Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.

Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию. Шифрование может производиться банковской организацией, например, номер банковской карты тоже индивидуальный, он не повторяется и принадлежит исключительно держателю банковской карты.

Как общаться в Сети?

1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.

2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.

3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни.

4. Не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

Как защитить персональные данные в Сети

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.

4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

5. Используйте только сложные пароли, разные для разных учетных записей и сервисов.

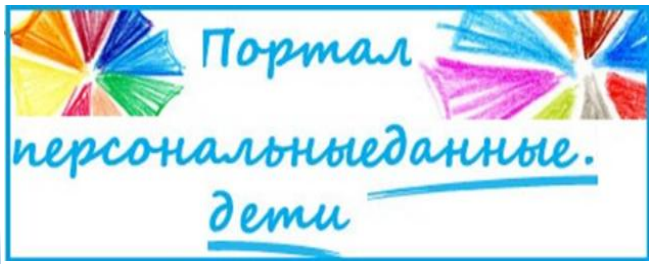
6. Старайтесь периодически менять пароли.

7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

РОСКОМНАДЗОР

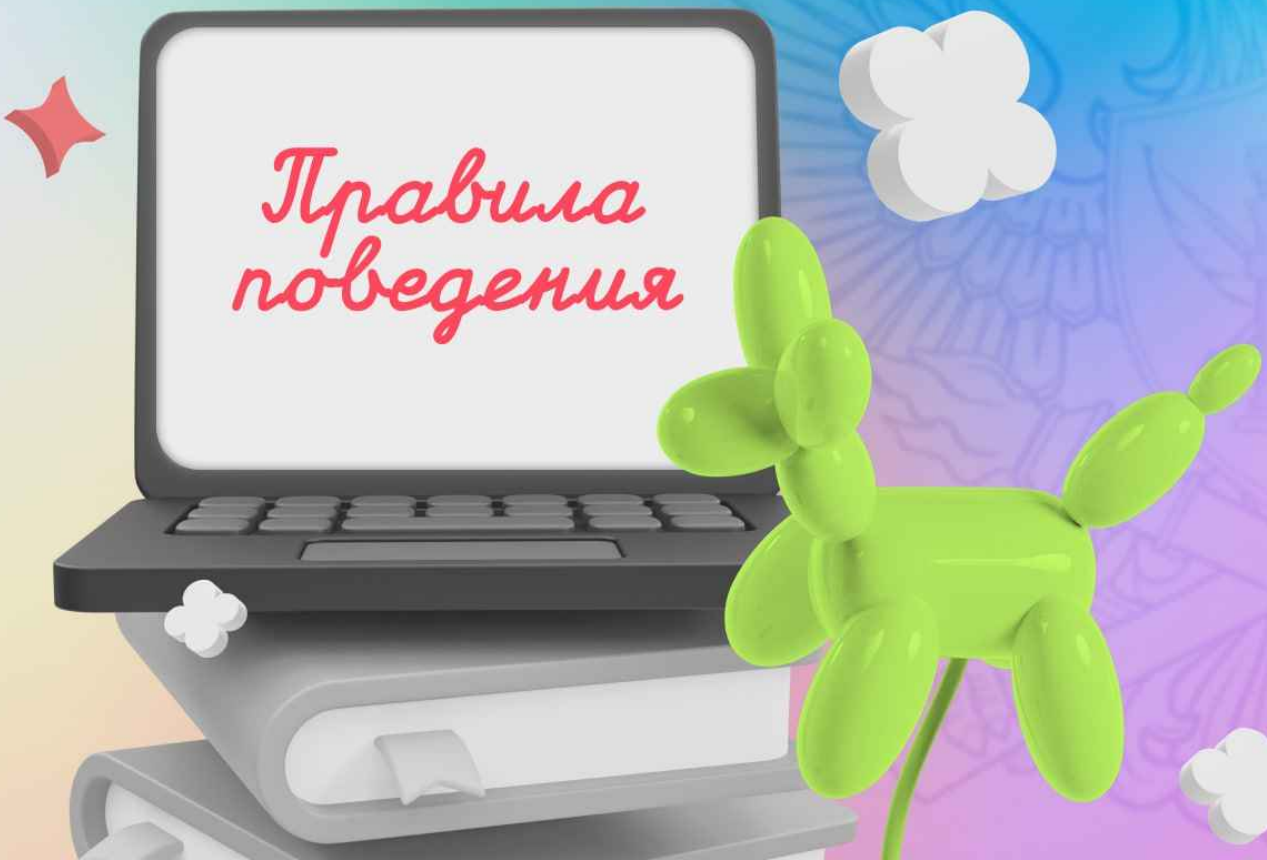
Управление Роскомнадзора по Алтайскому краю и Республике Алтай

Правила общения в сети «Интернет»



РОСКОМНАДЗОР

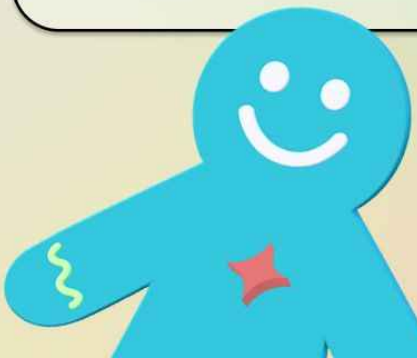
Дети в интернете



Что нужно делать?

Рассказывай родителям, если встретил в Сети что-то, что вызывает беспокойство, неудобство или страх.

Учись. Узнавай о киберугрозах и правилах пользования сайтами и социальными сетями.



РОСКОМНАДЗОР

Что *нужно* делать?

Устанавливай настройки приватности. Открывай свою страничку только для друзей, с которыми знаком лично.

Перед публикацией поста или отправкой сообщения спрашивай себя: насколько комфортно я буду чувствовать себя, показывая эти материалы незнакомцу?

Перепроверяй сообщения от друзей с просьбой срочно выслать денег. Сначала перезвони другу и удостоверься, что просьба действительно направлена от него.

РОСКОМНАДЗОР

что нельзя делать?

Не встречайся лично с теми, с кем общался только по Сети.

Не указывай свои полные фамилию, имя, отчество, возраст, место жительства и учебы.

Не публикуй фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные: названия улиц, государственные номера автомобилей, название школы.

Не выкладывай фотографии своей квартиры: обстановку и ценности.

РОСКОМНАДЗОР

реальные последствия виртуального общения

19% детей жалеют о своих публикациях в Сети

16% детей признались, что к ним пытались втереться в доверие незнакомые взрослые

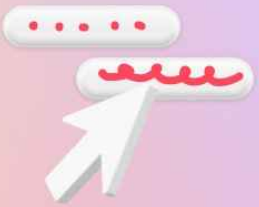
✱ По данным Kaspersky Safe Kids

РОСКОМНАДЗОР

что нельзя делать?

Не устанавливай приложения для соцсетей, которые позволяют отследить активность подписчиков на твоей странице. Как правило, такие сервисы запрашивают логин и пароль от аккаунта, которые могут использоваться для взлома страницы.

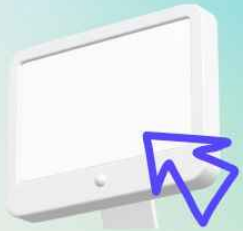
Не отправляй важные документы через социальные сети и не публикуй фотографии документов.



Проявляй осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей. Особенно, если не знаком лично с отправителем.

РОСКОМНАДЗОР

Что *нужно* делать?



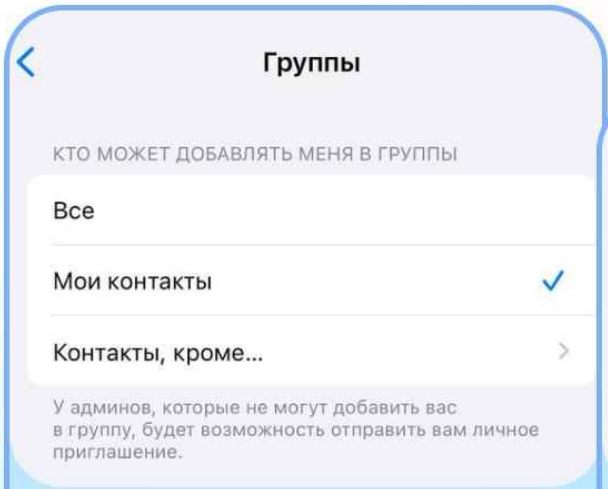
Для входа в соцсети используй только доверенные браузеры, обновляй антивирусные программы и сканируй компьютер на наличие вредоносных программ.

Не вводи логин и пароль от соцсетей и других сервисов при подключении к бесплатному общественному Wi-Fi, который не запрашивает авторизацию по номеру телефона.

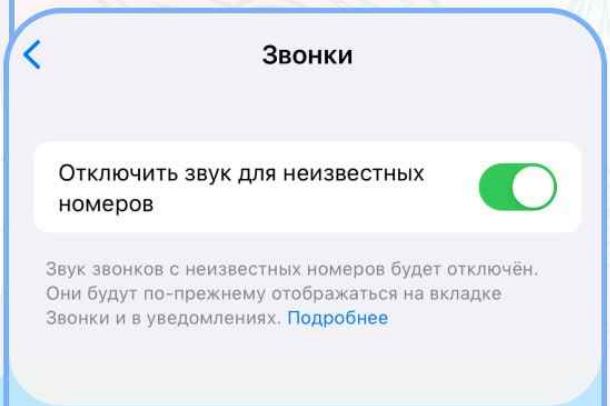
Используй разные пароли для соцсети и для электронной почты, которую указываешь в ней.

РОСКОМНАДЗОР

WhatsApp: отключить звук для звонков с незнакомых номеров и добавление в группы



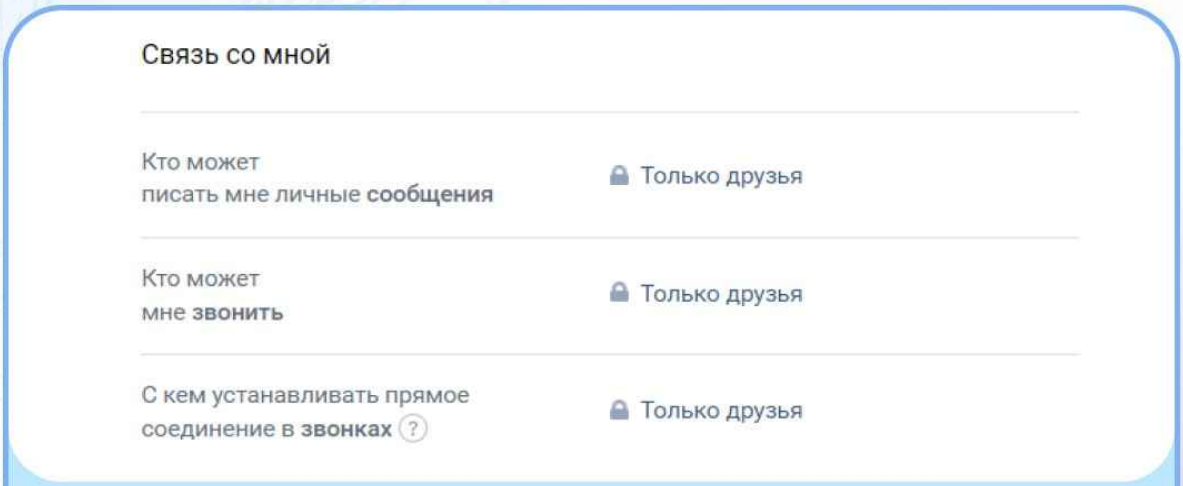
Настройки
→ Конфиденциальность
→ Группы



Настройки
→ Конфиденциальность
→ Звонки

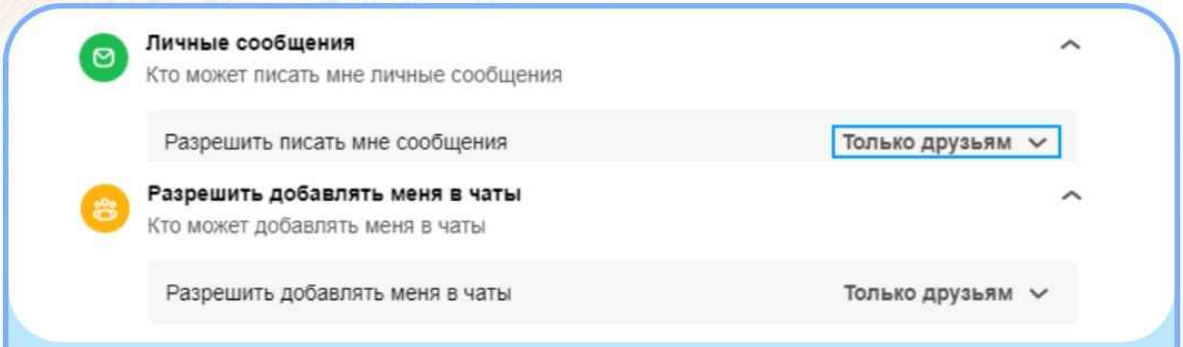
РОСКОМНАДЗОР

VK: отключить личные сообщения от пользователей не из списка друзей

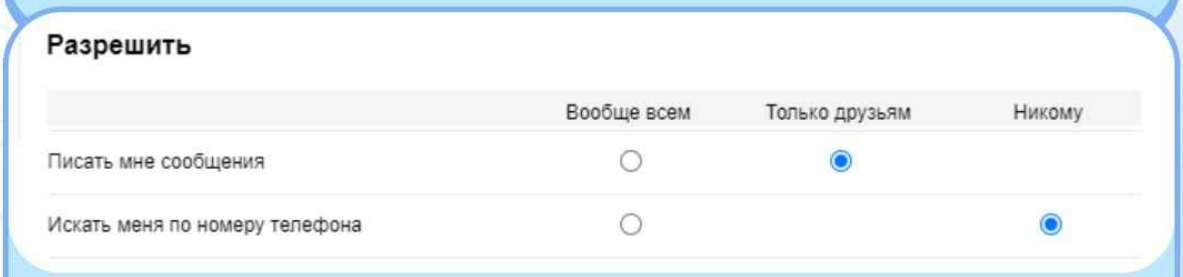


Настройки → Приватность → Связь со мной

ОК: отключить личные сообщения от пользователей не из списка друзей



Настройки → Личные сообщения



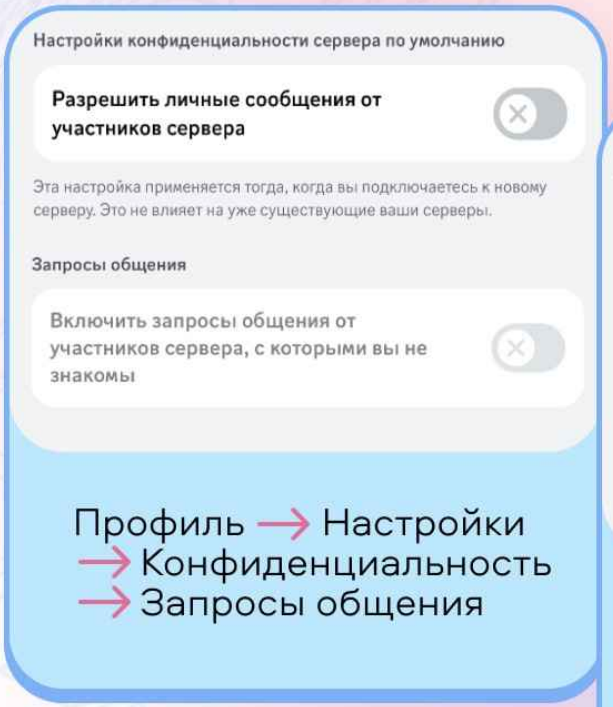
Настройки → Приватность

Как ограничить получение личных сообщений от незнакомцев?

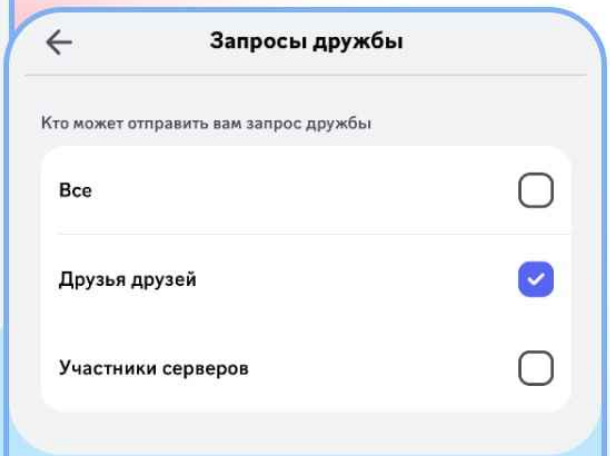
Пошаговая инструкция

РОСКОМНАДЗОР

Discord: отключить запросы общения от незнакомцев



Профиль → Настройки → Конфиденциальность → Запросы общения



Профиль → Настройки → Конфиденциальность → Запросы дружбы

Провокаторы в сети Интернет склоняют россиян к экстремизму, терроризму и другим серьезным преступлениям.

В группе риска - подростки и молодежь !

РОДИТЕЛЯМ ВАЖНО:

Заранее проинформировать детей обо всех возможных угрозах сети Интернет, в том числе о вербовке в террористические организации.

Научить ребенка не отвечать на сомнительные предложения и сообщения в социальных сетях.

Как с этим бороться?

Обучать детей навыкам цифровой грамотности:

- рассказывать о рисках
- развивать способность анализировать информацию
- обучать критическому мышлению
- подавать пример осознанных решений в цифровой среде

РОСКОМНАДЗОР

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

- кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;
- кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;
- с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;
- и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.

Таких идентифицирующих данных огромное множество, к ним относятся:
фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Так, *если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.*

Получается, что персональные данные - **это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которые позволяют идентифицировать вас.**

В целом можно сказать, что персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

Какие бывают персональные данные?

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся:
отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.

К специальным персональным данным относятся:

расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам.

Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить как конкретного человека, установить нашу личность.