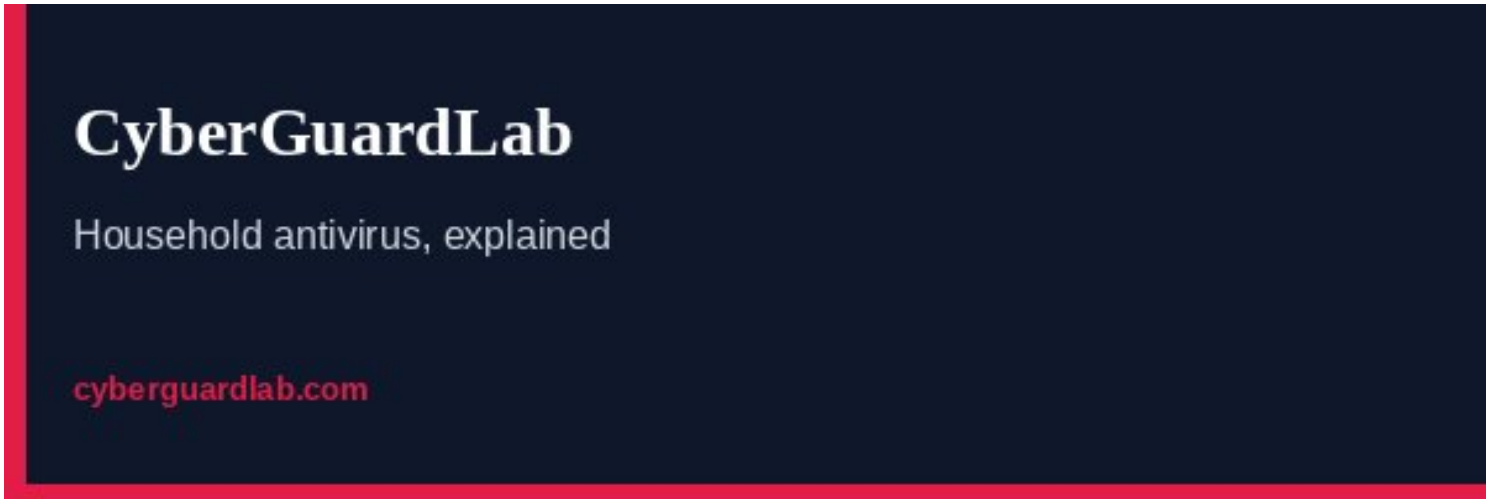
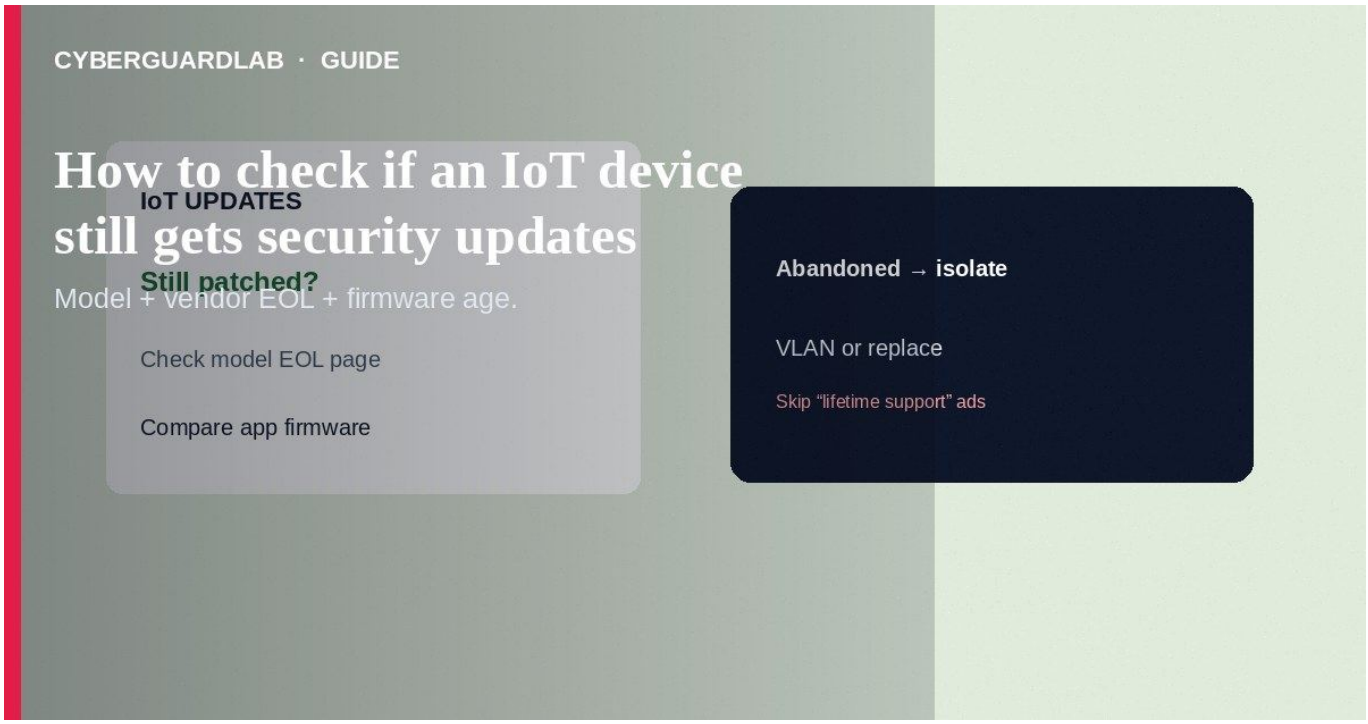


How to check if an IoT device still gets security updates

https://cyberguardlab.com/blog/iot-device-security-updates-check

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



To check whether an IoT device still gets security updates, identify the exact model, read the vendor's support/end-of-life page, and confirm the device app or admin UI still offers firmware newer than what is installed. If the vendor stopped patches, plan replacement or strict VLAN isolation. This how-to is update/support verification-not ISP outage/bill phishing, not WPA3 setup alone, and not Android Private DNS.

1. Steps: verify update support

* Find the exact model and hardware revision (sticker, About screen, or purchase invoice)-marketing names are not enough.
* Note the current firmware version from the device app or web UI.
* On a computer, open the vendor's official support site (type the brand; avoid ads).
* Search the model's download/firmware or security-bulletin page for the newest release date and supported OS/app requirements.

* Look for end-of-support / end-of-life statements, "legacy," or archived product lists.
* In the official app, run Check for updates only on the real device/network-not via a link from cold email.
* Enable auto-update when the vendor provides it and you trust the channel.
* Record the last successful update date in a household inventory spreadsheet.
* If no updates for a long period and the product is marked retired, schedule replacement or move it behind isolation rules.
* Change default passwords regardless of update status.

Retail boxes rarely guarantee multi-year patches. Trust dated support pages and changelogs over packaging claims-and budget replacement for exterior cameras that face the open internet.

2. Signals the device may be abandoned

Signal | Meaning | Action

Vendor EOL page lists your model | No more security fixes expected | Replace or isolate strictly

App removed from Play/App Store | Support likely ending | Do not sideload random APKs; plan exit

Firmware years behind advisories | Known issues may remain | Update if available; else isolate

Only third-party "mod" firmware | High brick/backdoor risk | Prefer vendor images or replace

3. Steps: verify update support

* Find the exact model and hardware revision (sticker, About screen, or purchase invoice)-marketing names are not enough.
* Note the current firmware version from the device app or web UI.
* On a computer, open the vendor's official support site (type the brand; avoid ads).
* Search the model's download/firmware or security-bulletin page for the newest release date and supported OS/app requirements.
* Look for end-of-support / end-of-life statements, "legacy," or archived product lists.

* In the official app, run Check for updates only on the real device/network-not via a link from cold email.
* Enable auto-update when the vendor provides it and you trust the channel.
* Record the last successful update date in a household inventory spreadsheet.
* If no updates for a long period and the product is marked retired, schedule replacement or move it behind isolation rules.
* Change default passwords regardless of update status.

4. After you confirm status

* Keep patched devices on an IoT VLAN when possible.
* Disable UPnP on the router if you do not need it; review port forwards.
* Refuse "camera firmware" emails-those overlap with ISP-style phishing tactics.
* Protect household PCs that view camera feeds with Norton or Bitdefender (TotalAV, McAfee, Avast on-site).

FAQ

The app says "up to date" but the website has a newer file.

Compare version strings carefully. Install only from the vendor's documented method (app vs manual file).

How is this different from ISP bill phishing?

Update checks use official support pages you navigate to. Phishing invents urgent payment/outage links.

No EOL page exists-what then?

Use last firmware date, app store presence, and whether security bulletins still mention the model. When unsure, isolate.

Can Private DNS keep an abandoned camera safe?

No. DNS encryption on a phone does not patch camera firmware.

If you still want a paid suite

Avoiding how to check if an IoT device still gets security updates does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* CISA: Securing IoT
* FTC: Connect to Protect / device security tips
* CISA: Secure our world-home network
* NIST consumer IoT labeling context (overview)

Also read

* How to segment smart TVs and cameras on a separate VLAN
* How to spot a fake ISP outage or bill phishing email
* How to update home router firmware
* How to change your router admin password safely
* How to turn on WPA3 or the strongest Wi-Fi encryption you have