

Facial Recognition: What it is, how it works, and how to use it safely

Gridinsoft Help Center

What it is

How it works

- Capture: a camera snaps your face (photo or video).
- Template: software measures landmarks (eyes, nose, angles, texture) to create a faceprint.
- Match: that faceprint is compared to a database or your device's secure storage to decide unlock / no match.

Where it's used

- Phones & laptops: fast unlock and payments
- Airports & stadiums: identity checks and watchlists
- Retail & banking: login, fraud prevention, VIP/service flows

Risks & limits

- Privacy: images can be stored, shared, or breached.
- Bias & accuracy: lighting, camera quality, and demographic bias affect results.
- Spoofing: simple systems can be fooled by photos or masks; stronger ones use liveness checks (depth/IR/motion).

Stay in control

- Use liveness-enabled systems (depth/IR) and keep devices updated.
- Prefer on-device matching over cloud storage when possible.
- Review permissions/policies: who keeps your image, for how long, and why?
- Have a fallback (PIN/password) and rotate it regularly.
- In sensitive contexts, ask for alternatives (manual ID, passkeys, security keys).