для этого в аккаунте Google можно создать отдельную электронную почту.

5. Расскажите сыну или дочери о том, что разница между хорошим и плохим в реальной жизни и в сети одинакова.

6. Объясните про правила этикета в сети: незаконное скачивание компьютерных игр, музыки, программ, приложений является кражей и наказуемо по закону. Нужно уважать чужую интеллектуальную собственность.

7. Ребенок должен усвоить, что в интернете нужно также соблюдать правила хорошего тона: не грубить, не писать плохих комментариев, не вступать в споры и не реагировать на провокации.

Все эти правила достаточно просты. Если вы изначально выстраиваете с ребенком доверительные отношения, донести их до него не составит труда. Ведь сегодня правильное использование интернета и современных технологий открывает перед нами безграничные возможности.