Conduit Browser Hijacker: What it is, signs to spot, and how to remove it

Gridinsoft Help Center

What it is

What you may notice

- Homepage/search engine changed; new tab opens to a strange site
- Extra ads, pop-ups, and random redirects
- A toolbar or extension you don’t remember installing
- Slower browsing and higher data use

How it gets in

- Bundled with "free" installers or fake updates
- Rogue extensions from untrusted sources
- Drive-by downloads and deceptive ads

Remove it now (quick steps)

- Remove unknown extensions and reset the browser to defaults.
- Uninstall suspicious apps; then reboot.
- Run a full anti-malware scan to clean leftovers.
- Check DNS/proxy settings and set back to automatic if changed.

Prevent it

- Install apps/extensions only from official stores.
- Choose Custom install and deselect extra offers.
- Keep your browser and OS updated; use real-time protection.
- Be cautious with "free" codecs, PDF viewers, and cracks.