SAFE AT HOME?

Smart devices have created new conveniences — and new risks

BY MATT ALDERTON

GETTY IMAGES

Having a voice-activated smart speaker in your home is like having a personal concierge. Whether you want to know the weather, hail an Uber or hear your favorite song, simply ask your Amazon Echo or Google Home. Your wish is their command. But what if your concierge could be kidnapped and turned against you?

"Ultimately, any device you put in your home that's connected to the Internet is at risk," says Gary Davis, chief consumer security evangelist for Intel Security, a software company based in California.

A 2014 study by Hewlett-Packard examined 10 of the most popular smart-home devices and found an average of 25 security vulnerabilities on each. A 2015 analysis of 50 devices by Symantec, a leading cybersecurity company based in Virginia, likewise found at least one security flaw in all of them.

For consumers, the message is clear: "Smart" isn't always "safe." Here are some ways your smart-home devices can put you at risk:

INFORMATION SHARING

"There's a concern about what information these connected devices are collecting," says attorney Christopher Dore, a partner at Edelson PC, a Chicago-based law firm that specializes in class-action lawsuits against consumer technology companies. Even seemingly mundane facts could become a liability. For example, the company that makes your smart refrigerator could collect data about your diet and sell that to your insurance company, which could use the details to raise your premiums. In a real-life scenario, law enforcement officials in Arkansas subpoenaed an >

5 Trustworthy Smart-Home Devices

There's no such thing as a hack-proof device, but you can increase your home's smart security by choosing those with built-in safety features from manufacturers with good cybersecurity track records. Here are five:

BY MATT ALDERTON

ASKED AND ANSWERED

If you need to know the weather or want to hear a song, ask Amazon's Echo. You'll quickly have a response from this smart speaker that has numerous security features. For example, you can turn off its listening function and delete your Alexa command history using its companion app. *$179.99*

HEATING THINGS UP

The Nest Learning Thermostat, which adapts to your life and programs itself, features "Secure Boot" technology that blocks incompatible or malicious software, ensuring that only Nest's software is running on the device. *$249*

LIGHT UP YOUR LIFE

Illiminate the house while you're away to keep would-be burglars at bay. Philips Hue white and color ambiance A19 starter kit allows you to control lighting away from home. In 2016, security researchers demonstrated how Philips Hue smart bulbs could be hacked from as far as 400 meters. Proving its commitment to security and transparency, the company worked with the researchers to quickly engineer a fix. *$199.99*

A MUST-SEE TV

In addition to offering true-to-life color, the Samsung QN65Q7F flat 65-inch 4K ultra HD smart QLED TV now comes with GAIA, a three-layer security solution that's designed to safeguard all areas of the smart TV ecosystem, including its connected services, software and hardware. *$3,499.99*

SECURITY IS KEY

August Smart Lock, Apple HomeKit Enabled lets you lock and unlock your door with a digital instead of physical key. Because it has to comply with Apple's stringent security requirements — which mandate end-to-end encryption of information shared between smart-home and Apple devices — its HomeKit edition enjoys an inherent security advantage. *$229*

PROVIDED BY THE COMPANIES

Echo owner to turn over its recordings, hoping the audio would lead them to an arrest in a murder case.

DEVICE HIJACKING

During a 2016 conference, Davis learned how hackers could remotely install ransomware on a connected thermostat. In the middle of summer, they could set the thermostat to 99 degrees and refuse to unlock it until the owner pays. They could even program smart lights to create a strobe effect that could cause an epileptic seizure. The potential for similar scenarios is endless.

NETWORK PENETRATION

Davis says hackers could use connected devices as "back doors" into your home network. Once inside, they can traverse your wireless router to get inside your computer or smartphone — and access all the information inside them, including usernames, passwords to banking and e-commerce sites, Social Security numbers and personal photos.

DDOS ATTACKS

Distributed denial of service attacks, or DDOS, occur when hackers virtually disable companies by inundating websites with traffic from multiple sources — and they use your smart-home devices to do it. The downside for homeowners could be restricted access to video-streaming services or social media platforms, as was the case in October 2016, when an attack utilizing more than 100,000 connected devices such as DVRs and printers blocked access to Twitter, Netflix, Amazon, PayPal and other popular sites.

Ultimately, however, experts say the best way to protect yourself might be the simplest: Don't buy technology you don't really need.

"In the technological world, it takes a certain amount of skepticism to protect yourself," Dore concludes. "Maybe you can tell you're out of milk without a Wi-Fi-connected fridge. Just open the door." ■

GETTY IMAGES