

8 Участвуй только в безопасных онлайн-активностях

Выбирай безопасные сайты и приложения, используй только проверенные платформы для общения и игр. Участвуй в тех образовательных онлайн-активностях (олимпиадах, конкурсах, курсах, вебинарах и других событиях), которые проверены твоими близкими взрослыми, и которые помогут тебе развивать навыки и знания.



9 Развивай критическое мышление

Проверяй и перепроверяй информацию: не верь всему, что видишь в интернете. Проверяй факты и источники информации, особенно если это касается новостей или заманчивых предложений.

Будь осторожен с рекламой: не кликай на подозрительные ссылки, которые могут привести к вирусам или мошенничеству. Помни, что ссылки из подозрительных писем, сообщений и постов в мессенджерах или социальных сетях могут содержать вредоносное программное обеспечение и заразить твой компьютер или мобильное устройство.



10 Будь бдителен при онлайн-покупках

Не доверяй сайтам, которые выглядят подозрительно, и проверяй отзывы о продавцах перед покупкой товаров онлайн. Совершай покупки только вместе с родителями.

Не делай покупки в личных сообщениях в мессенджерах или социальных сетях: мошенники могут получить доступ и контроль к денежным средствам и твоим аккаунтам.

Будь предельно осторожен с предложениями сделать донат (добровольное денежное пожертвование).



11 Никогда не продавай свои аккаунты в мессенджерах, социальных сетях, онлайн-играх, а также СИМ-карты и банковские карты!

Мошенники могут воспользоваться ими в корыстных целях, но ответственность придется нести тебе, твоим родителям и близким. Никогда не сообщай номер, ПИН-код, CVC-код и другие данные своей банковской карты, а также коды из СМС-уведомлений и электронных писем посторонним людям.



12 Изучи правила и нормы поведения в Интернете

Придерживайся правил, чтобы избежать конфликтов и неприятных ситуаций. Соблюдай законы, действующие в нашей стране — они также распространяются на поисковые запросы, поведение людей в Интернете и публикуемый ими контент.

Будь осторожен с публикациями в социальных сетях и сообщениями в мессенджерах. То, что кажется забавным или безобидным, может нарушать закон, или оказаться вирусным и быстро распространиться среди большой, не всегда желательной, аудитории. Прежде чем разместить пост или отправить сообщение, внимательно оценивай его содержание. **Помни:** Интернет — это публичное пространство, и необдуманные поступки могут иметь серьезные последствия.

Если ты столкнулся с противоправным контентом в Интернете, сообщи об этом родителям и/или учителям, а также отправь ссылки и скриншоты в правоохранительные органы и Роскомнадзор.



Кибербезопасность, цифровая грамотность, навыки распознавания онлайн-рисков — это важный аспект твоей жизни в современном мире!

Следуя этим рекомендациям, ты сможешь защитить себя от различных онлайн-угроз, а также создать безопасное и позитивное онлайн-пространство для себя и других.

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 омбудсмана, 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/>

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, кибербуллингом, 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.