

Двойная защита всегда лучше обычной

или как использовать двухфакторную аутентификацию

 **Двухфакторная аутентификация** — метод проверки, который должен показать, что в аккаунт действительно входит его владелец через дополнительное подтверждение различных типов данных (**факторов**).

1 Фактор



то, что мы знаем —
пароли и кодовые фразы

2 Фактор



то, что мы имеем —
устройство и номер
телефона, на которые
приходят дополнительные
коды для подтверждения

3 Фактор



то, что присуще только нам
— отпечатки пальцев
и сетчатка глаза

Каждый день
взламывается около

30 000 сайтов

Каждую минуту
подвергаются атаке свыше

90 000 сайтов

 Подключенная двухфакторная аутентификация **значительно усложнит работу мошенникам**. Помимо пароля, им потребуется получить доступ к вашим смс, почте или даже устройству.

Как это использовать?

 Подключи двухфакторную аутентификацию во всех аккаунтах, где есть твоя личная информация. Сделать это можно в настройках профиля.

 Если у тебя пропал телефон, при первой же возможности позвони оператору и заблокируй сим-карту. Так мошенник не сможет переставить её в другое устройство и получить доступ к твоим аккаунтам и личным данным.

 Придумай сложные и разные пароли для всех своих аккаунтов.

 Смени пароли, если тебе внезапно пришло уведомление с кодом для входа в какой-либо сервис, хотя перед этим ты никаких действий не предпринимал.