

# 1. РЕКОМЕНДАЦИИ ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Дети и взрослые используют разные устройства, чтобы общаться и узнавать много нового в Интернете. Но важно пользоваться им очень аккуратно.

Если ты с разрешения родителей во время учебы или отдыха используешь Интернет, следуй правилам, которые описаны ниже. Они помогут тебе быть внимательным и осторожным в онлайн-сети, а также заботиться о себе, своих близких, друзьях и других людях.

**1 Используй Интернет только с разрешения родителей и будь осторожен онлайн. Старайся ограничить время, проведенное в Интернете. Делай перерывы, чтобы не переутомляться. И занимайся другими видами деятельности.**



**2 Обсуждай с родителями и близкими взрослыми те развлекательные сайты, мессенджеры или игры, в которых хочешь зарегистрироваться или которые используешь.**



**3 Вместе с родителями настрой в телефоне, на планшете или компьютере конфиденциальность: спрячь свою личную информацию, пусть ее видят только близкие, друзья и учителя.**



**4 Не публикуй в Интернете личную информацию: не пиши свою фамилию, имя, дату рождения, номер телефона, свой домашний адрес и номер школы. Исключение составляют только чаты с родителями или школьные чаты с учителями.**



**5 Не выкладывай в Интернете свои фото, видео или голосовые сообщения – ими могут воспользоваться злоумышленники.**



**6 Если у тебя есть страница или канал в социальных сетях, которые ты ведешь с разрешения родителей, ограничь доступ к своим публикациям для посторонних людей. Попроси родителей помочь тебе настроить их так, чтобы твои посты могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно, учителя).**



**7 Попроси родителей научить тебя создавать сложные пароли: пароль должен состоять из букв, цифр и специальных символов.**



**8 Не используй один и тот же пароль для разных приложений. Регулярно меняй пароли. Никогда не делись своими паролями с другими, даже с друзьями, пароль должны знать только родители.**



**9 Регулярно напоминай родителям обновлять антивирус на твоих устройствах, он защищает от вирусов и нежелательных программ. Но антивирусные программы должны выбирать взрослые.**



**10 Будь вежлив в Интернете с другими пользователями, если ты общаешься в чатах, например, чате класса.**



**11 Обсуждай с родителями или учителями ситуации, с которыми ты сталкиваешься в Интернете, и которые тебя тревожат или пугают. Обязательно прекрати общение и расскажи об этом родителям или учителям, если кто-то в Интернете:**

- обижает тебя, или ты чувствуешь себя там не так, как хочешь (например, неудобно или неприятно),
- ведет себя странно, расспрашивает о твоей семье или просит сделать что-то плохое или постыдное.



- 12 Не общайся с незнакомыми людьми и не принимай их в друзья,** если у тебя есть мессенджеры или социальные сети. Не принимай от них и не отправляй им личные сообщения. Общайся только на проверенных родителями платформах.
- 13 Если в Интернете случилось что-то плохое,** например, кто-то написал тебе что-то обидное или ты увидел что-то нехорошее в Интернете, сохрани это как картинку или сообщение, чтобы показать близким взрослым.
- 14 Если с разрешения родителей ты играешь в онлайн-игры,** то используй псевдоним, то есть выдуманное, а не настоящее имя.
- 15 Обсуждай с родителями, в какие игры ты играешь и что смотришь в Интернете.** В играх и видео в Интернете иногда показывают плохое поведение или говорят плохие слова. Выбирай вместе с родителями только безопасные сайты, игры и видео. Всегда спрашивай взрослых, если что-то непонятно.
- 16 Не всему в Интернете можно доверять.** Проверь вместе с родителями или учителями информацию и источники, особенно новости и заманчивые предложения. Избегай подозрительных ссылок и сообщений, чтобы не скачать вирусы или не попасть на обман.
- 17 Совершай покупки в Интернете только вместе с родителями.** Не покупай ничего в личных сообщениях в социальных сетях или мессенджерах — так мошенники могут украсть деньги или доступ к твоим аккаунтам.
- 18 Никогда не сообщай никому кроме родителей ПИН-код банковской карты и коды из СМС-уведомлений.**
- 19 Участвуй только в тех онлайн-занятиях, которые разрешают и предлагают родители и учителя.** Это могут быть олимпиады, конкурсы, курсы или вебинары.



Эти правила помогут тебе защитить себя от различных неприятностей в Интернете, а также создать безопасное и позитивное пространство для себя и других.

## КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

**Если что-то тебя настораживает или пугает – обязательно обратись к родителям или учителям за поддержкой и помощью!**

### Телефоны доверия, горячие линии

- ✦ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации** (бесплатно, круглосуточно) **8-800-600-31-14**
  - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.
- ✦ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**
  - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям.
- ✦ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации** (бесплатно, круглосуточно) **8-800-100-12-60#1**
- ✦ **Горячая линия поддержки по вопросам травли Травли.NET** **8-800-500-44-14** (ПН-ПТ с 10:00 до 20:00 по московскому времени).

# 3. РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) ПО КИБЕРБЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

## Уважаемые родители!

В современном мире, насыщенном цифровыми технологиями, вопрос кибербезопасности становится все более актуальным. Дети и подростки активно используют Интернет для общения, учебы и развлечений, и важно, чтобы они понимали риски и умели защищать себя в виртуальном пространстве.

Проблема кибербезопасности заключается в том, что Интернет может быть источником не только полезной информации, но и угроз. Дети и подростки могут столкнуться в онлайн с мошенничеством, кибербуллинг, вредоносным контентом и другими опасностями. Это может привести к негативным последствиям для их психического здоровья, репутации и даже физической безопасности.

Нам, взрослым, необходимо уделять внимание вопросам кибербезопасности наших детей. Обсуждая с ними правила безопасного поведения и использования онлайн-пространства, объясняя, как распознавать те или иные риски, мы можем научить детей быть устойчивыми и защищенными в сети Интернет.

### ВАЖНО

Медицинские и психолого-педагогические исследования, а также рекомендации СанПиН показывают, что использование электронных устройств и Интернета лучше **полностью исключить в раннем детстве (до 3 лет)**. Намного полезнее для детей живое общение, продуктивная развивающая деятельность, чтение, рисование и игры со сверстниками.

**В старшем дошкольном возрасте** экранное время может составлять **не более 1 часа в день** и только в присутствии взрослых. **В младшем школьном возрасте** продолжительность использования цифровых устройств **не должна превышать 1,5 часов**. **В подростковом и юношеском возрастах — не более 2 часов в день**.

При этом во всех возрастах непрерывный просмотр или онлайн-активность должны чередоваться с гимнастикой для глаз и другими видами интеллектуальной и физической деятельности. Каждый родитель, опираясь на рекомендации, стоит перед серьезным решением: определить, сколько времени пойдет его ребенку на пользу с учетом возраста, учебы, общения и отдыха.

**Вы можете воспользоваться следующими простыми рекомендациями, чтобы помочь детям и подросткам быть более компетентными, осознанными, внимательными и осмотрительными в интернет-среде.**



### 1 Обучайте детей и подростков основам кибербезопасности

- ✦ Поговорите с детьми о том, почему важно защищать личные данные и как это может помочь избежать проблем.
- ✦ Проверяйте настройки конфиденциальности и научите детей создавать надежные пароли, использовать двухфакторную аутентификацию и не делиться с незнакомцами личной информацией в Интернете.
  - **Надежный пароль** — это сложный пароль, состоящий из букв, цифр и символов. Обычно его трудно угадать или подобрать. Важно периодически менять пароли в мессенджерах, электронной почте и социальных сетях.
  - **Личная информация** — фамилия и имя, полная дата рождения, домашний адрес, номер телефона, номер школы и класса, информация о семье, другая личная информация (например, паспортные данные, данные медицинского полиса, СНИЛС и др.). Этими сведениями могут воспользоваться злоумышленники. Даже фото, видео и голосовые сообщения могут быть ими использованы.
- ✦ Используйте надежное антивирусное программное обеспечение на Ваших устройствах и регулярно обновляйте его. Обсуждайте с ребенком или подростком важность защиты от вредоносных программ.
- ✦ Рассказывайте о подозрительных людях в Интернете. Объясните ребенку или подростку, что не стоит общаться с незнакомцами в сети Интернет, и что делать, если кто-то ведет себя странно или пытается заставить делать что-то неприемлемое.
- ✦ Помогите детям и подросткам понять и осознать, почему не стоит отвечать на сообщения и звонки с незнакомых номеров по мобильной связи, в мессенджерах и социальных сетях. Объясните, что это может привести к нежелательным контактам и опасности.
- ✦ Обучайте распознаванию подозрительных ссылок. Расскажите ребенку или подростку о рисках перехода по ссылкам из неизвестных источников и научите его проверять ссылки перед переходом.

### 2 Обсуждайте и устанавливайте семейные правила использования Интернета и кибергигиены

- ✦ Определите вместе с ребенком или подростком, сколько времени он может проводить в Интернете, какие сайты он может посещать и с кем общаться, какие мессенджеры и социальные сети он может использовать.
- ✦ Если Ваш ребенок старшего дошкольного или младшего школьного возраста пользуется мобильным устройством или персональным компьютером, установите программы родительского контроля, чтобы ограничить доступ к нежелательному контенту и отслеживать активность в Интернете.
- ✦ Установите разумные ограничения на использование цифровых устройств и перерывы для других видов деятельности. Это поможет избежать переутомления и зависимости от Интернета.

### 3 Поддерживайте атмосферу доверия и регулярно обсуждайте с ребенком или подростком онлайн-опыт

- ✦ Поощряйте детей и подростков обсуждать с Вами вопросы, связанные с Интернетом и информационной безопасностью, делиться своими переживаниями, опасениями и проблемами, связанными с онлайн-пространством, без страха наказания. Проводите беседы о том, что делают дети в Интернете, с кем общаются, во что играют, какие сайты посещают, какой медиаконтент им интересен, и обсуждайте возможные риски. Рассмотрите возможность совместного просмотра контента и обсуждения увиденного.

### 4 Будьте примером для подражания

- ✦ Показывайте ребенку или подростку, как Вы сами соблюдаете правила информационной безопасности, и обсуждайте с ним Ваши совместные действия в Интернете. Показывайте, как правильно вести себя в Интернете, не нарушайте правила и нормы поведения в онлайн при ребенке, объясняйте, почему важно соблюдать эти правила.

## 5 Развивайте у детей навыки обращения за помощью и сообщения об опасности Вам и другим надежным взрослым (родственникам, учителям, сотрудникам правоохранительных органов)

- Обучайте детей и подростков тому, как фиксировать онлайн-риски с помощью скриншотов, сохранения видео- и аудиосообщений от незнакомцев. Все это может стать серьезной доказательной базой в критических ситуациях. Этот навык может помочь не только в виртуальном мире, но и в реальной жизни.

## 6 Помогайте детям и подросткам развивать критическое мышление

- Научите их анализировать информацию в Интернете, распознавать опасности: объясните, как распознавать мошенничество, кибертравлю и другие формы онлайн-угроз. Приводите примеры кибервиктимизации, ненадлежащего, рискованного и опасного онлайн-поведения, чтобы дети и подростки могли лучше понять, как избежать подобных ситуаций.
- Развивайте у ребенка аналитические навыки, чтобы он мог оценивать информацию в Интернете, сомневаться в достоверности источников и отличать достоверные источники от недостоверных. Расскажите, что не вся информация в Сети является правдивой.
  - Придумайте «волшебное слово-пароль», которое будете знать только Вы и Ваш ребенок, чтобы он мог распознать опасность: в случае, если ребенок ответил на сообщение или звонок незнакомца, с помощью этого слова ему будет проще распознать опасность.

## 7 Проявляйте поддержку и вовлеченность

- Постарайтесь быть вовлеченными в онлайн-активности: участвуйте в играх и социальных сетях вместе с детьми и подростками, чтобы лучше понять их интересы и окружение, это позволит поддерживать доверительный контакт с ними.
- Поощряйте детей и подростков заниматься безопасными и конструктивными офлайн и при необходимости онлайн-активностями, такими как образовательные игры, спорт или творческие проекты. Активная, интересная и насыщенная положительными эмоциями и событиями реальная жизнь — мощный источник позитивной самореализации без «бегства» в виртуальный мир.

## 8 Отработайте совместно с ребенком действия в ситуациях риска

- Важно заранее объяснить ребенку, как правильно действовать при столкновении с опасными онлайн-коммуникациями:
  - не вступать в перепалку, сразу заблокировать агрессора или мошенника, сохранить скриншоты переписки в качестве доказательств и обязательно рассказать о ситуации взрослым — родителям, учителю или обратиться в поддержку платформы, где произошел инцидент.
- Обращайтесь за помощью: если Вы заметили, что Ваш ребенок стал жертвой кибервиктимизации или проявляет опасное поведение в Интернете, не стесняйтесь обращаться за помощью к специалистам.

## 9 Регулярно обновляйте знания о кибербезопасности и кибергигиене, отслеживайте изменения в законодательстве и правилах платформ

- Следите за новостями и тенденциями в области кибербезопасности, изучайте новые методы защиты от киберпреступлений. Будьте в курсе изменений в законодательстве и правилах использования платформ, чтобы обеспечить максимальную защиту Вашего ребенка или подростка, адаптируйте свои подходы к обеспечению безопасности в соответствии с изменениями в Интернете.

### Алгоритм действий родителя при обнаружении подозрительной онлайн-активности ребенка

- Обратите внимание на изменения в поведении ребенка или подростка. Если Вы заметили, что он стал более замкнутым, погруженным в онлайн, раздражительным или проявляет другие нетипичные для него эмоции, это может быть сигналом о проблемах в Интернете.
- Поговорите с ребенком. Выясните, что именно его беспокоит, и предложите свою помощь.
- Обратитесь за помощью к специалистам. Если Вы не можете самостоятельно решить проблему, обратитесь к психологу, социальному педагогу, психотерапевту или другим специалистам.

В ситуациях, когда ребенок сообщает Вам о совершенном в отношении него преступлении воспользуйтесь 8 памяткой [Навигатора профилактики виктимизации детей и подростков \(2024\)](#)



Более подробные рекомендации для родителей Вы найдете в пособии [«Риски в цифровой среде: диагностика, профилактика, коррекция»](#). — М: АНО «Центр глобальной ИТ-кооперации», 2024. — 152 с.



## КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ



### Телефоны доверия, горячие линии

- Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
  - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- Всероссийский Детский телефон доверия 8-800-2000-122**
  - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
  - Также для обращения доступна короткая комбинация **123** (бесплатно, круглосуточно).
- Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
  - ПН-ПТ с 10:00 до 20:00 по московскому времени.

#### Онлайн-помощь

- Горячая линия «Дети Онлайн» <http://detionline.com/helpline/about>
- ЧАТ-БОТ «Добрыня» (антибуллинг) <https://t.me/BylingBot>
- Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь» — сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете <https://youthombudsman.ru/help>
- Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

#### Информационно-методические материалы и ресурсы

- Касперский детям <https://kids.kaspersky.ru/>