Malvertising - What it is, red flags to spot, and how to stay safe

Gridinsoft Help Center

What it is

Malvertising is when attackers hide malicious code inside online ads. You don’t have to click a sketchy site - a booby-trapped ad on a legit page can redirect, phish, or install malware through drive-by downloads and pop-ups.

How it works - quick tour

- Compromised ad networks serve malicious creatives to reputable sites
- Hidden code redirects you to exploit pages or fake updates
- Fingerprinting picks targets and avoids security sandboxes
- Payloads include spyware, ransomware, and credential stealers

Red flags

- Pop-ups asking to install updates or enable notifications
- Pages that reopen themselves or trigger multiple redirects
- Downloads starting without you clicking a clear button
- Security prompts that look slightly off-brand

If it hits - first moves

- Close the tab or kill the browser process - don’t click prompts.
- Run a full anti-malware scan, reboot, then scan again.
- Clear browser cache and notifications, remove unknown extensions.
- From a clean device, change passwords and enable MFA if anything seemed phishy.

Prevent it

- Keep the browser, plugins, and OS updated.
- Use a reputable ad blocker and DNS/web filtering.
- Disable or limit browser plug-ins like legacy players.
- Avoid pirated streams and shady download portals.
- For orgs: enable network-layer protections and inspect egress traffic.