Baiting: What it is, common lures, and how not to take the bait

Gridinsoft Help Center

What it is

Baiting is a social-engineering trick: attackers dangle something tempting-an "urgent" work file, free software, a giveaway-to make you install malware yourself. The lure feels legit; the payload hides in the download.

How it works

- A believable hook (HR forms, invoices, prize emails, "codec needed" pop-ups).
- You click -> a file or installer runs -> malware slips in quietly.
- The malware steals logins, plants backdoors, or encrypts files.

Common lures

- "Payroll_update_Q3.pdf.exe" or macro-heavy docs
- Fake download buttons or "update your player" prompts
- USB drives "found" near the office (curiosity bait)
- Ads for cracked/pro "free" software

Spot the signs

- Files asking to "Enable macros" or bypass browser warnings
- Unwanted installers bundled with a needed tool
- New extensions, startup items, or sudden redirects after a click

If you took the bait

- Disconnect from the internet.
- Run a full anti-malware scan and remove findings.
- From a clean device, change passwords and enable MFA.
- Tell IT/Security if this is a work device; watch accounts for alerts.

Prevent it

- Download only from official sources; ignore "free" cracks.
- Don’t enable macros unless you must (and trust the sender).
- Verify sender and domain; when unsure, call to confirm.

- Keep OS, browser, and extensions updated; use real-time protection.