# Bluebugging: What it is, signs to spot, and how to block Bluetooth hijacks

Gridinsoft Help Center

## What it is

Bluebugging is a Bluetooth break-in. An attacker sneaks onto a phone or laptop through a weak or misconfigured Bluetooth connection, then takes control features meant for headsets or car kits-calls, messages, contacts, even mic access.

## What you might notice

- Bluetooth turns on by itself or won’t stay off
- Unknown device shows as paired/connected
- Weird call logs or texts you didn’t send
- Battery/network use spikes when you’re not using the device

## How it works

The attacker gets near you (Bluetooth is short-range), tricks the device into pairing or abuses a Bluetooth bug, then grabs permissions: read/send SMS, place or record calls, pull contacts, or install more malware. Older firmware and "always discoverable" settings make this easier.

## If you suspect it

- Turn off Bluetooth immediately.
- Forget unknown devices in Bluetooth settings.
- Update your OS/firmware and reboot.
- Change account passwords (from a clean device) and enable MFA.
- Check messages, call history, and linked devices for anything unfamiliar.

## Prevent it

- Keep Bluetooth off when not in use; avoid "always discoverable."
- Remove old pairings you no longer use.
- Update your phone/laptop and accessories regularly.
- When pairing, confirm the on-screen PIN matches and reject surprise prompts.
- Limit Bluetooth permissions (calls, messages, contacts) to accessories that truly need them.