Macro Virus - What it is, how it spreads, and how to block it safely

Gridinsoft Help Center

What it is

A macro virus hides inside Office files like Word documents or Excel spreadsheets and runs tiny programs called macros when you open the file. Criminals use it to download more malware or steal data. For background and safe settings, see our macro attack explainer.

How it spreads - quick tour

- Phishing emails with "urgent" invoices or resumes
- Downloads that ask you to Enable Content or Enable Macros
- Malicious templates or add-ins that auto-load

What you may notice

- Office prompts to enable macros on a file from email or the web
- Brief command windows flashing, odd network traffic
- Documents that lock, crash, or show scrambled content

Remove it now

- Close the document and don’t enable macros.
- Run a full anti-malware scan, reboot, then scan again.
- In Office, check and remove unknown add-ins/templates.
- From a clean device, change passwords if sensitive files were opened.

Prevent it

- Keep the default: Block macros from the internet in Office.
- Open unknown docs in Protected View or online preview.
- Verify invoices and attachments out of band before opening.
- Use reputable email and web filtering plus EDR/anti-malware.
- Store trusted templates centrally and train staff to never enable macros unless required.