

В Интернете немало угроз: негатив, агрессия, непристойности, буллинг, опасные незнакомцы... Как защитить ребёнка от всего этого?

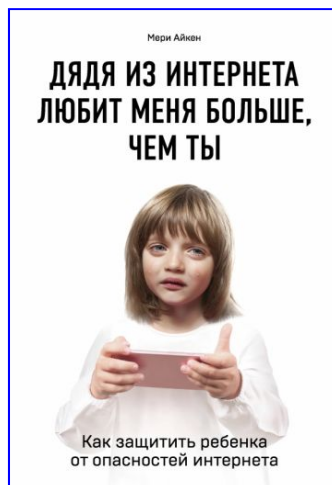
В наши дни мы все проводим много времени в интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг (травля), неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков.

Детям и подросткам интернет необходим для выполнения школьных заданий, общения с учителями и другими учениками, интерактивных игр и выполнения других задач. Это прекрасное место для обучения и общения. Но родители должны быть в курсе того, что их дети видят и слышат в интернете, с кем общаются и что рассказывают о себе.



Айкен, Мери. Дядя из интернета любит меня больше, чем ты : как защитить ребенка от опасностей интернета / М. Айкен ; перевод с англ. Е. Деревянко. - Москва : Бомбора : Эксмо, 2020. - 398 с.

Интернет скрывает больше опасностей, чем мы можем себе представить. Из этой книги вы узнаете, как вовремя распознать угрозу, предотвратить несчастные случаи, обезопасить личные данные, избавиться от интернет-зависимости и контролировать деятельность ребенка в интернете.



**Рымарева
Екатерина Александровна**

**Межпоселенческая
центральная библиотека**

**ул. Советская, 12, ОДК, 2 этаж
Телефон: 8(39158) 2-14-72**

**Соц.сети: <https://ok.ru/profile/590370695200>,
<https://vk.com/bibliotmbs>**

Сайт: <http://tmbs2011.ru>



**МБУК «ТЮХТЕТСКАЯ МБС»
МЕЖПОСЕЛЕНЧЕСКАЯ
ЦЕНТРАЛЬНАЯ БИБЛИОТЕКА**



**Как защитить
ребенка от
опасностей
интернета**

**ТЮХТЕТ
2022**

Общие рекомендации

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

Храните имена пользователей и пароли в безопасности

Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.

Периодически меняйте пароли

Настройте расписание смены паролей учетных записей каждые 3-6 месяцев или каждый раз, когда платформа сообщает о взломах или утечках данных. Вы можете использовать менеджер паролей, чтобы отслеживать все свои пароли в интернете и упростить их поиск вашим детям.

Не разглашайте личную информацию в интернете

Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.

Будьте внимательны в социальных сетях

Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

Мониторинг истории поиска в интернете

Родителям детей любого возраста рекомендуется периодически проверять историю браузера, чтобы понять, какие сайты посещают их дети.

Используйте надежное решение для кибербезопасности

Kaspersky Safe Kids помогает защитить детей, когда они находятся в сети. Это решение можно использовать на всех устройствах вашего ребенка. Оно состоит из двух приложений: одно нужно установить на устройство ребенка, второе – на смартфон родителя, чтобы просматривать отчеты и менять настройки. Встроенный родительский контроль позволяет управлять временем, которое дети проводят перед экраном на разных устройствах. Настройте и пересмотрите параметры родительского контроля на всех своих устройствах в соответствии с возрастом ваших детей. Это поможет защитить детей от доступа к неприемлемому контенту в интернете.

Проверяйте возрастные ограничения

Многие приложения и веб-сайты имеют собственные возрастные ограничения для создания учетных записей, просмотра и регистрации. Но проблема в том, что на большинстве таких сайтов фактически нет функции проверки возраста. Например, Facebook, Snapchat и Myspace разрешают доступ только с 13 лет, но дети могут указать другой возраст и зарегистрироваться в любом случае.

Объясните опасность передачи геоданных

Публичная демонстрация данных о местоположении подвергает детей различным опасностям: от сетевых интернет-хищников, которые могут найти их, до риска кражи личных данных. Убедитесь, что дети понимают, что означает, когда в приложении спрашивается, можно ли передавать данные о местоположении.

Объясните детям об опасности личных встреч с незнакомцами

Дети никогда не должны лично встречаться с незнакомцами, с которыми они общались в интернете, если за такой встречей не наблюдает родитель.

Создайте список правил использования интернета

Один из лучших способов управлять использованием интернета детьми всех возрастов – это сесть и совместно составить список правил использования интернета в соответствии с их потребностями. Вы можете показать ребенку сайты для детей и подростков, поговорить о том, почему важно установить правила, и попросить их поделиться, если он чувствует себя некомфортно или ему угрожает что-то найденное в интернете и т. д. Установите границы, но будьте реалистом.

Используйте одинаковые правила при общении онлайн и лично

Научите детей тому, что к онлайн и к личному общению применимы одни и те же правила. При общении в интернете и написании комментариев лучше оставаться добрым и вежливым, не следует писать ничего такого, что не смогли бы сказать в лицо. Это также применимо и при анонимной публикации сообщений. Публикация обидных и грубых вещей – это не только некрасиво и неприятно по отношению к другим, но также может навредить репутации вашего ребенка.

Расскажите о существовании фальшивых рекламных объявлений

Обсудите с детьми рекламные программы и мошенничество, связанное с фальшивыми рекламными объявлениями, с которыми они могут столкнуться в интернете. Некоторые объявления выглядят как реальные предложения, побуждающие загрузить фальшивое приложение, зарегистрироваться для участия в розыгрыше или предоставить личную информацию в обмен на бесплатные продукты.