Block ads with Pi-hole and Home Assistant

A practical companion to the 20-minute On Porpoise video. Work through the steps, then use the boxes to record your own network details.

What Pi-hole does: A device asks DNS for a domain name. Pi-hole checks that name against its blocklists. It can refuse known ad or tracking domains before the device connects. Home Assistant can show its statistics and let you toggle blocking. Pi-hole filters domains, not page content; it will not reliably remove ads served from the same domain as a video, such as YouTube ads.

Before you begin

Have ready	Write yours here
A Linux computer that stays on, connected to your network	Host / device: _____
A stable local IP address for that computer	Pi-hole IP: _____
Access to your router settings and Home Assistant	Router IP: _____

Set up Pi-hole

1 **Install Pi-hole on Linux** (09:50)

On the always-on Linux computer, follow the current official installation guide. Its quick-start command is `curl -sSL https://install.pi-hole.net | bash`. The guide also offers a download-first method if you prefer to review the installer. Record the host IP and the web admin login.

2 **Configure DNS and blocking** (12:14)

Open the Pi-hole web admin page. Choose an upstream DNS provider, confirm blocking is enabled, and check that the default adlists are active. Record your upstream choice: _____. Pi-hole only filters devices that actually send their DNS requests to it.

3 **Point a test device at Pi-hole** (14:31)

Start with one Windows 11 PC: open **Settings > Network & internet**, choose its Wi-Fi or Ethernet connection, then edit **DNS server assignment**. Select Manual, enable IPv4, and enter the Pi-hole IP as Preferred DNS. Browse normally and watch the Pi-hole query log. Once the test works, set your router DHCP DNS to the Pi-hole IP so new devices can use it automatically. If your router cannot set DHCP DNS, see the Pi-hole post-install options.

Connect and check your setup

Keep this page near your router settings while testing. The video chapters are shown beside each step.

4 **Add Pi-hole to Home Assistant** (16:29)

Go to **Settings > Devices & services > Add integration**, choose **Pi-hole**, and enter its host and web port. With Pi-hole v6, create an app password under **Settings > Web Interface/API** in the Pi-hole admin page and use that for the integration. Home Assistant then adds sensors and a blocking switch.

5 **Build a simple dashboard** (17:30)

Add the Pi-hole sensors or switch to a Home Assistant dashboard so you can see queries and blocked requests. The video adds an optional card through HACS at 17:30; the standard integration works without a custom card. If you use HACS, choose and review the specific card before installing it.

6 **Verify on a real device** (after setup)

Confirm the device lists the Pi-hole IP as its DNS server. Browse a few sites, then check that its requests appear in the Pi-hole query log and Home Assistant sensors. Test a blocked domain only after normal browsing works. If no queries appear, recheck the client or router DNS setting.

Quick checks

Check	Result / note
Pi-hole admin page opens	_____
Windows DNS points to Pi-hole	_____
Client queries appear in Pi-hole	_____
Home Assistant shows Pi-hole sensors	_____

If something looks wrong

No queries: The device may be using another DNS server, browser DNS-over-HTTPS, or a VPN. Check its actual DNS route. **Sites fail to load:** Confirm Pi-hole itself is online and can reach its upstream DNS; restore the previous DNS setting while you troubleshoot. **Some ads remain:** Domain filtering cannot remove every ad, particularly ads delivered from the same domain as the content.

Watch and reference

Watch the On Porpoise video | Key chapters: 09:50 install, 12:14 configure, 14:31 Windows DNS, 16:29 Home Assistant, 17:30 HACS card.

Checked against: Pi-hole installation, Pi-hole post-install, Home Assistant Pi-hole integration, and Microsoft network settings. This is a companion handout, not a verbatim transcript.