

2. РЕКОМЕНДАЦИИ ДЛЯ ПОДРОСТКОВ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Современный мир стремительно меняется, развиваются онлайн-технологии, различные гаджеты и девайсы, которые все мы используем в повседневной жизни. Интернет также стал некоторой частью нашей реальности и инструментом, с помощью которого можно общаться, учиться, узнавать новое. И, как с любым инструментом, им нужно пользоваться аккуратно, помня о некоторых рисках и угрозах виртуального мира.

Если ты во время учебы или досуга используешь интернет и его ресурсы на смартфоне, планшете или персональном компьютере, пожалуйста, воспользуйся следующими рекомендациями. Они помогут тебе быть более компетентным, осознанным, внимательным и осмотрительным в онлайн-пространстве, проявить заботу о себе, своих близких и других людях.

1 Помни о защите своей личной информации

Не делись в онлайн своими или чужими личными данными: никогда не публикуй свои фамилию и имя, полную дату рождения, домашний адрес, номер телефона, номер школы и класса, в которых учишься, информацию о семье или другую личную информацию в интернете. Этими сведениями могут воспользоваться злоумышленники. Даже твои фото, видео и голосовые сообщения могут быть ими использованы. Используй никнеймы (псевдонимы) при регистрации на сайтах, в социальных сетях, мессенджерах или в играх, а не свое настоящее имя.



Исключение: официальные платформы (например, Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг» или Госуслуги) и мессенджеры (например, Сферум, Max).

2 Используй настройки конфиденциальности

На мобильных устройствах, в мессенджерах, социальных сетях, чтобы ограничить доступ к твоей информации. Убедись, что твои профили и аккаунты настроены так, чтобы только близкие, друзья и учителя могли видеть личную информацию. Если ты активно ведешь свою страницу, канал или паблик, ограничь доступ к своим постам: настрой видимость своих публикаций так, чтобы их могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно учителя).



3 Применяй безопасные пароли и не сообщай их никому

Надежный пароль - это сложный пароль, состоящий из букв, цифр и символов. Обычно его трудно угадать или подобрать. Не используй один и тот же пароль для разных аккаунтов. Никогда не делись своими паролями с другими, даже с друзьями. Регулярно меняй пароли, чтобы обезопасить себя.



4 Используй антивирусное программное обеспечение и фаервол

Для защиты от вредоносных программ и нежелательного трафика.



5 Обсуждай вопросы онлайн-безопасности с родителями или учителями

Сообщай о проблемах: если кто-то угрожает тебе или ты чувствуешь себя некомфортно в интернете, расскажи об этом взрослым или учителям. Обращаться за помощью и принимать ее - важный навык современного человека. Сохраняй доказательства: если ты стал жертвой кибербуллинга, другого онлайн-насилия или мошенничества, сохраняй скриншоты и сообщения как доказательства. Помни о кибербуллинге: если ты стал жертвой онлайн-травли, сообщи об этом взрослым. Будь внимателен к онлайн-играм или медиаконтенту: некоторые игры могут содержать агрессивное поведение, а видео и фото - неподобающий, токсичный контент. Обсуждай с родителями, в какие игры ты играешь, какие онлайн-платформы и контент тебе интересны.



6 Старайся придерживаться безопасного общения

Интернет так устроен, что иногда может сложиться иллюзия доверия, безопасности, анонимности и конфиденциальности. Может показаться, что ты хорошо знаешь человека, с которым в реальной жизни никогда не встречался, но уже какое-то время общаешься в Сети. Но это может быть небезопасным. Поэтому не общайся с незнакомыми людьми в интернете и не принимай запросы в друзья от тех, кого не знаешь в реальной жизни. Не отправляй личные сообщения незнакомцам: будь осторожен с тем, что ты пишешь и отправляешь в личных сообщениях. Если кто-то в интернете ведёт себя странно или пытается заставить тебя делать что-то, о чём тебе может быть стыдно или ты не хочешь говорить, прекрати общение и сообщи об этом взрослым. Самый надежный способ позаботиться о себе - прервать контакт с незнакомым пользователем, который может писать или звонить тебе.



7 Позаботься о своей кибергигиене

Старайся ограничить время, проведённое в интернете. Делай перерывы и занимайся другими видами деятельности, чтобы избежать переутомления, усталости глаз и зависимости от цифровых устройств.



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 или постов в социальных сетях содержат вредоносное программное обеспечение и загрузить его на 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.



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 ПИН-код своей банковской карты, а также коды из СМС-уведомлений посторонним людям.



12 Изучи правила и нормы поведения в интернете

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.



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** (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 «Ребёнок в опасности» Следственного комитета Российской Федерации** (бесплатно, круглосуточно) 8-800-100-12-60#1. Также для обращения доступна короткая комбинация 123.

✳ **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/>