

Личная информация и цифровая безопасность



Личная информация в сети требует осторожности каждый день.

Что важно беречь в сети

Имя, фото, адрес, пароль и даже геолокация могут стать личными данными.



Вопрос классу: что о вас видно в сети?

Что уже опубликовано

Вспомните, что вы уже писали в профилях и чатах: имя, город, школу, номер телефона или фото. Даже одна деталь иногда помогает постороннему собрать полную картину.

Где информация может появиться

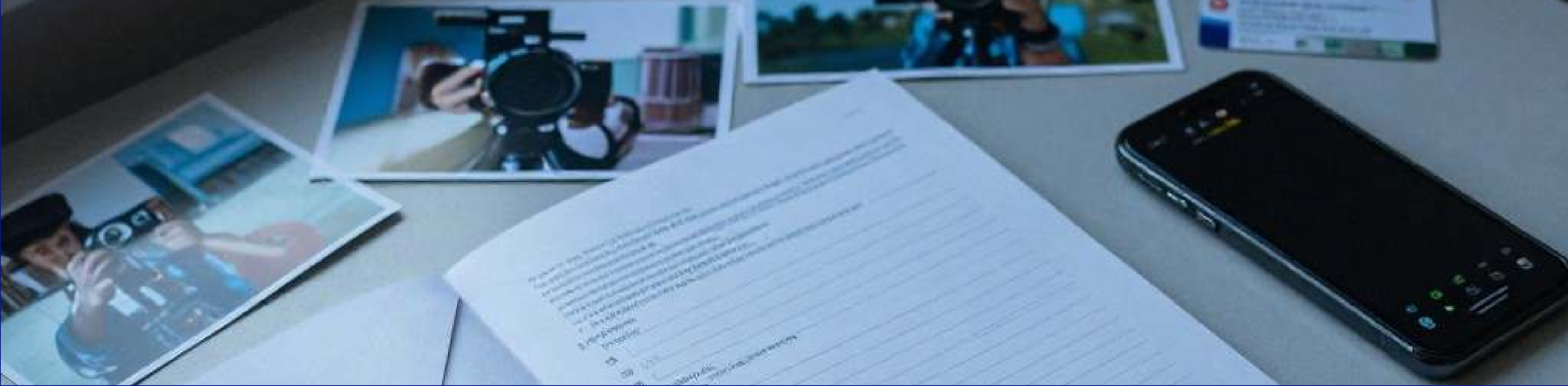
Не всё, что видно только друзьям, остаётся закрытым навсегда. Скриншот, пересылка и случайный репост быстро делают частную информацию публичной, поэтому важно думать заранее.

Мелочи тоже работают

Люди часто недооценивают простые сведения вроде названия школы или любимого маршрута. Но именно такие кусочки помогают связать аккаунт с реальным человеком и его привычками.

Пора навести порядок

Полезно иногда проверять свои старые публикации и сообщения. Так легче понять, какие данные стоит удалить, скрыть или больше никогда не отправлять незнакомцам.



Какие данные считаются личными

Контакты и адрес

К личным данным относятся имя, фамилия, номер телефона и адрес. По ним человека можно найти, связаться с ним или понять, где он живёт и учится.

Учёба и привычки

Школа, класс, дата рождения и расписание занятий тоже важны. В сочетании с фото они помогают незнакомцу точнее определить, кто вы и где бываете.

Изображения подсказывают больше

Фотографии и видео часто выдают больше, чем кажется. На фоне могут быть таблички, номера домов, формы, билеты, документы или экран с нужной информацией.

Самые чувствительные данные

Геолокация, пароли, коды из SMS и личные сообщения особенно чувствительны. Если они попадут не туда, можно потерять доступ к аккаунту или деньгам.

Никнейм тоже имеет значение

Даже никнейм иногда становится личной информацией, если он совпадает с именем, годом рождения или названием школы. Лучше выбирать нейтральные варианты без лишних подсказок.

Истории о том, как детали складываются в портрет

Фото, которое многое выдает

На фото в форме видно школу, район и даже время, когда ребёнок обычно бывает рядом. Если рядом добавлены имя и класс, незнакомцу уже легче связать снимок с конкретным учеником.

Геометка и маршрут

Пост о поездке кажется обычным, но отметка на карте и время публикации показывают, где человек находится прямо сейчас. В сочетании с привычными маршрутами это может сделать его легко узнаваемым.

Портрет из мелочей

Даже короткая биография в профиле складывается из маленьких деталей: город, любимая секция, имя питомца и дата рождения. Вместе они образуют заметный цифровой след, который трудно стереть одним нажатием.



Зачем злоумышленникам ваши данные

1. Доступ к аккаунтам

Для начала данные используют, чтобы обманом получить доступ к аккаунтам. Зная имя, школу или друзей, мошеннику проще сделать сообщение правдоподобным и вызвать доверие.

2. Кража денег

Потом информация помогает выманивать деньги. Если злоумышленник знает, как вы общаетесь и кому доверяете, он может попросить перевод, код или помощь от имени знакомого.

3. Обман через доверие

Ещё один риск — фишинг и поддельные страницы входа. Личные данные делают такие ловушки убедительнее, а значит, повышают шанс, что человек сам передаст пароль.

4. Травля и шантаж

Иногда данные используют для кибербуллинга и давления. Скриншоты, переписки и фотографии могут превратить в повод для насмешек, шантажа или распространения слухов.

5. Долгий след утечки

Если информация уже утекла, последствия не заканчиваются сразу. Появляются спам, навязчивые сообщения и фальшивые аккаунты, которые выдают себя за настоящего человека.

Фишинг и обман под видом «своих»

1. Сначала остановитесь

Сообщение может выглядеть как обычная просьба от друга или знакомого, но важно не спешить. Настоящий человек редко требует код, пароль или деньги прямо сейчас.

2. Давление — тревожный знак

Мошенники часто давят на эмоции: пугают, торопят или обещают помощь. Чем сильнее срочность, тем внимательнее нужно проверить, кто пишет и зачем.

3. Проверяйте сообщение

Если вас просят перейти по ссылке, сначала посмотрите на адрес и стиль сообщения. Ошибки, странные символы и непривычный тон часто выдают подделку.

4. Уточняйте отдельно

Лучше связаться с человеком другим способом: позвонить, написать в другом чате или спросить лично. Так вы быстро узнаете, действительно ли он отправлял просьбу.



Что нельзя сообщать никому

1. Пароли и коды

Пароли и коды подтверждения нельзя пересылать даже близким знакомым. Если их узнает посторонний, он может войти в аккаунт и менять настройки без вашего ведома.

2. Документы и карты

Паспортные данные, номер карты и фото документов подходят только для официальных сервисов. В обычном чате такие сведения могут быстро попасть к мошенникам.

3. Адрес и перемещения

Точный адрес, маршрут до дома и расписание поездок помогают понять, где вы живёте и когда вас нет дома. Этой информацией легко злоупотребить.

4. Чужая переписка

Личные сообщения и переписки тоже не стоит пересылать без разрешения. В них могут быть чьи-то секреты, которые нельзя раскрывать чужим людям.

5. Сначала проверка

Если просят срочно отправить эти данные, это уже повод остановиться. Безопаснее ответить отказом, проверить запрос у взрослого и не торопиться.

1

**сообщение от знакомого
профиля всё равно
нужно проверять другим
способом.**

Даже знакомый аватар не гарантирует безопасность:
аккаунт могли украсть или подделать.

Рекомендации по цифровой безопасности и защите аккаунтов

3

**простых настроек уже
заметно снижают
лишний доступ
к профилю.**

Приватность уменьшает круг людей, которые видят
ваши данные и записи.

Рекомендации служб поддержки социальных сетей и цифровой
безопасности

Что нельзя показывать на фото и видео

Адрес и школа

Точный адрес дома, номер школы, класс и маршрут легко связывают фото с конкретным человеком. Даже без подписи такой снимок помогает незнакомцам понять, где вы бываете каждый день.

Подсказки о месте

Геолокация, таблички улиц и номера домов на фоне выдают место съёмки. Если нужно поделиться кадром, лучше убрать метку и убедиться, что фон не раскрывает лишнего.

Документы в кадре

Билеты, пропуска, ключи и документы содержат номера и штрихкоды, по которым можно получить доступ к поездке, сервису или личным данным. Такие вещи нельзя показывать в кадре.

Экран и переписка

Экран телефона или компьютера часто раскрывает коды, переписки, списки контактов и уведомления. Перед публикацией стоит проверить, не видно ли на фото или видео того, что должно оставаться личным.



Боты, подписки и «выигрыши»

1. Проверить отправителя

Сначала проверьте, кто прислал сообщение: официальный сервис или неизвестный аккаунт. Настоящие розыгрыши не требуют сразу сообщать пароль, код из SMS или номер карты.

2. Оценить условия

Потом прочитайте условия внимательно. Если за «приз» просят лишние данные, вход через странную ссылку или срочное подтверждение, это похоже на попытку обмана, а не на подарок.

3. Не спешить с ссылкой

Не переходите по ссылкам сразу. Поддельные страницы часто копируют название известного сервиса, но отличаются адресом, ошибками в тексте или странным оформлением.

4. Проверить отдельно

Самое безопасное решение — отказаться, закрыть сообщение и проверить информацию на официальном сайте или через приложение. Если розыгрыш настоящий, его условия будут понятными и прозрачными.

Ситуация 1: незнакомец пишет в личку

1. Не вступать в диалог

Если пишет незнакомец, не отвечайте сразу и не продолжайте разговор из любопытства. Любая просьба о фото, номере, адресе или коде уже повод насторожиться.

2. Заметьте давление

Проверьте, не пытается ли человек давить на срочность, обещать подарок или запугивать. Такие приёмы нужны, чтобы вы меньше думали и быстрее отправили личные данные.

3. Не делиться данными

Ничего не отправляйте, даже если собеседник представляется знакомым или взрослым. Настоящие взрослые не просят коды и не требуют секретную информацию в личных сообщениях.

4. Сообщить и заблокировать

Сделайте скриншот, заблокируйте контакт и покажите переписку взрослому. Так вы сохраните доказательства и поможете быстрее остановить опасный контакт.

Ситуация 2: ссылка «от друга»

1. Не доверять автоматически

Даже если сообщение пришло от знакомого имени, не открывайте ссылку сразу. Аккаунт друга могли взломать, а сообщение — отправить без его ведома.

2. Проверить адрес

Посмотрите на адрес: подозрительные символы, лишние буквы и странный домен часто говорят о подделке. Мошенники специально делают адрес похожим на настоящий.

3. Замечать тревожные признаки

Если ссылка просит снова войти в аккаунт, ввести пароль или скачать файл, остановитесь. Настоящий сервис обычно не требует срочно вводить данные через случайное сообщение.

4. Уточнить отдельно

Уточните у друга другим способом — позвоните или напишите в другом чате. Так вы быстро поймёте, отправлял ли он ссылку на самом деле.



Ситуация 3: посты о том, где вы находитесь

Не сообщать об отсутствии

Публикации о том, что дома никого нет, помогают понять, когда квартира пустует. Такие сведения лучше не выкладывать до возвращения взрослых или завершения поездки.

Делиться позже

Фотографии из реального времени показывают, где вы находитесь сейчас, а не когда-то потом. Для безопасности лучше отложить публикацию до окончания прогулки, поездки или встречи.

Убирать геометки

Геометки и отметки места могут раскрыть привычные маршруты и любимые точки. Даже короткий пост иногда даёт достаточно информации, чтобы связать человека с конкретным адресом.

Выбирать правильное время

Безопаснее рассказывать о событии после него: так вы сохраняете впечатления, но не сообщаете посторонним, где вас можно найти прямо сейчас.

Что собирают игры и сервисы

Что собирают	Зачем это нужно
Никнейм	Учётная запись
Почта, IP	Вход и связь
История действий	Сохранение прогресса

Типичные данные, запрашиваемые играми и учебными платформами при регистрации и входе.

Разные сервисы собирают не только имя пользователя, но и технические данные. Это помогает им работать, но пользователю важно отделять публичный никнейм от личной информации.

Никнейм должен быть нейтральным, а личные данные — минимальными. Внутри сервиса лучше не писать имя, класс, адрес и другие сведения, по которым легко узнать человека.

Чужие данные тоже нужно защищать

1. Нужно согласие

Чужие фотографии, скриншоты и перепосты нельзя использовать без разрешения, особенно если на них видно лицо, имя, адрес или личную переписку. Уважение к чужим данным так же важно, как к своим.

2. Не распространять

Если вам прислали чужой личный контент, не пересылайте его дальше «ради шутки». Один лишний пересыл делает проблему шире и может навредить человеку ещё сильнее.

3. Сохранить доказательства

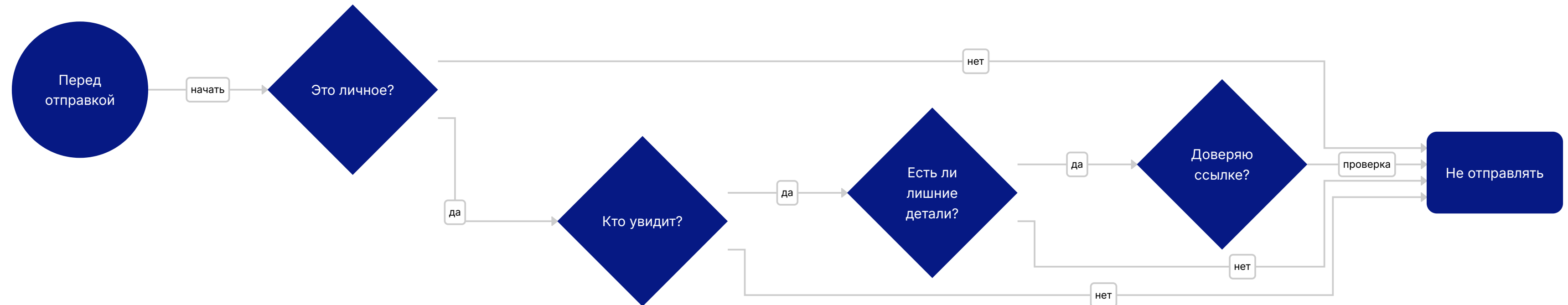
При травле в сети сохраните скриншоты, ссылки и дату публикации. Это поможет взрослым, учителю или модератору быстро понять, что произошло, и принять меры.

4. Попросить помощи

Если кого-то обижают, сразу сообщите взрослому и используйте жалобу в сервисе. Самое полезное действие — остановить распространение, а не участвовать в нём.

Чек-лист перед отправкой или публикацией

Последовательность коротких проверок перед публикацией или отправкой сообщения.



Что делать, если данные уже попали не туда

1. Сохранить доказательства

Сначала сохраните переписку, скриншоты и ссылки, чтобы не потерять доказательства. Это поможет понять, что именно произошло, и объяснить ситуацию взрослому или службе поддержки.

2. Защитить аккаунт

Потом смените пароль и включите двухфакторную защиту, если она доступна. Так вы уменьшите риск повторного входа в аккаунт посторонними людьми.

3. Попросить помощи

Сообщите о случившемся родителям, учителю или другому доверенному взрослому. Если проблема в сервисе или школе, обратитесь туда как можно быстрее.

4. Убрать лишний доступ

Удалите опасные публикации, проверьте настройки доступа и посмотрите, кто может видеть профиль. Иногда достаточно закрыть аккаунт и ограничить подписчиков.

Главные выводы: безопасность начинается с привычек

Безопасность в сети строится на простых привычках: не раскрывать лишнее, проверять сообщения и ссылки, защищать профиль и уважать чужие данные. Если что-то кажется странным, лучше сразу обратиться к взрослому.