Shared from the 2018-05-29 San Francisco Chronicle eEdition

Be smart when you use smart gadgets

By Barbara Ortutay and Anick Jesdanun

Mark Lennihan / Associated Press 2015

Revelations that an Amazon Echo sent a private conversation to an acquaintance show the risks that come with tech devices.

Revelations that an Amazon Echo smart speaker inadvertently sent a family's private conversation to an acquaintance shows the risks that come with new technologies.

According to Amazon, the Echo's Alexa voice assistant misheard a word as "Alexa" — a trigger to activate the device — and interpreted subsequent conversation as a "send message" request. That conversation in a home in Portland, Ore., was then recorded and sent to an acquaintance in Seattle on the family's contact list.

Amazon blamed an "unlikely" string of events, and the company already has many privacy safeguards built into the device. Yet the incident shows that even with the best intentions, the risk is never zero. Gadgets these days come loaded with microphones and cameras — some smartphones even have three. They are all vulnerable to hacking or programming errors, and there's nothing consumers can do to eliminate the risks short of unplugging entirely.

But there are ways to minimize the risks for when gadgets don't act the way they are supposed to:

Kill the microphone: Most smart speakers have a physical button to disable the microphone, so a private conversation can't be recorded to begin with. You can hit that when you're having sensitive conversations. The button on the Echo will turn red; other devices have similar cues. It doesn't make sense to keep the mike disabled throughout the day, though. If the Echo can't hear you, it won't be able to order more toilet paper or play smooth jazz.

Limit the microphone: Disabling the microphone isn't practical on a smartphone, but you can limit what apps have access to it. Go to the settings and turn off mike access to all but the essential apps — such as a voice recorder or videoconferencing. Netflix doesn't really need voice access; you can simply type the show you're searching for.

About that camera: Facebook CEO Mark Zuckerberg famously puts a piece of tape over his laptop's camera to prevent spying if anyone were to hack his device. Buy yourself a roll. Or use bandages. If you have a home-security camera that's connected to the internet, turn the camera to the wall when you're home. Just remember to turn it back before you leave, or you defeat the point of having a security camera.

Block the signals: For smart-phones and other gadgets you carry with you, a shielding bag, or Faraday bag, can help prevent unwanted spying. The good ones will block cellular and other signals, meaning privacy-compromising information such as your location won't leak out either. Just remember, your phone won't get any calls while it's in the bag — that's the whole point.

Be informed: Apple, Samsung and other tech companies have worked over the years to ensure that their products work "out of the box," without users having to pore through lengthy manuals and operating instructions. The downside is that users are often unaware of all the things their gadgets can do, good or bad. Checking reputable online reviews, how-to guides and even instructional videos will help you get the most out of new technologies. They'll also tell you about any known glitches and risks.

Of course, the safest approach is to avoid the gadget altogether. It might not be practical with a smartphone these days, but do you really need a smart speaker or a television set that's connected to the internet? (Well, it's hard to buy a TV without "smart" capabilities these days, but nothing says you actually have to connect it.)

From toothbrushes to slow cookers to toys, if companies can dream it up, it's out there. Companies often release smart gadgets without thinking through the risks and ensuring their security. This makes them easy targets for hackers — or simply programming bugs. This is especially so from manufacturers that aren't well known or that specialize in toys and other things that aren't tech.

Barbara Ortutay and Anick Jesdanun are Associated Press writers.

See this article in the e-Edition Here