

Как обеспечить информационную безопасность ребенка. Общие правила

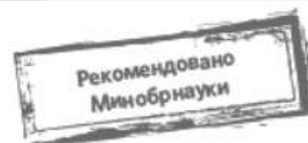


- 1** Ваше внимание к ребенку – главный метод защиты. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него.
- 2** Внимательно изучите связанные аккаунты в социальных сервисах, где есть аккаунт ребенка. Это vkontakte.ru, blogs.mail.ru и др. Смотрите, что размещают группы и люди, на которых он подписан, включая фото и видео.
- 3** Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но при этом содержать и ссылки на нежелательные и опасные сайты. Например, порно-сайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес.
- 4** Поощряйте вашего ребенка сообщать обо всем странном или отталкивающем. Не реагируйте слишком остро, когда он это делает. Из-за опасения потерять доступ к интернету дети не говорят родителям о проблемах, а также могут начать использовать интернет вне дома и школы.
- 5** Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь его друзьями в интернете так же, как интересуетесь реальными друзьями.

ПАМЯТКА

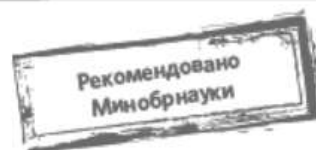
для школьников

Как безопасно общаться в социальных сетях



- 1 Ограничь список друзей.** У тебя в друзьях не должно быть случайных и незнакомых людей.
- 2 Защищай свою частную жизнь.** Не указывай пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.
- 3 Защищай свою репутацию.** Держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели то, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.
- 4 Не используй реальное имя.** Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.
- 5 Не сообщай свое местоположение.** Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.
- 6 Используй сложные пароли.** При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.
- 7 Используй разные пароли.** Для социальной сети, почты и других сайтов создавай разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

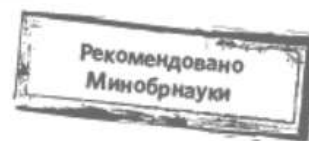
Как защититься от кибербуллинга



КИБЕРБУЛЛИНГ – ситуация, когда человека в Сети преследуют сообщениями, которые содержат оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование.

- 1 Не бросайся в бой.** Лучший способ: посоветоваться, как себя вести, и если нет того, к кому можно обратиться, то вначале нужно успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
- 2 Управляй своей киберрепутацией.** Ищи способы выяснить, кто стоит за анонимным аккаунтом обидчика. Анонимность в Сети мнимая.
- 3 Береги виртуальную честь смолоду.** Не веди хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет сложно.
- 4 Игнорируй единичный негатив.** Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- 5 Блокируй агрессора.** В программах обмена мгновенными сообщениями, в социальных сетях можно запретить конкретным адресам присылать сообщения.
- 6 Поддержи жертву кибербуллинга.** Покажи преследователю, что оцениваешь его действия негативно. Сообщи взрослым о факте агрессивного поведения в Сети.

Как защититься от компьютерных вирусов



КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

- 1 Загрузи современную операционную систему.** Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.
- 2 Обновляй операционную систему.** Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.
- 3 Используй права пользователя.** Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.
- 4 Не рискуй.** Используй антивирусные программные продукты проверенных производителей с автоматическим обновлением баз.
- 5 Ограничь доступ к своему компьютеру.** Не разрешай посторонним пользоваться своим компьютером.
- 6 Выбирай тщательно источники.** Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.