

CyberGuardLab

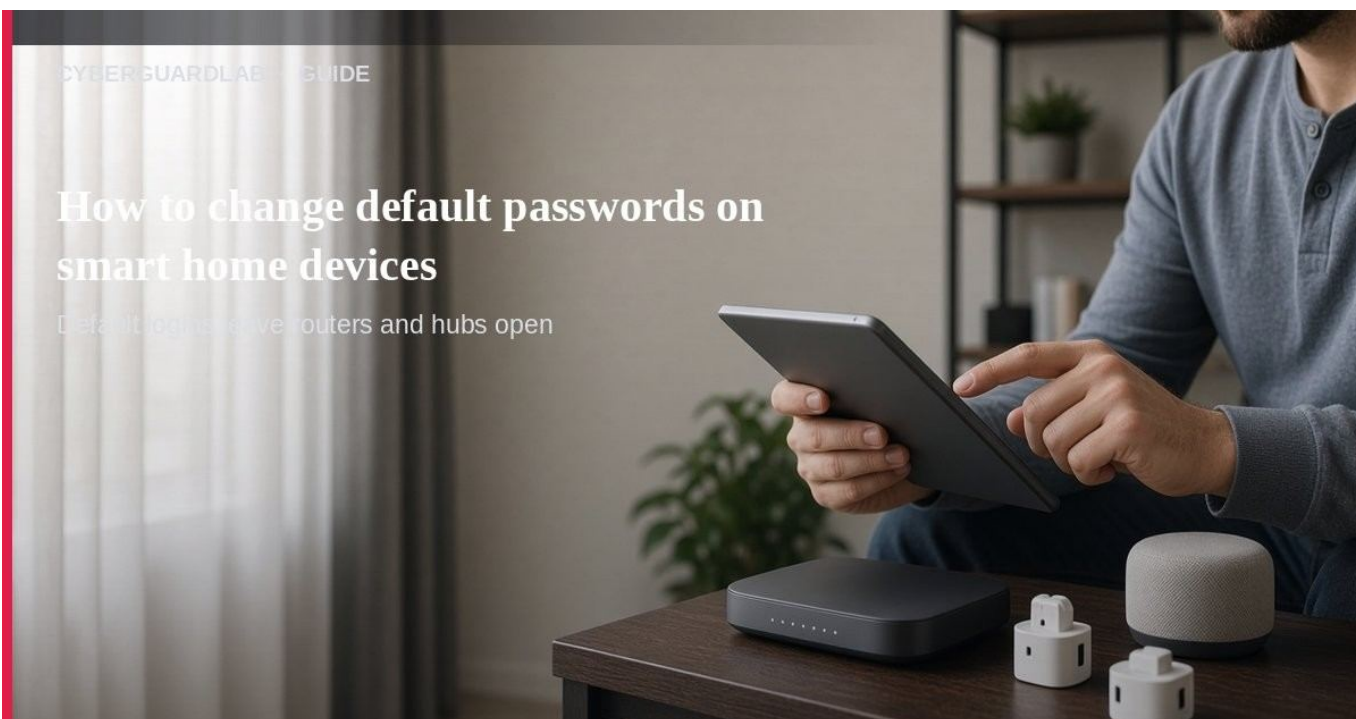
Household antivirus, explained

cyberguardlab.com

How to change default passwords on smart home devices

<https://cyberguardlab.com/blog/smart-home-default-passwords>

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.



CYBERGUARDLAB GUIDE

How to change default passwords on smart home devices

Default logins leave routers and hubs open

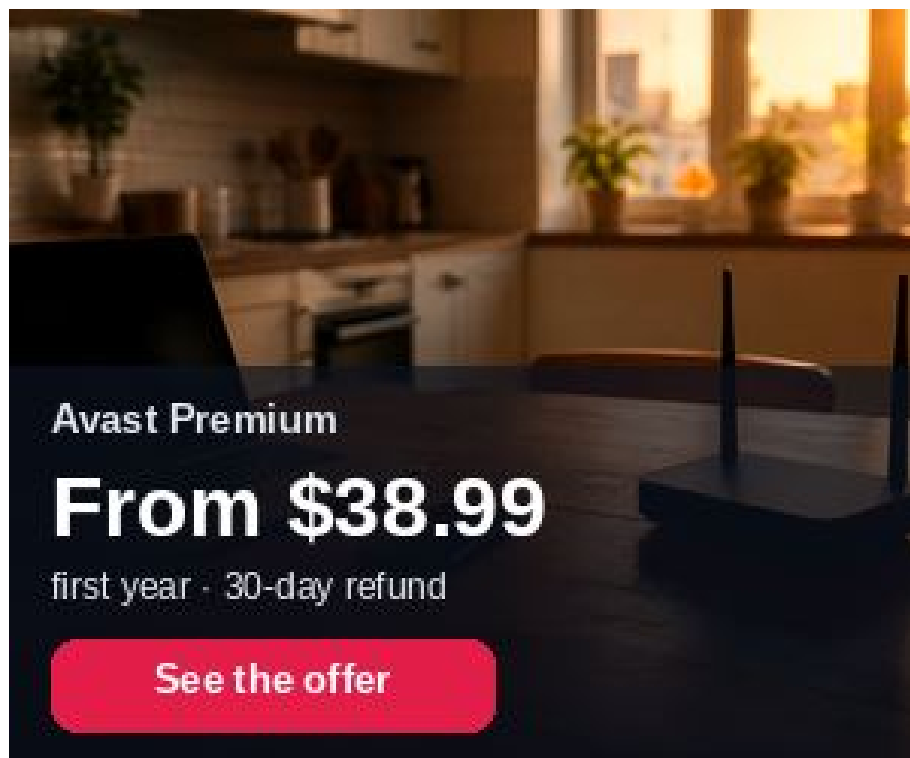
Many smart TVs, plugs, cameras, speakers, and other internet-connected gadgets ship with a factory default password that is shared across the product line and easy to look up online. CISA warns those defaults provide little or no protection and should be changed before (or as soon as) the device joins your network. This guide is about default passwords on household IoT / smart devices - not the full home security camera setup guide, not guest Wi-Fi how-to alone, and not router firmware updates as the primary keyword. No paid antivirus is required to change a password.

1. Why default passwords are a household risk

From CISA device guidance:

Paid link

Avast Premium | See the Avast first-year offer



[See the Avast first-year offer](https://cyberguardlab.com/avast)

Offer page: <https://cyberguardlab.com/avast> Hop: <https://trysecurities.com/offer/avast?dtm=gg&cid=>

- * Defaults are often identical across many units and published in manuals or forums.
- * Attackers scan the internet for devices still using those credentials.
- * A compromised gadget can expose personal info, join a botnet, or become a foothold onto your Wi-Fi.
- * Holiday-gift IoT (smart TVs, cameras, watches, toys) often needs setup the same day - change credentials during unboxing, not "later."

2. Change defaults in 7 practical steps

- * Inventory what's online - List smart TVs, plugs, bulbs, speakers, cameras, printers, and the router itself.
- * Change the device admin password - In the companion app or on-screen settings, replace admin/admin or admin/1234 with a long unique passphrase (CISA: strong passwords; FTC Wi-Fi guide also stresses unique router admin credentials).
- * Change the Wi-Fi join password if the device creates its own hotspot - Some gadgets temporarily host a setup network; lock that down per the manual.
- * Enable MFA on the cloud account when the maker offers it (CISA: MFA reduces damage if the password leaks).
- * Review security/privacy settings - Turn off features you do not need (open remote access, unnecessary cloud sharing).
- * Apply updates / patches - CISA: install manufacturer updates promptly; also see update router firmware.
- * Put IoT on guest Wi-Fi when possible - FTC and CISA-style home advice: a separate guest network limits malware on a gadget from reaching your PCs (see guest Wi-Fi).

3. Router defaults still matter

FTC home Wi-Fi guidance: change both the Wi-Fi network password and the router admin password, use WPA3 or WPA2 Personal, turn off remote management / WPS / UPnP when you do not need them, and log out of the admin session when finished. Defaults on the router undo the work you do on individual gadgets. See also how to check if your home Wi-Fi is safe.

4. When "buy nothing" is enough

- * Unique passwords + guest Wi-Fi + updates solve most default-password risk without shopping.

* A Windows PC still benefits from Windows Security / Microsoft Defender for everyday browsing - not because the TV password changed. See [Is Microsoft Defender enough?](#).

* Skip any pop-up that claims your smart TV is "infected" and demands payment - treat that like other fake warnings (fake virus popups).

FAQ

Do I have to change the password on every smart plug?

Yes if it has a login or cloud account. Shared factory defaults are the weakness CISA calls out.

Is this the same as securing cameras?

Related, but cameras have extra privacy steps covered in home security cameras. This page's primary job is killing default credentials across gadgets.

Can I leave the default if the device is "only on my Wi-Fi"?

Defaults still help anyone who gets on your network (guest device, malware, weak Wi-Fi). Change them.

Do I need paid antivirus for a smart TV?

No. Change the password, update firmware, and segment onto guest Wi-Fi.

What password style should I use?

CISA favors strong unique passwords; a password manager helps - see [password manager vs browser passwords](#).

If you still want a paid suite

Fixing default IoT passwords is free. Microsoft Defender remains a valid buy-nothing choice for household PCs. If you later want multi-device paid protection, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * [Secure New Internet-Connected Devices \(CISA\)](#)
- * [Risks of Default Passwords on the Internet \(CISA\)](#)
- * [Use Strong Passwords \(CISA\)](#)
- * [Turn On MFA \(CISA\)](#)
- * [Update Software \(CISA\)](#)
- * [How To Secure Your Home Wi-Fi Network \(FTC\)](#)
- * [Windows Security overview \(Microsoft\)](#)

Also read

- * [How to secure home security cameras](#)
- * [Set up a guest Wi-Fi network at home](#)
- * [Update your home router firmware](#)
- * [How to check if your home Wi-Fi is safe](#)
- * [Password manager vs browser passwords](#)