How to keep your smartened-up home safe from hackers

December 28 2017, by Anick Jesdanun

This July 25, 2017, file frame grab from video shows the Nest Cam IQ camera. As people get voice-activated speakers and online security cameras for convenience and peace of mind, are they also giving hackers a key to their homes? Many devices from reputable manufacturers have safeguards built in, but safeguards aren't the same as guarantees. (AP Photo/Ryan Nakashima, File)

More people are getting voice-activated speakers and other smart devices for convenience and security. But doing so could also be giving

hackers a key to their homes.

Many devices from reputable manufacturers have safeguards built in, but those can't guarantee against hacks. Gadgets from startups and no-name brands may offer little or no protection.

Before buying one, here are some risks to assess.

___

LISTENING IN

Speakers with built-in microphones are increasingly popular. Devices such as Amazon's Echo and Google Home let people check the weather or their personal calendar with simple voice commands. Beyond that, many smart TVs and TV streaming devices now have voice-activated functions, often for playback controls and video search. Many newer toys also come with microphones so kids can talk to them and get canned responses.

Many of these devices are constantly listening for your commands; when they receive them, they connect to corporate servers to carry them out. What if you're having private conversations at home? Are they getting sent over the internet, too?

In some cases, sound recordings will only leave home when you trigger the device. You might have to speak a command phrase like "OK Google" or press a button to get the device's attention. Check before buying to make sure a product includes such safeguards.

In this Wednesday, Sept. 27, 2017, file photo, Amazon Echo and Echo Plus devices, behind, sit near illuminated Echo Button devices during an event announcing several new Amazon products by the company, in Seattle. As people get voice-activated speakers and online security cameras for convenience and peace of mind, are they also giving hackers a key to their homes? Many devices from reputable manufacturers have safeguards built in, but safeguards aren't the same as guarantees. (AP Photo/Elaine Thompson, File)

Some gadgets go further. Smart speakers, for instance, typically have a mute button to disable the microphone completely. Amazon says its mute function involves disconnecting the circuit, so that hackers cannot override the intent.

But there's no easy way for consumers to verify manufacturer promises, such as Amazon's assertion that the Echo never transmits recordings to the cloud unless it's been activated. That's where it helps to stick with reputable brands, as their reputations are at stake if they're caught in a

lie. Bigger companies can also quickly fix security holes that crop up.

Missteps are still possible, even with reputable brands. One of the WikiLeaks disclosures alleged that the CIA commandeered some Samsung smart TVs as listening devices even when the TV appeared to be off. And beware of internet-connected toys , as manufacturers frequently rush their products to market, sometimes skimping on privacy features in the process. (You can check online to see if other parents or consumer groups have identified problems.)

One more catch: Voice commands sent over the internet are typically stored indefinitely to help manufacturers personalize their services (and, potentially, advertisements). These voice snippets may include music or conversations in the background. They can be sought in lawsuits and investigations. Reputable brands let you review and delete your voice history; be sure to do so regularly.

___

In this Wednesday, Sept. 27, 2017, file photo, Amazon Echo Spots are displayed during a program announcing several new Amazon products by the company, in Seattle. The round version of the Echo Show has its own 2.5-inch display that can provide visual information, such as the weather or a clock face. It also provides access to Alexa and supports optional video-calling support. Once people get their first smart product, they are likely to buy more. (AP Photo/Elaine Thompson, File)

WATCHING YOU

Online security cameras such as the Cam IQ , from Google sibling company Nest, let you check in on your pets or kids when you're not home. They also typically store video online, so you can see whether your housekeeper actually cleaned the kitchen last week. Some services routinely send video to online storage; others do so only when triggered by a sound or motion.

Again, reputable brands are likely to take security seriously, but no system is perfect.

If you want to be very careful, you might want to turn the camera to face the wall when you're home. You might also want to turn off the microphone, since it could capture background conversations. Or just unplug the camera altogether ... though you'll also have to remember to reconnect it when you leave.

Along similar lines, consider covering up the front-facing camera on your laptop with opaque tape unless you need it regularly for video chats. Laptops aren't supposed to send video unless you activate an app that needs it, but malware has been known to activate the camera remotely.

In this Wednesday, Sept. 27, 2017, file photo, David Limp, senior vice president of Devices and Services at Amazon, displays a new Echo, left, and an Echo Plus during an event announcing several new Amazon products by the company, in Seattle. Internet-connected lights, locks and laundry machines are on the cusp of broadening beyond tech-savvy enthusiasts. Voice-activated speakers such as Amazon's Echo and Google Home are partly the reason. The more people use

such speakers, the more they seek out what else they can do. (AP Photo/Elaine Thompson, File)

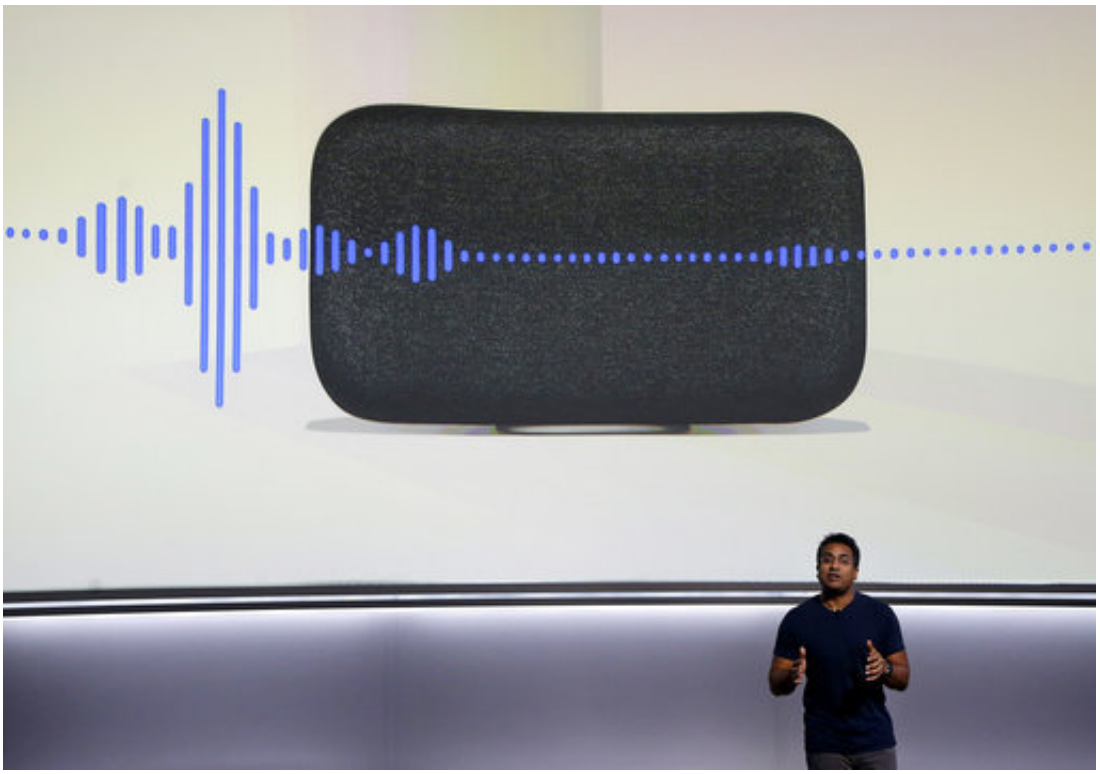
___

DIGITAL TRAILS

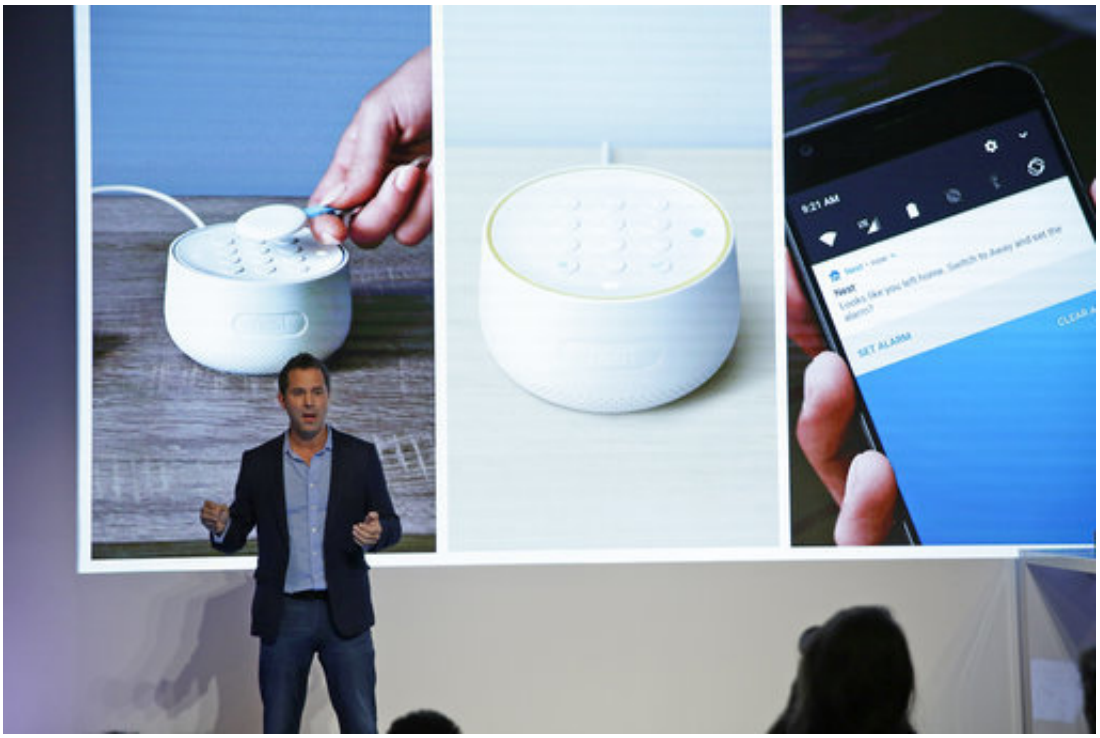
Smart locks let you unlock doors with an app, so you can let in guests even when you're not home. Burglars might try to hack the system, though it's often easier for them to just break a window.

Some rental properties are also turning to smart locks to control access. When you move out, the landlord can automatically disable your digital key. But these systems also let landlords track your whereabouts and those of your guests. If you create a guest key that's used daily, for instance, the landlord might suspect you have an unauthorized occupant.

Even if you own the home, these keys can leave a digital trail. In a child-custody dispute, for instance, your ex might subpoena the records to learn that you've been staying out late on school nights.



In this Wednesday, Oct. 4, 2017, file photo, Google's Rishi Chandra speaks about the Google Home Max speaker at a Google event in San Francisco,. Once people get their first smart product, they are likely to buy more. They also tell friends and neighbors about them, or perhaps buy some as gifts. (AP Photo/Jeff Chiu, File)



In this Wednesday, Sept. 20, 2017, file photo, Maxime Veron, head of product marketing for Nest Labs, talks about the features of the Nest Secure alarm system during an event in San Francisco. As people get voice-activated speakers and online security cameras for convenience and peace of mind, are they also giving hackers a key to their homes? Many devices from reputable manufacturers have safeguards built in, but safeguards aren't the same as guarantees. (AP Photo/Eric Risberg, File)