Browser Isolation: What it is, why it protects you, and the easiest ways to use it

Gridinsoft Help Center

What it is

Browser isolation puts your web activity in a safe bubble-a sandbox or remote container-so risky pages can’t touch your actual device. You browse normally; anything malicious stays trapped on the other side.

Why it matters

Most attacks start in the browser (drive-by downloads, fake updates, exploit kits). Isolation keeps clicks and scripts away from your files, passwords, and network-so a bad site becomes a dead end.

How it works

- Local sandbox: the page runs in a sealed container on your machine.
- Remote/Cloud isolation: the page runs on a server; you see a safe visual stream.
- Policy controls: copy/paste, downloads, and uploads can be allowed or blocked.

When to use it

- Opening unknown links (support tickets, ads, search results)
- High-risk roles (finance, HR, admins) or frequent research on shady sites
- Shared computers, kiosks, and BYOD environments

Good to know

- It reduces risk, not judgment-phishing can still trick users to share data.
- Remote isolation can add a bit of latency; tune policies for key workflows.
- Pair with MFA, EDR, and DNS filtering for layered defense.

Quick start

- Pick a solution (local sandbox for individuals, remote isolation for teams).
- Set simple rules: allow known sites, restrict downloads elsewhere.
- Train users: "unknown link? open in isolation."