Internet-connected 'smart' devices are dunces about security

March 9 2017, by Mae Anderson And Barbara Ortutay

This April 13, 2016, file photo shows the seal of the Central Intelligence Agency at CIA headquarters in Langley, Va. Everything from your TV to your lights and shades can be controlled by an app on your phone or even your voice. But the allegation that the CIA and MI5 commandeered some Samsung smart TVs to work as listening devices is a reminder that inviting these "conveniences" into your home comes with a risk. (AP Photo/Carolyn Kaster, File)

These days, it's possible to use your phone—and sometimes just your

voice—to control everything from your TV to your lights, your thermostat and shades, even your car or medical device. (At least, once you have gadgets that can listen.)

But the WikiLeaks allegation that the CIA commandeered some Samsung smart TVs as listening devices is a reminder that inviting the "Internet of Things" into your home comes with some risk.

How safe are your connected devices? Tread carefully, but don't freak out, experts say.

A GROWING INDUSTRY

Connected devices are unquestionably popular. Research firm Gartner expects there to be 8.4 billion connected "things" in use in 2017, up 31 percent from 2016. By 2020, this number could reach 20.4 billion, with smart TVs and digital set-top boxes serving as the most popular consumer gadgets.

For businesses, meanwhile, smart electric meters and commercial security cameras are expected to be the most popular "internet of things" products.

Such gadgets are convenient, but they can present easy targets for hackers. In October of 2016 hackers seized control of webcams and digital video recorders and recruited them into internet "botnets" that launched denial-of-service attacks against popular websites such as Netflix and Twitter, forcing them offline for some users.

LIMITED GOVERNMENT

There's a growing call for regulation to secure connected devices, but it's unclear whether this will happen. Last year, the Department of

Homeland Security released a report describing runaway security problems with devices that recently gained internet capabilities, a collection that includes medical implants, surveillance cameras, home appliances and baby monitors.

"The growing dependency on network-connected technologies is outpacing the means to secure them," Department of Homeland Security Secretary Jeh Johnson said at the time. This, of course, was during the Obama administration; more regulation so far appears unlikely under President Donald Trump.

Forrester Research analyst Josh Zelonis said consumers can't wait for the government to fix things. Instead, he said, people have to demand that manufacturers are accountable for the security of their products and that they support the products throughout the product's lifetime, not just when it's sold.

Which, of course, is far easier said than done.

BRAND APPEAL

One problem: Many people don't realize they have to secure connected devices with passwords like they do with computers. "People don't think of a TV or a camera as a computer and that's all it is," said Gartner analyst Avivah Litan.

If a device comes with a default password, it needs changing the moment you hook it up. Similarly, your Wi-Fi password shouldn't still be the one it came out of the box; it needs a hard-to-guess passphrase to ensure that it can't be easily hacked.

Another problem: Cheaper devices from no-name companies also pose more of a security risk. While big companies like Apple, Amazon or

Samsung can patch up security holes as soon as they find them, smaller companies don't have the resources—or, sometimes, the ability or willingness—to do so.

"Bigger companies typically have more resources and more to lose, so they are typically more secure," said Patrick Moorhead, analyst at Moor Insights & Strategy.

Password-protecting most connected devices, though, should go a long way toward ensuring they won't be used to take down Netflix.

"Don't buy from smaller vendors," Moorhead said. "Don't buy devices that don't encrypt data everywhere." And change the password if you can.

MEASURED CAUTION

Sydnee Thompson, a 24-year-old from Troy, Michigan, is cautious but ultimately sanguine about her connected devices. She has an internet-connected TV, but she's been reluctant to get a "smart" device like Amazon's Echo home assistant because of worries that it would always be listening—and that others might also.

But Thompson uses a smartphone and already assumes that if the government wants to track her, it can. "If the government wants to find out something about you, they will," she said. "It's just the world we live in."

Cameron Matz from Stafford, Virginia, said he has several smart TVs and plans to keep using them. "We can't be afraid to live our life because some person out in the world is listening in on your conversation about daily activities."