

CyberGuardLab

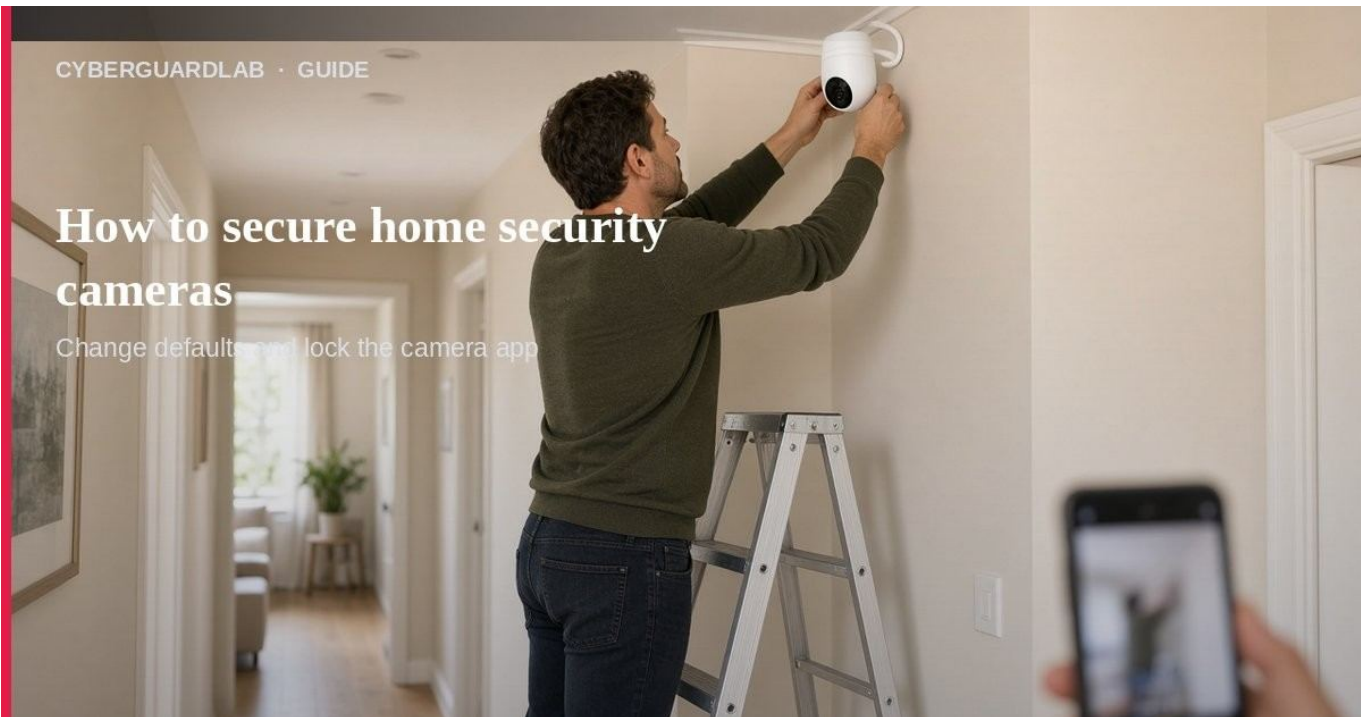
Household antivirus, explained

cyberguardlab.com

How to secure home security cameras

<https://cyberguardlab.com/blog/home-security-cameras>

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.



Home security cameras (doorbell cams, baby monitors, indoor/outdoor IP cameras) let you watch livestreams from a phone app - and they can be hacked if defaults stay weak. Per FTC camera guidance, start with encryption, unique passwords, updates, and a locked-down home Wi-Fi. This guide is about securing cameras you already own or plan to buy, not guest Wi-Fi setup alone or router firmware alone (those pages support this one). You do not need to buy antivirus to change a camera password.

1. Research before you buy (or audit what you have)

From FTC "How To Secure Your Home Security Cameras":

Paid link

Avast Premium | See the Avast first-year offer



[See the Avast first-year offer](#)

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

- * Look for built-in encryption for account info, livestreams, and archived video.
- * Check the manufacturer site, box, or support for how encryption is enabled.
- * Prefer cameras that support strong unique passwords and cloud MFA when video is stored online.
- * Consider whether you need remote viewing at all for private rooms (bedrooms).
- * Look for permission levels if you share the feed with a neighbor or sitter.

2. Lock down the home network first

Cameras usually sit on your Wi-Fi, so the router matters:

- * Strong router password; firewall on; latest router software.
- * Wi-Fi encryption set to WPA3 or WPA2 (FTC Wi-Fi advice).
- * Put cameras on a separate network / guest Wi-Fi from laptops and phones when your router allows it - so a compromised PC is less likely to reach the cams. See guest Wi-Fi and router firmware.
- * Review how to check if your home Wi-Fi is safe.

3. Numbered camera setup checklist

- * Change the default username and password - Never leave factory credentials.
- * Use a unique strong password - Not one reused from email or banking. See password manager vs browser passwords.
- * Turn on encryption / HTTPS - If the camera has a web login, the page should stay on https before and after login.
- * Enable MFA on the cloud account when available (CISA MFA guidance). See turn on 2FA.
- * Update camera firmware and the phone app - Check the maker's site or auto-update; keep the viewing app current.
- * Tighten remote viewing - Encrypt the feed; limit which devices can watch; disable remote viewing if you do not need it.
- * Share carefully - Use admin vs viewer roles; time-limit a friend's access when you are traveling.
- * Review access logs when the camera offers them (odd IPs or odd hours).

4. Privacy habits that do not require new software

- * Aim cameras away from bathrooms and private spaces when possible.

- * Know who has account access after a roommate moves out; rotate passwords.
- * Unplug or power off indoor cams when you want a hard off switch.
- * Before buying, check how long the maker promises software updates.
- * Pair camera hygiene with ordinary PC habits - Defender is enough for many households.

FAQ

How do I secure home security cameras?

Change defaults, unique passwords, MFA on cloud accounts, encrypt livestreams, update firmware/apps, harden Wi-Fi, and prefer a separate camera network.

Do I need paid antivirus for my camera?

No. Cameras are secured mainly through passwords, updates, encryption, and network separation. Antivirus on a PC does not replace those steps.

Is guest Wi-Fi enough?

It helps isolate cameras from daily devices. Still change camera passwords and keep firmware updated.

What if I think someone is watching my feed?

Change passwords, revoke shared users, update firmware, review logs, and contact the manufacturer. Report account takeover patterns at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov) when money or identity is involved.

Should bedroom cameras stay remote-viewable?

FTC urges extra caution for private rooms; consider disabling remote viewing if encryption and access controls are weak.

If you still want a paid suite

Camera privacy is mostly configuration, not a new antivirus subscription. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is unique passwords, MFA, updates, and network separation. If the household later wants 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

- * [How To Secure Your Home Security Cameras \(FTC\)](#)
- * [Securing Your Internet-Connected Devices at Home \(FTC\)](#)
- * [How To Secure Your Home Wi-Fi Network \(FTC\)](#)
- * [Turn On MFA \(CISA\)](#)
- * [Update Software \(CISA\)](#)
- * [ReportFraud.ftc.gov \(FTC\)](#)
- * [Windows security overview \(Microsoft\)](#)

Also read

- * [Set up a guest Wi-Fi network at home](#)
- * [Update your home router firmware](#)
- * [How to check if your home Wi-Fi is safe](#)
- * [Turn on 2FA for Gmail, Apple, and bank](#)
- * [Password manager vs browser passwords](#)