

Internet of Things (IoT) - What it is, common risks, and how to secure it

Gridinsoft Help Center

What it is

The Internet of Things (IoT) is the web of everyday devices that connect and talk to each other - from smart TVs and speakers to thermostats, cameras, doorbells, cars, and factory sensors. They share data and act automatically without much human input.

Why it matters

IoT makes life easier and boosts efficiency, but each device can become a doorway into your home or business if it is insecure. Weak passwords, old firmware, and exposed services are common pitfalls.

How it works - quick tour

- Sensors + apps collect and send data to local hubs or the cloud
- APIs let phones and services control devices and automate actions
- Firmware on the device runs the show and needs updates to stay safe

Common risks

- Default or reused passwords that attackers guess quickly
- Outdated firmware with known vulnerabilities
- Open services or UPnP that expose devices to the internet
- Excessive data collection that hurts privacy

Prevent it

- Change default passwords and turn on MFA where available
- Update firmware regularly and enable auto-updates
- Put IoT on a separate Wi-Fi or VLAN and disable UPnP/remote admin
- Only install trusted apps and skills and review permissions
- Turn off features you do not use and limit cloud exposure