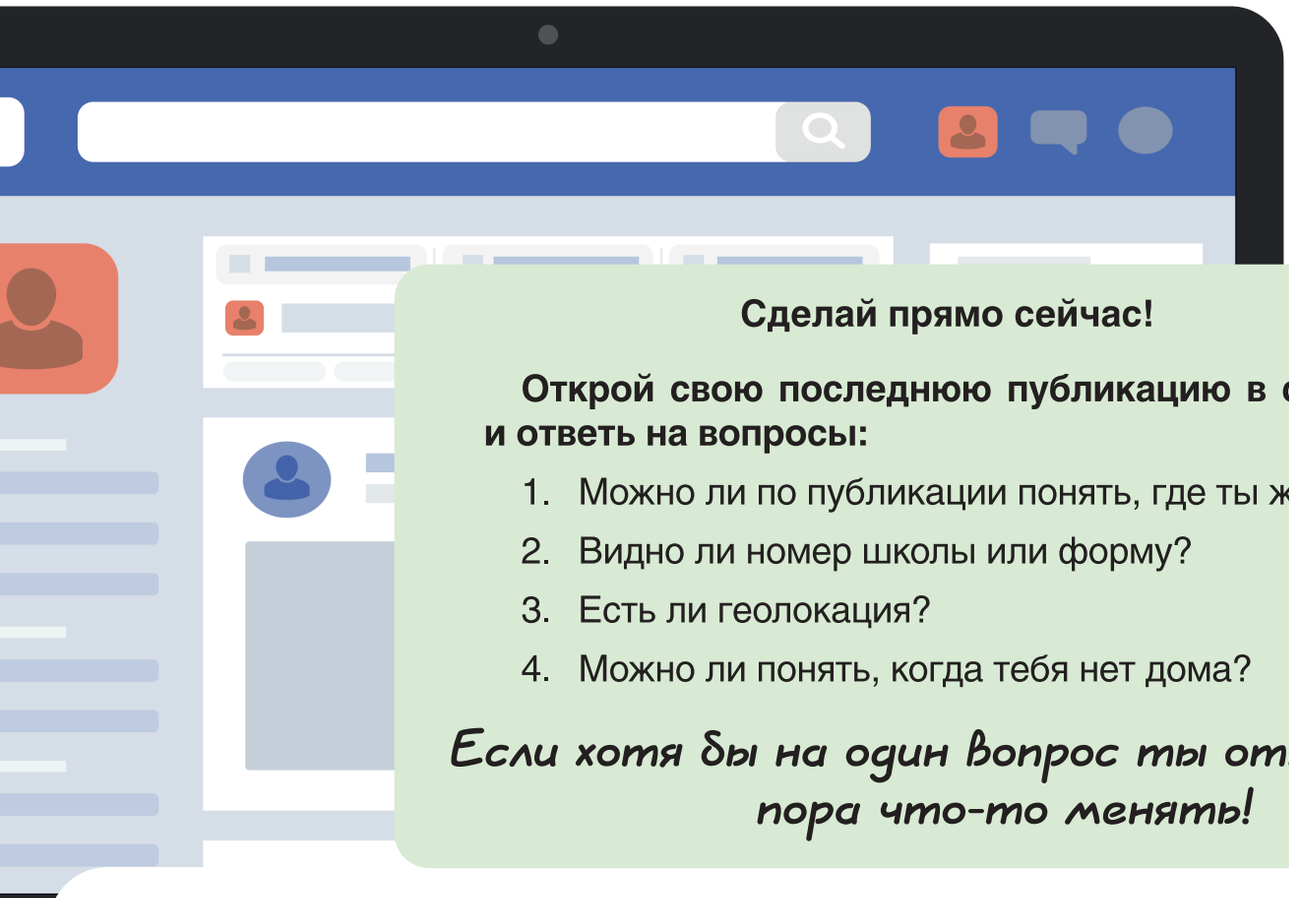


Сделай прямо сейчас!

Открой свою последнюю публикацию в соцсети и ответь на вопросы:

1. Можно ли по публикации понять, где ты живёшь?
2. Видно ли номер школы или форму?
3. Есть ли геолокация?
4. Можно ли понять, когда тебя нет дома?

Если хотя бы на один вопрос ты ответил «да», пора что-то менять!

Как социальные сети используют личную информацию?

Когда ты регистрируешься в соцсети, она просит ввести твой возраст, имя, интересы. Потом она отслеживает, что ты смотришь, что «лайкаешь» и с кем общаешься. Соцсети создают твой цифровой портрет — как будто рисуют твою виртуальную копию, чтобы показывать рекламу товаров, которые тебе понравятся, предлагать видео, от которых ты не сможешь оторваться.

А ещё соцсети всегда «хотят» знать, когда ты туда заходишь, сколько времени там проводишь, чем интересуешься и с кем дружишь. Однако это может быть опасно, ведь такое отслеживание не только крадёт у тебя время, когда вместо учёбы ты смотришь бесполезные видео, но и может совершить настоящую кражу денег с банковской карты, твоей личной или родителей.

Цели сбора информации в социальных сетях:

- ⊕ Показывать интересный контент.
- ⊕ Рекомендовать друзей.
- ⊕ Персонализировать новости.
- ⊖ Продавать данные рекламодателям.
- ⊖ Манипулировать эмоциями.
- ⊖ Создавать зависимость от соцсети.

Как тебя находят в интернете?

Даже если ты не называешь своё имя, тебя можно узнать по:

- фото комнаты — например, рассмотреть на стене диплом из школы;
- названию Wi-Fi или геолокации;
- отметкам — например, «Гимназия № 7», «Минск», «дом у вокзала»;
- фото формы или школьного бейджа;
- подпискам — например, ты подписан на кружок «Танец 26 школа».

Всё это — маленькие кусочки пазла. Собери их — и можно догадаться, кто ты, где живёшь, когда бываешь дома и даже кто твои родители.

Сделай прямо сейчас!

1. Открой свой профиль в режиме «чужого человека».
2. Посмотри свои последние 10 постов.
3. Ответь честно на вопросы:

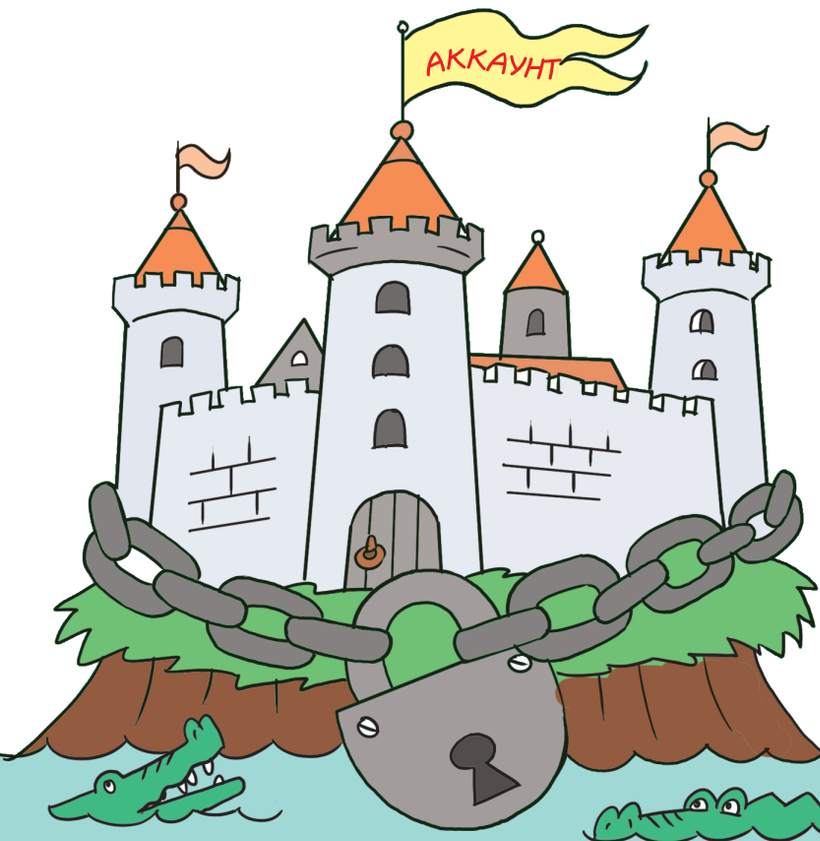
- Можно ли понять твой возраст?
- Видно ли, где ты учишься?
- Понятно ли, где ты живёшь?
- Видны ли твои друзья и семья?

Если ты ответил «да» на 2 и более вопроса, информация на следующих страницах книги точно для тебя!

Как обеспечить свою конфиденциальность?

Защита конфиденциальной информации — это хорошая привычка. И чем раньше ты начнёшь её формировать, тем увереннее будешь чувствовать себя в цифровом мире.

Интернет никогда не спит. Здесь можно общаться с друзьями, смотреть видео, учиться, играть и делиться тем, что тебе нравится. В Сети «обитают» миллиарды людей: школьники и студенты, учёные и художники, геймеры и блогеры. Но, к сожалению, не только они. Наряду с интересными и добрыми людьми в интернете могут встретиться те, кто не заслуживает доверия: мошенники, хакеры и просто слишком любопытные незнакомцы, которым интересно следить за тобой без разрешения. Одни хотят украсть твои данные, другие — взломать аккаунт, а кто-то просто может вести себя неприятно.



Хорошая новость: ты можешь защититься! Причём сделать это несложно! Мы расскажем тебе об этом, но одних знаний, конечно, мало — важно действовать. Подумай: ты же не оставляешь дверь дома открытой на ночь, правда? Так почему бы не закрыть «дверь» и в своём цифровом пространстве?

Один из самых простых и важных шагов — это настройки приватности. Они словно занавески на окнах или замок на шкафчике. Благодаря им ты сам выбираешь, кто может видеть твою страницу, оставлять комментарии, писать тебе сообщения, просматривать твои фото и видео. Всё это решаешь ты, а не кто-то другой!

Помни! Твой аккаунт в соцсетях — это твоя крепость. Потрать немного времени, чтобы заглянуть в настройки безопасности на своих устройствах, в мессенджерах и соцсетях. Отключи геолокацию, если она не нужна. Сделай личным то, что не должен видеть весь мир!

Настройки приватности

TikTok

• Открой TikTok и перейди на свой профиль (иконка справа внизу).

• Нажми на три полоски/точки в правом верхнем углу, выбери «Настройки и конфиденциальность».

• Перейди в раздел «Конфиденциальность».

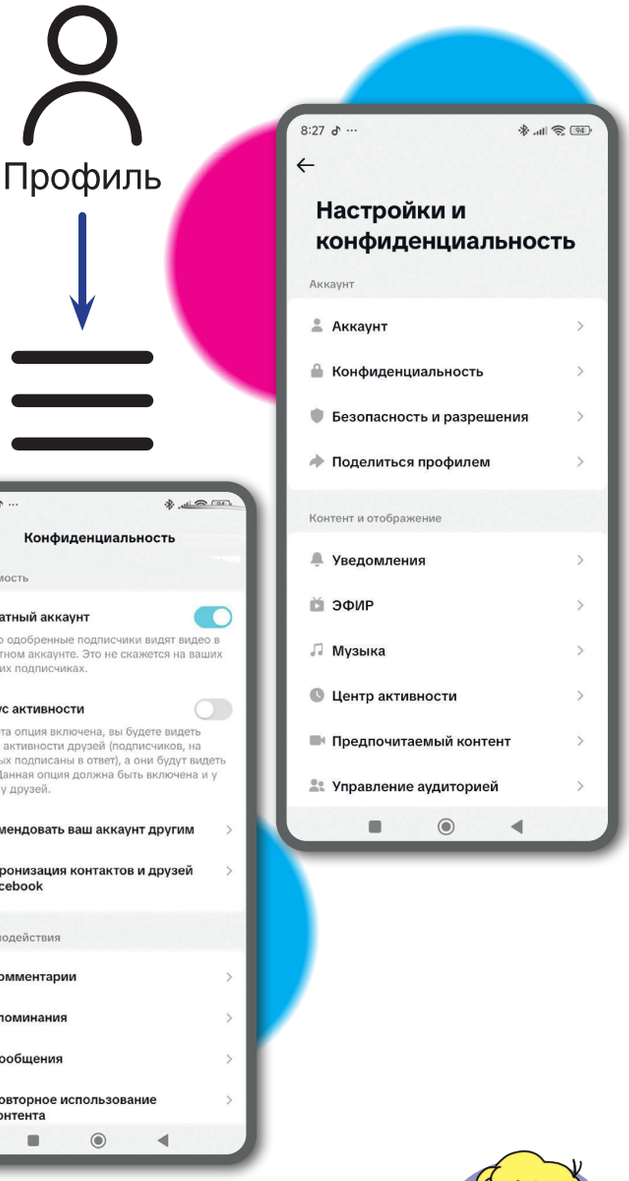
• Включи «Личный аккаунт».

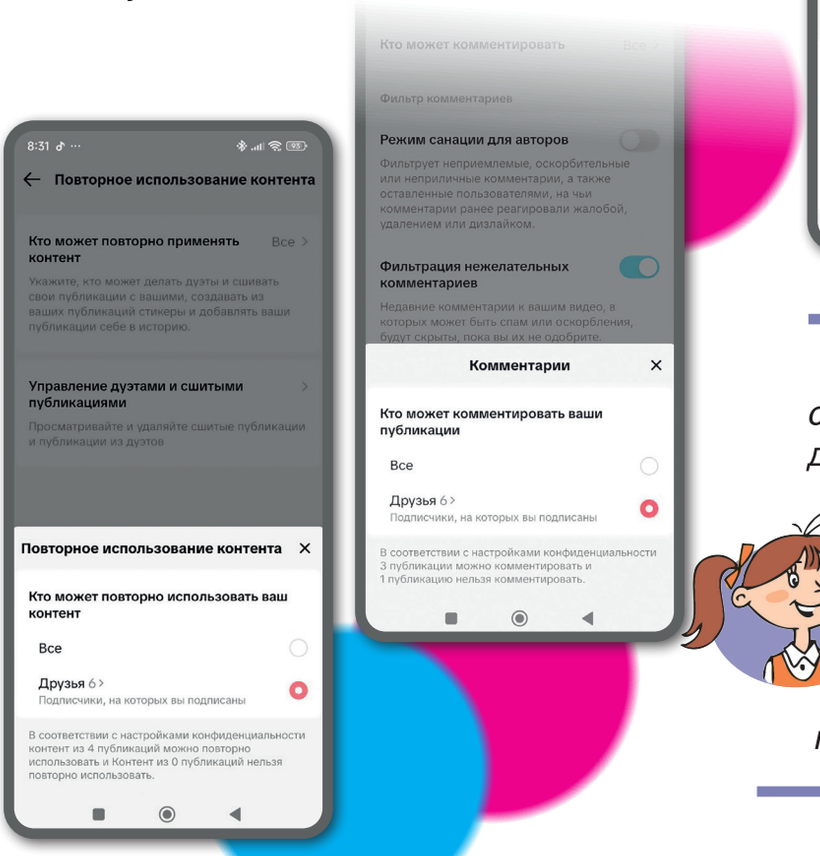
• Запрети рекомендовать твой аккаунт другим («Не показывать мой аккаунт в рекомендациях»).

• Ограничь скачивание видео, комментирование и отправку личных сообщений:

► в разделе «Взаимодействия» выбери, кто может комментировать — все, только друзья или никто;

► аналогично отрегулируй дуэты, сшивки, упоминания и сообщения.





Помни! Лучше оставить свой аккаунт доступным только для людей, которых ты знаешь лично!

Проверяй настройки хотя бы раз в 2 месяца. Платформы обновляются, а настройки меняются!

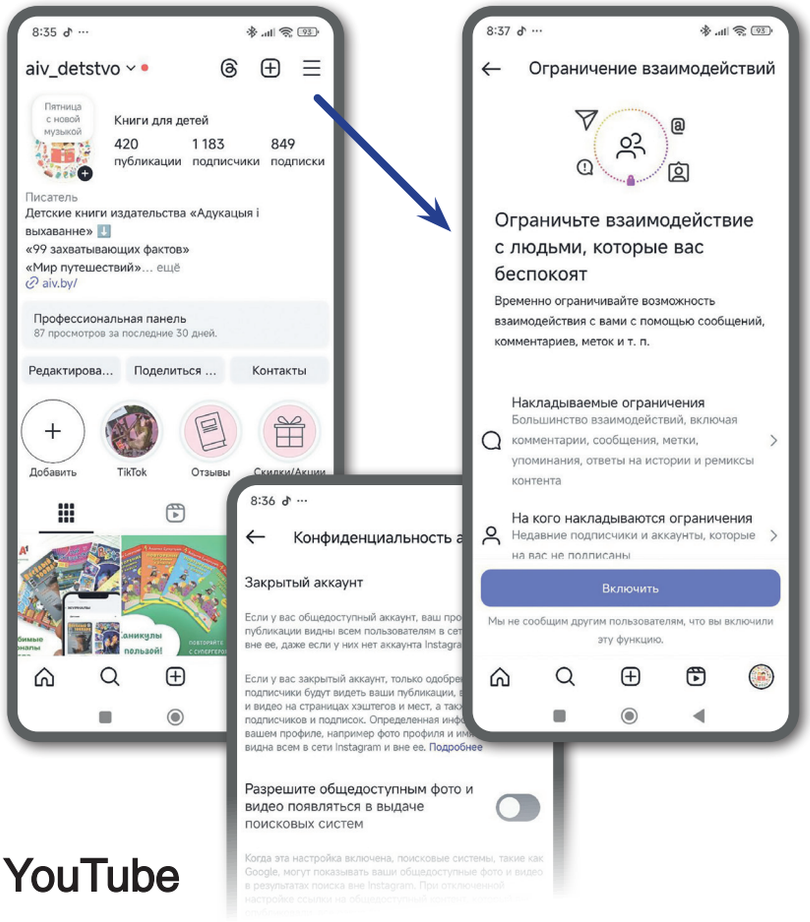
на популярных платформах

Instagram

- Открой приложение и перейди в свой профиль (иконка справа внизу).
- Нажми на три линии в правом верхнем углу.
- Пролистай вниз до блока «Кто может видеть ваш контент» и выбери раздел «Конфиденциальность аккаунта».
- Включи опцию «Закрытый аккаунт».

Теперь только одобренные тобой подписчики смогут видеть твои публикации и истории.

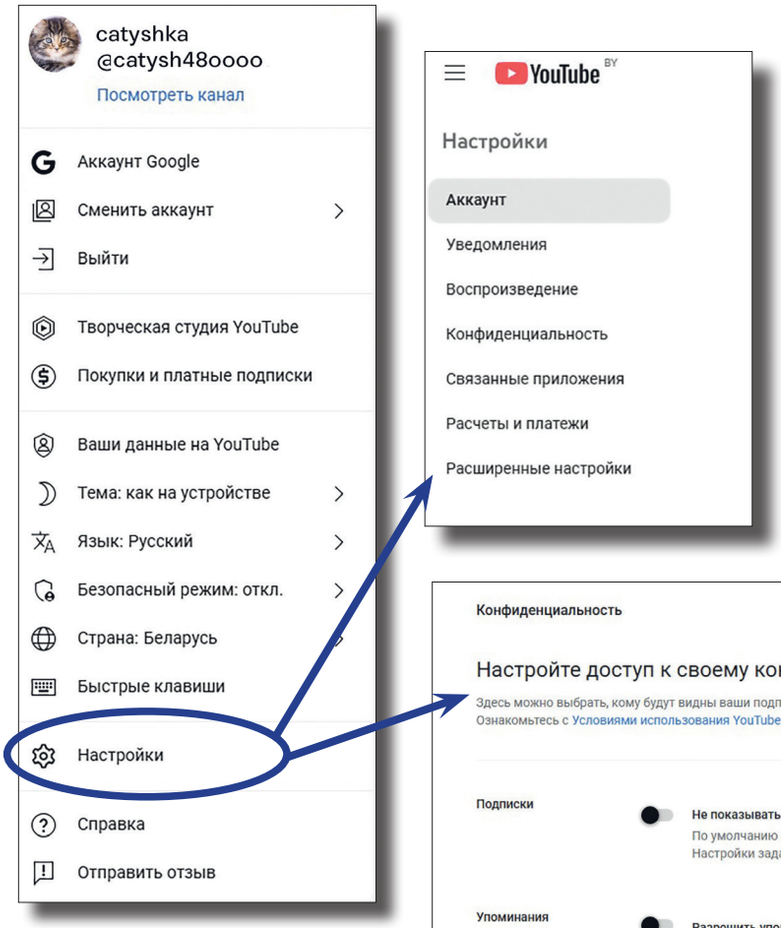
- Ограничь комментарии и сообщения: выбери тех, кто может писать сообщения и комментировать твои публикации (например, «Подписчики», «Только друзья»).
- Скрой свои истории от нежелательных людей в параметре «Скрыть истории».

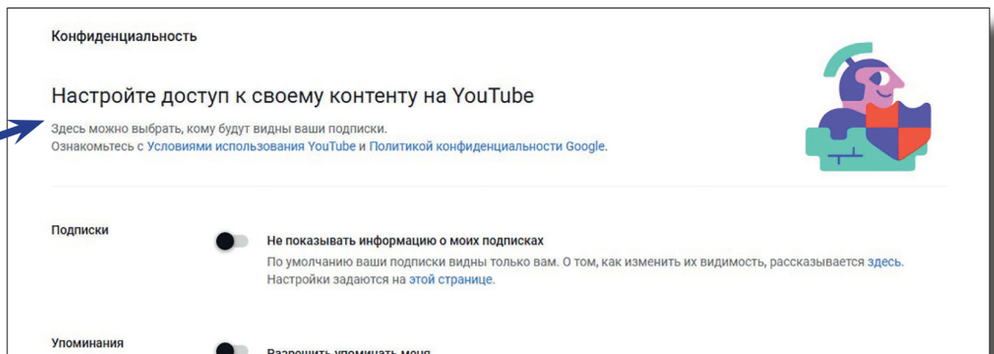


YouTube

- Открой YouTube и войди в свой аккаунт.
- Нажми на иконку профиля в правом верхнем углу. Выбери «Настройки».
- Перейди в раздел «Конфиденциальность». Здесь можно включить:
  - «Скрывать мои подписки».
  - «Скрывать понравившиеся видео».

Для приватности отдельных видео зайди в «Творческую студию» (YouTube Studio), выбери видео, нажми «Изменить» и в поле «Видимость» выбери «Приватное» или «Для пользователей со ссылкой».





Управление учётными записями

Что такое пароль?

Пароль — это аналог ключа. А все ключи уникальны. Таким должен быть и твой пароль.

Как хранить пароли?

Для хранения паролей используй блокнот (бумажный!) с кодовым названием, не пиши «Мои пароли». Не носи блокнот с собой в школу, а лучше спрячь в надёжном месте.

Скачай менеджер паролей (спроси у родителей).

Как придумать надёжный пароль?

1. Возьми своё любимое животное. Например, ты любишь кенгуру. Напиши название на клавиатуре с включённой английской раскладкой. Получится rtyuehe *(Можно намеренно допустить орфографическую ошибку (лучше более одной), чтобы пароль был более «стойким». Например, вместо «кенгуру» писать «кИнгОру»).*

2. Добавь цифры (лучше совершенно случайные): «rtyuehe394».

3. Добавь заглавную букву и символ: «Rtyuehe394!».

Получился надёжный пароль: Rtyuehe394!

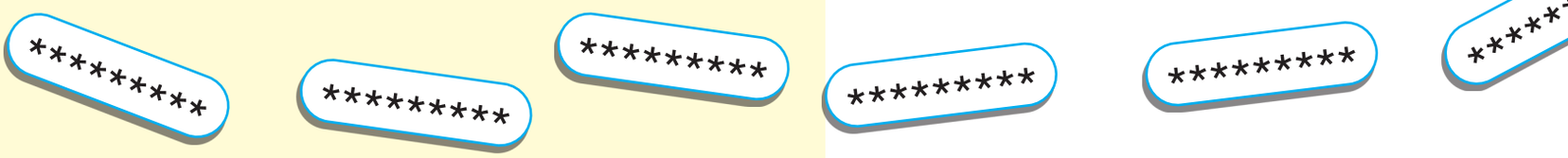
Ненадёжные пароли:

- 123456 — самый популярный пароль в мире.
- qwerty — просто ряд букв на клавиатуре.
- Дата рождения.
- Слово «пароль» или password.
- Твоё имя, имя питомца.

Что делать при утере доступа?

- Прежде всего, не паниковать!
- Попробуй восстановление через e-mail или телефон, если у тебя есть к ним доступ.
- Если не получилось, попроси взрослого написать в техподдержку.
- Обязательно измени пароли на всех остальных платформах!

Для создания надёжного пароля не рекомендуется использовать слова, в которых могут содержаться какие-либо общеизвестные факты/имена/прозвища/названия животных, которые касаются личности пользователя пароля. Лучше придумать «стойкий» пароль, состоящий из не менее 12, а лучше 13–16 символов. Его автоматически может создать генератор паролей в интернете.



Двухфакторная аутентификация

Зачем нужна двухфакторная аутентификация?

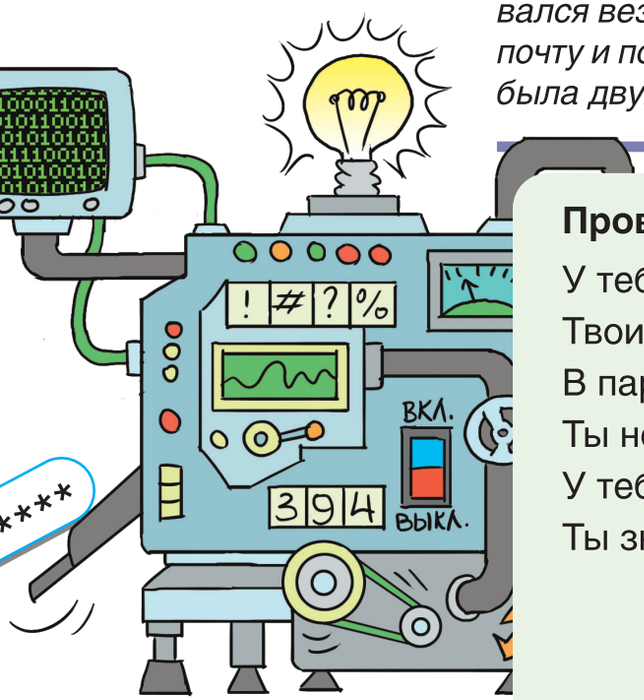
Представь: ты поставил крепкий замок на дверь — это твой пароль. Но вдруг кто-то всё же подобрал к нему ключ или подсмотрел, как ты его вводишь. Что тогда? Именно тут на помощь приходит двухфакторная аутентификация (2FA).

Ты, скорее всего, уже сталкивался с 2FA, например, когда входишь в аккаунт и тебе приходит СМС с кодом. Или когда ты открываешь специальное приложение, которое каждые 30 секунд выдает новый набор цифр — уникальный и одноразовый. Это как секретный ключ, который постоянно меняется, и никто, кроме тебя, не может его получить. Есть и другие варианты: подтверждение через электронную почту, push-уведомление на телефон или даже сканирование отпечатка пальца. Главное, что это работает только у тебя.

2FA (читается как «ту-эф-эй») — дополнительный уровень защиты, который не даст злоумышленникам пробраться внутрь твоего устройства даже при наличии пароля. Потому что одного пароля недостаточно — нужен ещё второй код, который получаешь только ты.

Порядок подключения двухфакторной аутентификации

1. Зайди в настройки безопасности аккаунта.
2. Найди позицию «Двухфакторная аутентификация».
3. Подключи номер телефона или приложение (например, Google Authenticator).



Даня потерял доступ к игровому аккаунту. Он пользовался везде одним паролем. Злоумышленник взломал почту и поменял все пароли и настройки. Если бы у Дани была двухфакторная защита, этого бы не случилось.

Проверь прямо сейчас!

У тебя разные пароли для важных сервисов.
Твои пароли длиннее 8 символов.
В паролях есть цифры и символы.
Ты не используешь личную информацию в паролях.
У тебя включена 2FA на важных аккаунтах.
Ты знаешь, где хранятся твои пароли.