

Fork Bomb - What it is, what it does, and simple ways to prevent it

Gridinsoft Help Center

What it is

A fork bomb is a tiny program or command that clones itself over and over until your computer runs out of processes and resources. The system becomes slow or unresponsive - sometimes it crashes - because it's too busy creating more copies.

How it works

- It starts one process that immediately spawns two.
- Each of those spawns two more - and so on - creating an exponential flood.
- CPU time, memory, and the allowed number of processes get exhausted.

What you might notice

- Apps stop responding and the mouse lags
- Fans ramp up and the desktop freezes
- You can't open new windows or terminals
- On servers: load average spikes and logins fail

If it hits

- Try to switch TTY (Linux: Ctrl+Alt+F2) and log in as an admin.
- Kill the user session or reboot safely if you still have control.
- After recovery, check shell history and disable any risky aliases or scripts.

Prevent it

- Limit processes per user (Linux: ulimit -u, PAM limits, systemd slices or cgroups).
- Use least privilege - don't run untrusted scripts as admin.
- On shared systems, restrict who can run code and review new accounts.
- Monitor for sudden process spikes and alert on abuse.