

# 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, –  
например, отпечатки пальцев  
и сетчатка глаза

Каждый день  
взламывается около

**30 000 сайтов**

Каждую минуту  
подвергаются атакам свыше

**90 000 сайтов**

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

## Как все это использовать?

- ✔ Подключите функцию двухфакторной аутентификации во всех аккаунтах, где есть ваша личная информация. Сделать это можно в настройках профилей
- ✔ Если у вас пропал телефон, при первой возможности позвоните оператору и заблокируйте сим-карту. Так мошенник не сможет переставить её в другое устройство и получить доступ к вашим аккаунтам и личным данным
- ✔ Придумайте сложные и разные пароли для всех своих аккаунтов
- ✔ Смените пароли, если вам внезапно пришло уведомление с кодом для входа в какой-либо сервис, хотя перед этим вы никаких действий не предпринимали