**Как научить детей кибербезопасности**



В результате резкого распространения [удаленного обучения](https://www.kaspersky.ru/blog/back-to-school-infographic/2234/) родителям стало гораздо труднее контролировать действия детей в интернете. Дети проводят в сети гораздо больше времени, чем хотелось бы многим родителям. Большинство родителей не всегда могут найти время, чтобы следить за действиями детей в интернете.

Это напряженное время для родителей, которые хотят защитить своих детей. [Недавнее исследование «Лаборатории Касперского»](https://www.kaspersky.ru/blog/connected-kids/7079/) демонстрирует масштаб проблемы. Вот что происходит с сегодняшней молодежью:

* 73% подростков не представляют жизни без смартфонов, а половина из них берут с собой телефон, когда ложатся спать.
* 44% детей в возрасте от 8 до 16 лет постоянно находятся в сети, предпочитая приложения для развлечения и социальные сети.
* 40% детей раскрывают в интернете конфиденциальную информацию, включая домашний адрес.
* Треть молодых людей сообщают в интернете неверную информацию о своем возрасте.
* 37% детей сталкивались с опасностями в интернете, включая кибербуллинг, финансовые угрозы и неприемлемый контент.

Ни один родитель не сможет отследить все, что ребенок делает на своем смартфоне и ноутбуке. А даже если и смог бы, стоит ли? Технологии играют важную роль в жизни, начиная с детства, и затем во взрослой жизни. Ранние годы – шанс для ребенка развить навыки, необходимые для обеспечения безопасности в интернете.

Идеальный подход – обучать и расширять возможности детей, чтобы они сами могли обеспечить свою безопасность.

**Обучайтесь, чтобы защитить своих детей!**

Если вы хотите, чтобы ваши дети были в безопасности, сначала необходимо понять, с какими опасностями они сталкиваются, когда выходят в интернет. Когда вы разберетесь в этом сами, вы также сможете помочь детям безопасно и весело проводить время в сети.

В интернете есть множество отличных ресурсов, где рассказывается об основных угрозах, в форме, понятной даже тем, кто далек от техники. Вы можете начать с изучения материалов в [Kaspersky Resource Center](https://www.kaspersky.ru/resource-center) – бесплатном ресурсе с понятными статьями о безопасности в интернете. Здесь приведены [определения](https://www.kaspersky.ru/resource-center/definitions) наиболее важных терминов и [инфографика](https://www.kaspersky.ru/resource-center/infographics), которую можно показать детям. Также ресурс содержит[/resource-center/threats](https://www.kaspersky.ru/resource-center/threats) [новости о последних угрозах и советы о том, как обезопасить свою семью](https://www.kaspersky.ru/resource-center/threats).

В целом, существует [три категории угроз](https://www.kaspersky.ru/blog/securing-todays-kids/6894/), с которыми дети сталкиваются в интернете:

* **Незнакомцы**. Злоумышленники скрываются на сайтах, привлекающих детей, таких как сайты социальных сетей и онлайн-игр. Такие злоумышленники часто сами притворяются детьми. Этот метод называется [кэтфишинг](https://www.kaspersky.ru/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim). Также существуют хакеры и киберпреступники, атакующие всех пользователей с недостаточно высоким уровнем безопасности, не важно, ребенок это или взрослый. Они также могут попытаться обманом выяснить у ребенка пароли или платежную информацию.
* **Сверстники**. Ваш ребенок может подвергаться издевательствам или травле со стороны своих знакомых. Это часто происходит в личных чатах в социальных сетях и приложениях для обмена сообщениями. Иногда другие дети могут публиковать личную информацию вашего ребенка, что доставляет ему сильные страдания. Если такая информация имеет сексуальный характер, например интимные фотографии, это может быть уголовным преступлением.
* **Самостоятельно**. Дети без присмотра могут сами создать для себя опасные ситуации в сети. Они часто нажимают кнопки или устанавливают программное обеспечение, не понимая последствий своих действий, а также публикуют личную информацию, например дату рождения или адрес.

Некоторые из этих угроз являются **социальными угрозами** – они связаны с вымогательством или манипуляциями. Часто незнакомей завоевывает доверие ребенка, а затем пользуется этим. Чтобы защититься от этих угроз, ребенку необходимо знать, как безопасно общаться с другими людьми.

Другой тип угроз – это **цифровые угрозы**, когда кто-то использует технологии для доступа к данным. Это могут быть вредоносные программы (например, для кражи личных данных), или фишинг (вынуждение обманным путем посетить поддельный веб-сайт). Для защиты от такого типа угроз необходимо объяснить ребенку, как правильно использовать интернет и [установить надежные антивирусные программы](https://www.kaspersky.ru/home-security).

**5 советов, как поговорить с детьми о кибербезопасности**

Каждый ребенок уникален. Каждого интересуют разные темы в интернете, и все по-разному справляются с опасностями. Не существует универсально правильного способа рассказать детям о безопасности в интернете. Вы сами должны найти способы заинтересовать ребенка этой темой и помочь ему понять, что делать. Вот несколько советов, как начать диалог.

**Используйте образовательные ресурсы, предназначенные для детей**

Часто непросто говорить с детьми об их безопасности в интернете. Это особенно сложно с детьми младшего возраста, которые просто не понимают многих используемых понятий. Как объяснить третьекласснику, что в сети есть киберпреступники и сексуальные маньяки? И что еще более важно, как донести эту информацию, не напугав ребенка?

С этой проблемой сталкиваются родители во всем мире. К счастью, существуют инструменты, предназначенные для того, чтобы донести до детей такую информацию.

Отличный вариант – бесплатная электронная книга [«Каспер, Скай и Зеленый медведь»](https://media.kaspersky.com/en/Kasper%2C%20Sky%20and%20Green%20Bear.pdf) ("Kasper, Sky and the Green Bear"). Это увлекательное повествование о мальчике и его лучшем друге – волшебном медведе по имени Кума. Каждая из историй в книге помогает объяснить фундаментальные понятия кибербезопасности. Уроки объясняют, как управлять конфиденциальностью, как выбрать надежный пароль и что делать жертвам кибербуллинга.

Книгу можно скачать бесплатно. Если ваши дети предпочитают учиться по видео, [на YouTube есть мультсериал](https://www.youtube.com/watch?v=y1QSnc0MaWM&t=16s), включающий эти же уроки. Подобные истории помогают детям понять основы кибербезопасности, не причиняя им излишнее беспокойство. Детей, обладающих этими знаниями, легко научить, как сохранять безопасность в интернете.

**Установите основные правила работы в интернете.**

Интернет – огромное запутанное место, в котором хорошо бы опираться на несколько базовых правил, которые помогут понять, как оставаться в безопасности.

Вместе с ребенком договоритесь о нескольких основных правилах использования им интернета. Для маленьких детей эти правила должны быть понятными и простыми для выполнения. Например, правила могут быть такими:

* Не выходить в интернет без разрешения взрослых.
* Не более 30 минут в день перед экраном устройства.
* Разрешено использовать только определенные приложения (например, YouTube с безопасным поиском или веб-браузер с фильтрами).
* Спрашивать разрешения для установки игр.

Можно записать эти правила и время от времени обновлять их.

Когда ваш ребенок станет старше, ему, вероятно, понадобится дополнительная свобода. Можно немного расширить правила, чтобы они включали следующее:

* Никогда не называть свое настоящее имя и адрес в интернете.
* Не авторизовывать платежи в приложениях без разрешения.
* Избегать сомнительных приложений.
* Не публиковать свою личную информацию и интимные фотографии.
* Обратиться к взрослым, если кто-то пытается заставить совершить нежелательные действия.

По мере того, как ребенок вступает в подростковый возраст, придется придумывать правила, поддерживающие его жизнь в сети. С детьми более старшего возраста можно совместно создавать полезные, но не ограничивающие правила.

Выше приведены только примеры правил, которые вы можете использовать. Каждый ребенок индивидуален и имеет уникальные потребности, поэтому вам придется разработать правила, подходящие именно вашему ребенку.

**Сосредоточьтесь на возможностях, а не на опасностях**

Цифровой мир не должен пугать детей и родителей. Гораздо правильнее не беспокоиться о том, что может случиться, а сосредоточиться на обучении детей навыкам, необходимым для безопасности в сети.

Можно составить список вопросов и утверждений, обсудить его с детьми и понять, что они знают ответы на все вопросы и согласны со всеми утверждениями. Этот список может содержать следующие пункты:

* Что делать, если кто-то заставляет испытывать неловкость?
* Какую информацию можно сообщать в интернете, а что можно сообщать только лично?
* Общаться можно только с друзьями, а не с незнакомцами.
* Как проверить, является ли сайт настоящим или фальшивым?
* Почему следует избегать опасных сайтов?
* Как создать надежный пароль и использовать телефон для двухфакторной аутентификации?
* Необходимо всегда спрашивать разрешения родителей, прежде чем совершать онлайн-платеж.
* Необходимо соблюдать осторожность при размещении своих секретов и фотографий в интернете.
* При возникновении сомнений следует поговорить со взрослым и попросить о помощи.

Это навыки кибербезопасности также необходимы и взрослым. Если вы обучите ребенка этому упреждающему подходу с раннего детства, во взрослом возрасте он уже будет знать, как обеспечить безопасность.

**Создайте доверительную и уважительную атмосферу**

В идеальном мире при возникновении вопросов об онлайн-безопасности дети всегда будут обращаться к вам за помощью. Но так не бывает.

Иногда дети чувствуют, что просьба о помощи может повлечь неприятности. Например, если ребенок стал жертвой фишингового мошенничества или кэтфишинга в результате нарушения установленных правил поведения в интернете. В этом случае ребенок сталкивается со сложной дилеммой: если он попросит вашего совета, у него могут возникнуть проблемы из-за нарушения правил.

Вот почему так важно дать ребенку понять, что вы всегда поддержите его, когда он будет в вас нуждаться. Пусть ребенок знает, что самое главное – это его безопасность. Если что-то пойдет не так, постарайтесь найти положительные моменты, из которых можно извлечь уроки.

Дети также могут беспокоиться, что вы просто не поймете их проблемы. Это может произойти в случае с преследованием и травлей – проблемами, которые могут возникнуть как в реальном школьном дворе, так и в цифровом мире. В вопросах подобного рода всегда важно, чтобы дети рассказывали вам о своих чувствах, а вы серьезно относились к их проблемам. Даже если для вас это звучит банально, для них это может иметь большое значение.

Самое главное – родители должны быть примером для подражания для своих детей. Убедитесь, что ваше собственное поведение в сети всегда является безопасным и ответственным. При нахождении рядом с детьми постарайтесь ограничить время, проводимое перед экраном устройств.

**Используйте правильные инструменты безопасности**

Интернет-безопасность – это сложная задача даже для взрослых, не говоря уже о детях. Существует множество комплексных угроз, и ребенок может столкнуться с проблемами даже при соблюдении всех правил.

Итак, как взрослым обеспечить безопасность в интернете? Для этого используются различные инструменты, которые помогут избежать основных угроз, возникающих при использовании цифровых услуг. Каждое устройство в вашем доме должно иметь следующие инструменты:

**Антивирус** – это основа интернет-безопасности. Он работает в фоновом режиме и защищает от вирусов, включая трояны, шпионских программ программ-вымогателей. Когда вредоносная программа пытается заразить ваше устройство, антивирус останавливает ее.

**Антифишинг**. Фишинг – один из самых популярных методов, используемых киберпреступниками, простой, но при этом весьма деструктивный. Чтобы ни вы, ни ваш ребенок случайно не перешли по фальшивой ссылке, нужна дополнительная защита.

**Защита веб-камеры**. Если злоумышленник получит доступ к веб-камере, он сможет шпионить за вами и вашими детьми. В период школьных уроков в Zoom нельзя просто отключить веб-камеру. Вместо этого нужно средство, защищающее от такой опасности.

**Блокировщик контента**. Лучший способ не стать жертвой хакеров и вирусов – избегать небезопасного контента. Можно использовать блокировщики контента, чтобы запретить детям посещать небезопасную область интернета.

**VPN**. VPN фактически защищает ваши данные при перемещении из одного места в другое. Это особенно важно, если ребенок использует общедоступные сети Wi-Fi, например, в школе.

**Защита паролем**. Детям очень трудно соблюдать правила надежных паролей. Инструмент Защита паролей создает надежный пароль и сохраняет его для следующего входа в систему.

Программы такого типа помогают предотвратить случайную опасность, с которой можно столкнуться в сети. Знакомство с [/home-securityлинейкой продуктов «Лаборатории Касперского»](https://www.kaspersky.ru/home-security) позволит вам найти решение, отвечающее потребностям вашей семьи.

**Как обеспечить кибербезопасность детей**

Быть родителями – это самая большая ответственность, с которой только можно столкнуться. Каждый родитель хочет, чтобы его дети исследовали мир, находили себя и использовали интересные возможности, но при этом находились в безопасности и по возможности избегали рисков.

Почему родителям иногда очень тревожно наблюдать, как их дети используют электронные устройства. И возникает вопрос: эти устройства – средство обучения и источник знаний, или они подвергают детей опасностям?

Приведенные выше советы помогут продуктивно поговорить с детьми о кибербезопасности, защитить их и развить у них навыки, необходимые для обеспечения собственной безопасности.

Но иногда родителям нужна дополнительная помощь. Kaspersky Safe Kids – одна из ведущих платформ кибербезопасности для семей, предлагающая набор основных инструментов, таких как:

* **Отслеживание по GPS** позволяет контролировать местоположение детей в любое время. Вы можете установить безопасную зону на карте и получать уведомление, если ребенок вышел за ее пределы.
* **Контроль времени использования устройства** для автоматического управления использованием устройства вашим ребенком. Эта функция позволяет ограничить время, которое ребенок каждый день проводит в играх и социальных сетях, и заставить ребенка выключать устройство перед сном.
* **Фильтрация контента** обеспечивает защиту от небезопасного контента и позволяет скрыть неподходящий контент при поиске в интернете и на YouTube. Вы можете управлять уровнем ограничений по своему усмотрению.

Решение [Kaspersky Safe Kids](https://www.kaspersky.ru/safe-kids) похоже на вспомогательные колеса детского велосипеда – помогает детям учиться без слез и царапин на коленях. В непредсказуемом мире интернета каждому ребенку нужно немного больше защиты.