

5 home security cameras you must avoid, Consumer Reports warns

 [msn.com/en-us/lifestyle/shopping/5-home-security-cameras-you-must-avoid-consumer-reports-warns/ar-AA1X4VXh](https://www.msn.com/en-us/lifestyle/shopping/5-home-security-cameras-you-must-avoid-consumer-reports-warns/ar-AA1X4VXh)

Cassian Holt

January 21, 2026

5 home security cameras you must avoid, Consumer Reports warns

Consumer Reports has identified five specific home security cameras that fall short on security, privacy, or performance, despite being marketed as ways to keep households safer. The stakes are high, since a vulnerable camera can invite spying hackers into the most private spaces. Shoppers comparing systems need to know which models to skip so they do not pay to put an easy entry point for intruders on their own walls.

According to one review of [five cameras](#) flagged by Consumer Reports, the Wireless Outdoor Camera struggles with both reliability and the security features associated with the SCM301. When a camera that is meant to deter crime instead introduces new digital risks, homeowners may end up less protected than before installation. For anyone already using SimpliSafe equipment, this finding raises questions about whether to keep the SCM301 in service or replace it with a better rated alternative.

The Arlo Ultra 3rd Gen also appears on the Consumer Reports list of devices that do not meet expectations. Evaluators point to a mix of concerns around how this premium model balances advanced features with privacy protections. Although the Ultra 3rd Gen promises high resolution footage and smart alerts, the same connectivity that enables those features can create openings if the software and account security are not handled carefully.

Security testers who examined [Arlo Ultra](#) alongside other cameras concluded that its shortcomings are serious enough that buyers should look elsewhere. Earlier reporting on vulnerable home cameras warned that spying hackers can easily see inside a home if a system such as an Arlo setup is not adequately protected. When a high end model ends up on a list of products to avoid, it signals that price alone does not guarantee strong digital defenses.

The Wyze Battery Cam Pro is another specific model that Consumer Reports recommends skipping. Analysts reviewing five underperforming cameras describe concerns about how the Wyze Battery Cam Pro manages its wireless connection and security controls. A battery powered design is meant to give homeowners flexible placement, but that flexibility loses value if the camera becomes an easy target for unauthorized access.

Coverage of [Home Security Cameras](#) explains that the Wyze Battery Cam Pro lands on the list alongside better known brands because of these tradeoffs. For renters and homeowners who often choose Wyze for budget friendly smart gear, this warning has real financial and privacy

implications. Choosing a different model can prevent the frustration of unreliable alerts and the far more serious risk of strangers watching recorded clips.

The Kangaroo Indoor + Outdoor Cam is marketed as a simple, all purpose solution that can move between rooms and exterior walls, yet Consumer Reports places it among the five cameras to avoid. Evaluators raise red flags about how this device protects user data and how well it stands up to attempts to bypass its security. A camera that covers both indoor and outdoor spaces can collect especially sensitive footage, which makes any weakness more alarming.

Investigations into [cameras that are](#) describe how spying hackers can easily see inside a home if a device is poorly secured. When a product like the Kangaroo Indoor + Outdoor Cam is singled out in that context, it signals that the convenience of a dual purpose camera does not outweigh the potential exposure. Households that want flexible coverage are better served by models that pair portability with stronger, independently vetted protections.

The Philips Hue Battery Camera rounds out the five cameras that Consumer Reports says consumers should avoid. This model is part of a broader smart lighting and security ecosystem, which makes its security posture especially significant. If the camera component is weak, it can undermine confidence in the entire Philips Hue setup, since a single compromised device can provide an entry point into the home network.

Analysts who reviewed five problematic cameras, including the Philips Hue Battery Camera, describe in [their findings](#) how integration with other devices can multiply the damage if a camera is compromised. For smart home users who rely on Philips Hue for lighting schedules, presence simulation, and app based control, that risk is significant. Choosing a better rated camera and pairing it with strong passwords and two factor authentication can help keep the benefits of smart lighting without inviting unwanted surveillance.

*This article was researched with the help of AI, with human editors creating the final content.

This article may contain affiliate links that Microsoft and/or the publisher may receive a commission from if you buy a product or service through those links.