Evil Maid Attack: What it is, why it beats sleep mode, and how to prevent it

Gridinsoft Help Center

What it is

An evil maid attack targets an unattended device - think laptop in a hotel room or office desk. An attacker with brief physical access can steal data or plant stealthy changes (even firmware tweaks) that later fake a login prompt to capture your password and unlock everything.

Why it matters

Full-disk encryption protects files only when the device is off and the key is locked. If someone tampers with boot code or firmware, they can trick you into handing over that key the next time you power on.

How it happens

- Boots from a USB to alter bootloader/firmware
- Installs a tiny implant that records your password at next startup
- Reboots - nothing looks different until you type the password

Prevent it

- Shut down (not sleep) and require pre-boot PIN/password
- Enable Secure Boot, BIOS/UEFI passwords, and TPM-based encryption
- Disable USB boot / set boot order, and seal the chassis with tamper-evident tape for travel
- Keep firmware up to date; don’t leave devices unattended

If you suspect tampering

- Do not boot normally.
- Boot from known-good media to collect logs and verify boot/firmware integrity.
- Rotate disk passwords/keys and consider a clean reinstall or firmware reflashing.
- Change account passwords from a separate clean device.