



Your Gift Goes TWICE As Far

We advocate for strong data privacy protections to help you take charge of your personal data. Donate today to have your gift matched and support all our work to keep you safe and informed.

Choose your donation amount



How to Keep Your Home Security Cameras From Being Hacked

CR's digital privacy and security experts offer their best advice for protecting your privacy

By Daniel Wroclawski

Last updated: May 26, 2020

When you shop through retailer links on our site, we may earn affiliate commissions. 100% of the fees we collect are used to support our nonprofit mission. [Learn more.](#)



Smart security cameras that can catch a thief in the act can be a great tool for protecting your home. But they're also a gateway for hackers to spy on you because they can access them through the internet. No wonder, then, that in a nationally representative survey conducted by Consumer Reports in 2018, 54 percent of Americans considered loss of privacy a reason not to use smart devices.

News stories about home security cameras getting hacked have become all too common. You may recall a story from January 2019 that went viral about a California family's Nest security camera being hacked to play fake warning messages that North Korea launched

What Matters to You Matters to Us

We test thousands of products so you can create your best home.

Join

Nest sent an email to its customers offering tips on how they can protect themselves, but Nest itself wasn't breached. Hackers probably got the log-ins to the family's account by other means.

How Hacks Happen

One way security cameras are vulnerable to hacks is through a technique called "credential stuffing." Hackers use usernames and passwords from other data breaches (that other hackers share online) to gain access to accounts. The combination of large data breaches, such as those at Equifax and Target, and consumers reusing the same passwords—52 percent of internet users reuse or modify the same passwords—make the work easy. In recent years hackers have made the log-in credentials for over 8.2 billion online accounts available on the internet.

MORE ON SECURITY CAMERAS AND PRIVACY

[CR's Home Security Camera Ratings & Buying Guide](#)

[Tips for Better Passwords](#)

[Password Manager FAQ](#)

[CR's Home Security System Ratings & Buying Guide](#)

[Digital Security & Privacy Guide](#)

This type of hack doesn't require the breach of a security camera company's system, so every brand is at risk. "These companies aren't technically at fault," says Robert Richter, who leads security and privacy testing for Consumer Reports. "Most companies offer a two-factor authentication system that acts as an extra deterrent against attacks like this. But there is more that these companies could do, like encouraging people to use that added security feature by default."

How to Protect Yourself

Data breaches and subsequent credential-stuffing attacks won't be going away anytime

Join

Or, [Sign In](#)

1. Keep your camera's firmware up to date. Manufacturers that are serious about protecting their cameras will routinely release firmware updates that fix software bugs and patch security vulnerabilities. Some cameras will automatically download and install these updates, while others require that you check for them on your own. (You'll usually find an update button under the Settings menu in your camera's app.)

2. Change your camera's password. In a nationally representative CR survey on data privacy conducted in May 2019, 13 percent of respondents with at least one online account said they used the same password for all of their accounts. That makes it a cinch for hackers to gain access to multiple accounts. Always create a unique password for each account. Here's the best way:

Do: Use something long and complex—like a random phrase or string of characters—with numbers, symbols, and uppercase and lowercase letters.

Don't: Include any personally identifiable information, such as names, birthdates, etc. Hackers can often get this information from public social media profiles, such as those on Facebook and Instagram, and then use it to guess your passwords and gain access to your accounts. You also want to avoid simple, commonly used passwords, such as [SplashData's 100 worst passwords of the year](#). For more tips on strengthening your passwords, read [our tips for better passwords](#).

3. Set up a password manager. [These programs](#) generate incredibly strong, random passwords for your digital accounts, securely store and remember them for you, and even automatically insert them into log-in prompts. Many password managers are free to use and available on an array of devices and web browsers.

4. Set up two-factor authentication if your camera offers it. This is an extra layer of security. You opt to have the camera company send you a single-use passcode via a text message, phone call, email, or [authentication app](#) that you use in addition to your username and password when you log in to the account. That way, if hackers crack your password, they still won't be able to access your camera unless they also gain access to your passcode.

But not all camera companies offer two-factor authentication. Among the models in CR's [home security camera ratings](#), only three major brands currently do: Amazon, Nest, and Ring.

All of these methods can improve your chances of avoiding a hack, but they're not foolproof. "None of these methods will work perfectly on their own," says Richter. "But right now, these measures are our best tools. Use them all!"

Top Cameras With Two-Factor Authentication

Consumer Reports conducts data privacy and security tests on wireless security cameras to help you find models that are as secure as possible. Cameras that include two-factor

evaluate each model's public documentation (such as privacy policies) to see what claims the manufacturer makes about the way it handles your data.

Below are a few cameras that do well in our data privacy and security tests and offer the extra security of two-factor authentication. They're listed in alphabetical order by brand.

CR QUICK TAKE



Amazon Cloud Cam (Key Edition)

Price: \$120

- 🔒 DATA PRIVACY
- 🔒 DATA SECURITY
- 🔒 VIDEO QUALITY



Unlock Home Security Camera Ratings

Become a Member or Sign in

CR QUICK TAKE



Nest Cam Indoor NC1102ES

Price: \$119.99 - \$199.99 [Shop](#)

- 🔒 DATA PRIVACY
- 🔒 DATA SECURITY
- 🔒 VIDEO QUALITY



Unlock Home Security Camera Ratings

Become a Member or Sign in

CR QUICK TAKE



Join

Or, [Sign In](#)

Nest Cam IQ Indoor NC3100US

Price: \$299.00 - \$299.99 [Shop](#)

-  DATA PRIVACY
-  DATA SECURITY
-  VIDEO QUALITY



Unlock Home Security Camera Ratings

Become a Member or Sign in

Digital security threats are on the rise, but a few simple measures can help protect your information. Share your privacy strategy, and our experts will recommend ways to do it better.

TIME TO COMPLETE: 5 MINUTES

[Let's Begin](#)

Passwords & Firmware 101

Online privacy and security are huge issues facing a lot of people today. On the "[Consumer 101](#)" TV show, Consumer Reports expert Maria Rerecich explains why it's not just phones and computers that people should be concerned about.

Recently Tested Home Security Cameras

See our full list of [home security camera ratings](#)

[Join](#)

Or, [Sign In](#)



Blue by Adt
Indoor Camera



Toucan
TWC200WU



Zmodo
Sight SD-H2601



Arlo
Ultra VMS5140-100NAS



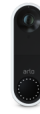
TP-Link
Kasa Cam KC200



TP-Link
Kasa Smart KC300S2
System (2 Camera
Kit)



D-Link
DCS-8525LH



Arlo
AVD1001-100NAS



D-Link
DCS-8300LH



Eufy
Cam E 1-Cam Kit



Blink
XT2



Arlo
Pro 3 VMC4040P