Tech Support Scam - what it is, common tricks, and how to shut it down

Gridinsoft Help Center

What it is

A tech support scam is when someone pretends to be from a trusted company (Microsoft, Apple, your ISP) to make you believe your computer is "infected" or "blocked." They use pop-ups, phone calls, or search ads to pressure you into paying for fake fixes, installing spyware, or giving remote control of your device.

Why it matters

Victims can lose money, hand over sensitive info, or unknowingly install malware. Scammers may also steal passwords and card details while "fixing" the issue.

How it works

- Hook: scary pop-up or call claims urgent problems and tells you to call a number or click a link.

- Pressure: the "agent" asks for remote access or payment to fix fake errors.

- Take: they install tools, steal data, or sell bogus subscriptions.

- Repeat: your number/email gets shared, so more scams follow.

Red flags

- Pop-ups that freeze the screen with loud warnings and a phone number.

- Callers who say they "detected problems" on your PC out of the blue.

- Requests for remote access, gift cards, wire transfers, or crypto.

- Spelling errors, generic company names, or pushy countdowns.

Do it right

- Close the tab/app. If stuck, press Alt+F4 (Windows) or Force Quit (macOS), then reopen the browser and clear recent tabs.

- Never call numbers in pop-ups or give remote access to strangers.

- Use your official support channels (vendor site, app’s help menu) if you need help.

- If you interacted: disconnect from the internet, remove any remote-control apps, run a full security scan, change passwords from a clean device, and contact your bank if you paid.