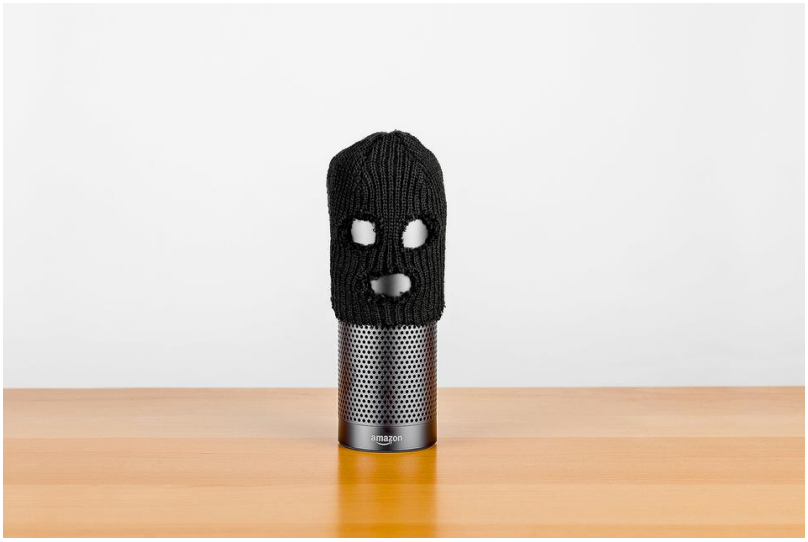
LEADERSHIP

Alexa, Just How Secure Are You?

Virtual assistants are vulnerable to hacks, eavesdropping and more. But there are ways to reduce the risks.



Check your voice recordings from time to time to be sure your smart speaker isn't picking up more than you think.
ILLUSTRATION: KEVIN VAN AELST FOR THE WALL STREET JOURNAL

By Matthew Kassel
Updated May 29, 2018 6:13 pm ET

You may think of your virtual assistant as a kind of trusty companion, giving out weather forecasts, recipes, news and all sorts of ephemera on request.

But these devices also pose a host of security risks that render users vulnerable to hacks, eavesdropping, data siphoning and other threats that might not be immediately apparent. That danger was highlighted Thursday when Amazon.com Inc. AMZN **-0.20%** ▼ said one of its Echo home speakers mistakenly recorded a private conversation and sent it to someone in the owners' contact list. Amazon, confirming a report by a local television station in Seattle, said the device misunderstood pieces of a conversation as commands.

While there's no way to ensure that such devices as Amazon's Alexa or Google's Home are completely safe, there are steps that can help protect your privacy. Such measures are increasingly important: According to a Gallup poll released in March, some 22% of U.S. adults use voice-activated assistants, a number that is certain to keep rising.

JOURNAL REPORT

- Insights from The Experts
- Read more at WSJ.com/LeadershipReport

MORE IN CYBERSECURITY

- CIOs' Biggest Security Fears
- How to Create a Cybersafe Company Culture
- Do Huawei and ZTE Pose a Real Threat?
- The Paper Ballot Makes a Comeback

Here are some tips to help keep your device as secure as possible.

Never buy secondhand. While prices can be steep for new devices, it's generally a bad idea to seek out deals on used smart speakers, says Candid Wueest, a cyberthreat researcher at Symantec Corp. The device could easily be manipulated, he says, into a remote eavesdropper on proud display in your house.

Don't defer to the default settings. Pay attention to your device's default settings and be conscious of the information you allow it to access. In many cases, you may be unknowingly putting your privacy at risk. For example, connecting your device with your calendar, enabling remote management from the web or linking a third-party account like a music streaming service can expose you to additional vulnerabilities. Going through this process "might feel a little tedious," says Mr. Wueest. "But you should do it."

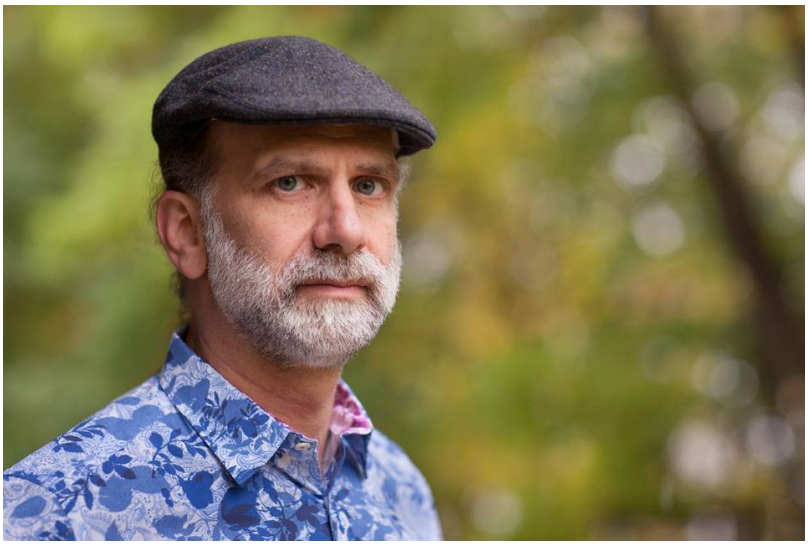
Use a separate router. Connect your device with a Wi-Fi router that is different from the one you normally use at home. It will act as a firewall, says Pam Dixon, executive director of the World Privacy Forum. To be sure, many routers carry hidden subscription fees and are hard to install, she says. As an alternative, you can create a guest network with a strong password on your home router—and also use that network for other internet-connected devices such as lightbulbs, door locks or thermostats.

Be careful what you say—or hit mute. Make a habit of checking your voice recordings from time to time to be sure your device isn't picking up more than you think—either through a hardware defect or because you've accidentally activated the microphone, which is triggered by wake words like "Alexa" or "OK, Google."

In most cases, you can go into the cloud and delete your recordings, though you should check your device's privacy rules because they can vary. Deleting recordings may slightly degrade the performance of your assistant, which learns more about you as you interact with it. But you may have good reasons to pare them down. "There are personal risks," says Ms. Dixon. "I can imagine that there have been divorces over this."

Use voice profiling. For certain functions like on-demand shopping, you may want to make sure that your speaker only takes commands from your voice, though the technology isn't perfect.

Another wrinkle is that this introduces a biometric voice print to the cloud, which could be stolen, experts say. You can set up multifactor authentication along with a spoken password to better protect your private data.



Cybersecurity expert Bruce Schneier says one privacy solution is to simply not own a smart speaker. PHOTO: GEOFFREY STONE

Don't buy one at all. "That is my personal solution," says Bruce Schneier, a cybersecurity expert who lectures on public policy at Harvard University. For Mr. Schneier, the real threat to our privacy is companies like Google and Amazon, which are also vulnerable to hacks and whose privacy policies can be vague and hard to decipher. (Google and Amazon both say they are committed to privacy.) Although regulations recently went into effect in the European Union that will make data collection more transparent, it isn't yet clear how all companies in the U.S. will be affected. Meanwhile, Mr. Schneier says, it comes down to trust: "As far as security is concerned, you're at the mercy of the company."

Mr. Kassel is a writer in New York. He can be reached at reports@wsj.com.

Appeared in the May 30, 2018, print edition.

- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**