kaspersky в поддержку юнисеф для каждого ребенка

Безопасность детей в Сети

краткое руководство для родителей

Как настроить первый гаджет для ребенка

Первый гаджет у ребенка, согласно исследованию «Лаборатории Касперского» в Казахстане появляется уже в начальной школе, так ответили 61 респондентов. При этом, каждый десятый ребенок получает свой первый гаджет в руки уже в возрасте 5 лет, т.е. еще до того момента, как он пойдет в школу. В каком бы возрасте это не произошло, важно уделять внимание вопросу безопасности и правильно подготовить себя и своего ребенка.

- **Создайте для устройства детскую учетную запись.** Любой планшет и смартфон должны быть защищены и настроены в соответствии с возрастом его владельца.
- **Установите самые необходимые приложения.** Установите программы для определения местонахождения (например, онлайн карты), а также обучающие программы. Не забудьте **настроить параметры конфиденциальности** для каждого установленного приложения.
- **Не забудьте установить приложение для родительского контроля.** С его помощью вы сможете блокировать нежелательный контент, отслеживать время использования ребенком тех или иных приложений (и при необходимости ограничивать его), а также всегда будете знать, где находится ваш ребенок.

Совет!

Вместе с ребенком придумайте правила пользования гаджетами, которым будут следовать все члены семьи. Обсуждая правила, важно прийти к взаимопониманию и достичь согласия по поводу обязанностей и ожиданий, связанных с появлением нового устройства в жизни ребенка. Чтобы найти оптимальный баланс между цифровой и реальной жизнью, определите, в каких местах и в какое время все вы не будете пользоваться гаджетами, например за едой или перед сном. Посвящайте время занятиям, не связанным с технологиями, например чтению, подвижным играм или головоломкам, — это прекрасные альтернативы цифровым увлечениям. По мере взросления ребенка и развития технологий пересматривайте и корректируйте эти правила.

Как организовать жизнь ребенка с новым устройством и рассказать о правилах кибербезопасности?

Многих родителей волнует вопрос дисциплины, насколько сильно повлияет гаджет на то, как ребенок будет распоряжаться своим свободным временем, не будет ли пропускать академические или спортивные активности, не станет ли слишком много времени проводить в Интернете. На помощь вам придут правила, придуманные вместе с ребенком.

- **В первую очередь** покажите ребенку основные функции мобильного устройства. Например, продемонстрируйте ребенку как включать и выключать телефон, как пользоваться сотовым интернетом или подключиться к безопасному WI-FI, и как записывать контакты.

- **С самого начала открыто и спокойно обсуждайте с ребенком его цифровой опыт.** Он будет чувствовать себя в безопасности, зная, что с вами можно поделиться как хорошими, так и плохими впечатлениями.

- **Будьте в курсе последних тенденций и угроз цифрового мира** и понятно рассказывайте об этом ребенку. Ищите больше информации в Интернете, например, про кибербуллинг или цифровые навыки.

- **Объясните, что все, что ребенок опубликует в Интернете, останется там навсегда** и в будущем может сказаться на его репутации и возможностях.

- **Расскажите, что такое приватность** и почему нельзя публиковать слишком много личных данных в Интернете: никому не говорить, где он (она) живет или находится, в какой школе учится и не делиться своими учетными данными и паролями.

- **Объясните, что запросы в друзья от тех, кого ребенок не знает лично, нужно оценить и по возможности отклонить.** Дети должны четко понять: если незнакомец в Сети настойчиво пытается узнать личную информацию о нем или его родителях, то это как минимум повод для беспокойства.

- **Поощряйте любопытство, но ни в коем случае не осуждайте и не запугивайте ребенка.** Если вы будете регулярно обсуждать с детьми их цифровой опыт, делиться своим личным опытом, давать советы и рассказывать им о возможных рисках в дружеской обстановке, они увидят в вас союзника и наверняка обратятся к вам за помощью, когда столкнутся в Интернете с чем-то подозрительным.

О каких основных рисках нужно рассказать ребенку?

Современные киберпреступники нередко выбирают своей целью детей, потому что те не знают основных правил кибербезопасности и не умеют распознавать мошенничество. И мы, взрослые, должны обучить их основам интернет-безопасности, не дожидаясь неприятных ситуаций.

- **Научите** вашего ребенка распознавать фейковую рекламу, мошеннические опросы, предложение принять участие в лотерее и другие схемы, которые используются для незаконного сбора персональных данных.

- **Формируйте у ребенка привычку критично и с осторожностью относиться ко всему в Сети**, дважды подумать перед тем, как кликать по подозрительной ссылке, открывать сомнительное вложение электронной почты или сообщение от незнакомца.

- Важно донести до детей самое главное: **если в Сети ему что-то не нравится или кажется подозрительным, нужно попросить о помощи взрослого**, которому он доверяет.

- **Обсудите, какие приложения вы разрешаете скачивать на гаджет вашего ребенка.** Например, вы можете разрешить скачать TikTok, но при условии, что будет отключена геолокация и профайл будет приватным. Обратите внимание, что в интересах благополучия ребенка, многие социальные сети устанавливают минимальный возраст, с которого ребенок может регистрироваться в них.

Онлайн-покупки в интернете: как начинать говорить о финансовой безопасности?

Сайты в категории «Электронная коммерция» входят в топ-5 самых посещаемых детьми ресурсов в Интернете. Сюда относят, например, онлайн-магазины. Вполне естественно, что родителей может беспокоить вопрос, связанный с деньгами, которые ребенок может потратить в Сети.

Вот несколько правил, как научить ребенка пользоваться электронными деньгами:

- **Расскажите о том, как выглядят деньги вообще** и что из себя представляют деньги в электронном виде.
- **Установите лимит** на списание денежных средств. Можно примерно посчитать, какую сумму можно тратить в день, например на проезд или обеды в школе и дальше принимать решение о том, какой дневной лимит нужно установить.
- **Не кладите на карту ребенка сразу большую сумму,** а лучше пополняйте ее небольшими и регулярными переводами.
- **Расскажите о том**, что данные банковской карты (номер, фамилия и имя владельца, срок действия и CVV/CVC – код, который как правило находится на обратной стороне карты) это строго конфиденциальная информация и ее никому не надо сообщать.
- **Объясните**, что не стоит заходить в онлайн-банкинг, если вы подключены через общественные, незапароленные WI-FI сети, например в транспорте, кафе или кинотеатрах.

Лайфхак!

Очень важно, чтобы у ребенка сформировалось здоровое отношение к финансовым средствам, а родителям нужно периодически давать объяснения откуда берутся деньги, как и зачем нужно экономить и другие вопросы, без которых ребенку будет сложно в дальнейшей жизни. Это нужно сделать перед тем, как вы разрешите ему пользоваться финансами.

Правила онлайн-покупок на сайтах и в играх

В Интернете масса площадок, где можно потратить деньги и если ребенок распоряжается своими средствами, то будет важен разговор о планировании бюджета и безопасном осуществлении онлайн покупок. Если речь идет о доступе к аккаунту родителей, например, в онлайн-магазине, то ребенок может совершить покупки, которые точно не планировались и не были предусмотрены семейным бюджетом. Научите ребенка мерам безопасности:

- **Не доверять привлекательным предложениям**, например, если платформа выглядит подозрительно, появилось много рекламы (баннеров) и визуальных элементов, которых вы раньше не замечали, адрес страницы немного отличается от настоящего, но вас об этом предупредили и уверяют, что все нормально, так и должно быть. Скорее всего вы столкнулись с фишинговым сайтом.

- **Никому не сообщать** данные банковской карты и не называть верификационные кода из смс и push-уведомлений.

- **Не переходить** по внешним ссылкам в объявлении.

- **Не вносить предоплату** за товар, который вы еще не получили.

В игровом мире также есть возможность совершать покупки.

Многие даже бесплатные игры содержат внутриигровые покупки. За дополнительные опции, например, игровой инвентарь, внешний вид игровых персонажей, внутриигровые ресурсы приходится платить совсем не виртуальными финансами. Эти моменты тоже нужно регулярно проговаривать с детьми, обсуждать, что покупать нужно не все подряд и вообще так ли необходима та или иная покупка в виртуальном мире.

- **Ограничьте возможность таких покупок** с устройства и не привязывайте банковскую карту к игровому аккаунту, по крайней мере до тех пор, пока ребенок не научится самостоятельно и осознанно распоряжаться денежными средствами.

- Если ребенок все же купил что-то без вашего согласия, **попробуйте отменить транзакцию** через обращение в банк и написать разработчикам игры, объяснить им ситуацию, что средствами распоряжался несовершеннолетний без ведома и участия родителей.

Расскажите ребенку о мошеннических схемах в Сети

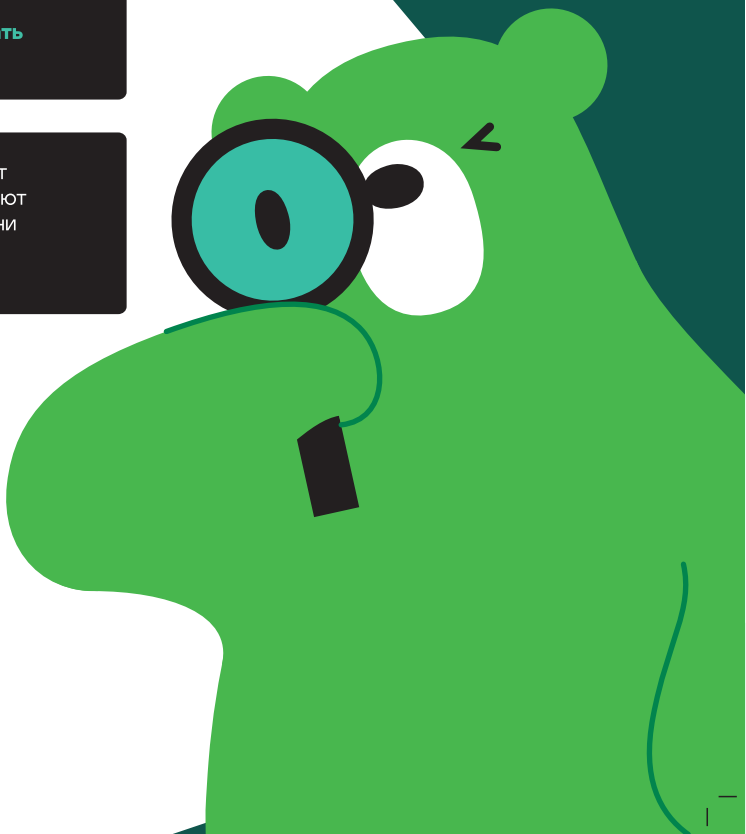
Большинство мошеннических схем действует не первый год и в целом хорошо известны. Можно рассказать ребенку о том, как защитить себя и попробовать любое подозрительное сообщение или столкновение с ситуацией, которая похожа на действия мошенников, сопоставить со следующими алгоритмами:

- Если приходит смс, в котором говорится об ошибочном переводе и просят вернуть якобы переведенные средства, то на них просто **не стоит реагировать**, даже если такое сообщение пришло от пользователя из вашей книги контактов.

- Если в сообщении даже от знакомого просят срочно помочь, например переводом денег, всегда нужно **перепроверить информацию** у первоисточника, перезвонив этому пользователю.

- Если пришло сообщение или push-уведомление от онлайн-банка о снятии денег в банкомате, **нужно немедленно рассказать родителям.**

- Если какое-то действие просят совершить немедленно или дают небольшое количество времени на обдумывание, это скорее всего **уловка мошенников.**



Родительский контроль – незаменимый помощник для защиты детей в цифровом мире

Использование родительского контроля - это легкий, но надежный способ контролировать поведение ваших детей в Сети, который позволяет предотвратить доступ к нежелательным сайтам и неприемлемому контенту. С таким приложением вы будете уверены в том, что ваши дети находятся под вашей защитой.

Среди возможных функций родительского контроля можно выделить:

- **Контроль времени использования устройства.** Такая функция позволит настроить расписание пользования гаджетом для поддержания баланса между цифровым и реальным миром.
- **Защита детей от нежелательного контента.** Функции фильтрации и блокировки предотвратят риск наткнуться на сайты для взрослых и с другим контентом, не подходящим для юного возраста.
- Защита не только в Сети. **Отслеживайте местоположение ребенка по GPS и настраивайте безопасный периметр на карте**, который ребенку нельзя покидать.
- **Уведомления о низком заряде устройства.** Эта функция поможет вам не потерять связь с ребенком.

Совет!

Уровень родительского контроля над деятельностью ребенка в интернете меняется по мере взросления ребенка. В подростковом возрасте контроль переходит в мониторинг, основанный на доверительных отношениях между родителем и ребенком. Поощряйте позитивное поведение в Интернете, практикуя его сами.

Для заметок

kaspersky в поддержку

юнисеф
для каждого ребенка

ЮНИСЕФ не продвигает какую-либо компанию, бренд, продукт или услугу.