A Cute Toy Just Brought a Hacker Into Your Home

By SHEERA FRENKEL DEC. 21, 2017

Researchers recently found the Furby Connect's Bluetooth connection could be hijacked by hackers, letting them turn on the doll's microphone and speak to children. Tony Cenicola/The New York Times

SAN FRANCISCO — My Friend Cayla, a doll with nearly waist-length golden hair that talks and responds to children's questions, was designed to bring delight to households. But there's something else that Cayla might bring into homes as well: hackers and identity thieves.

Earlier this year, Germany's Federal Network Agency, the country's regulatory office, labeled Cayla "an illegal espionage apparatus" and

recommended that parents destroy it. Retailers there were told they could sell the doll only if they disconnected its ability to connect to the internet, the feature that also allows in hackers. And the Norwegian Consumer Council called Cayla a "failed toy."

The doll is not alone. As the holiday shopping season enters its frantic last days, many manufacturers are promoting "connected" toys to keep children engaged. There's also a smart watch for kids, a droid from the recent "Star Wars" movies and a furry little Furby. These gadgets can all connect with the internet to interact — a Cayla doll can whisper to children in several languages that she's great at keeping secrets, while a plush Furby Connect doll can smile back and laugh when tickled.

But once anything is online, it is potentially exposed to hackers, who look for weaknesses to gain access to digitally connected devices. Then once hackers are in, they can use the toys' cameras and microphones to potentially see and hear whatever the toy sees and hears. As a result, according to cybersecurity experts, the toys can be turned to spy on little ones or to track their location.

"Parents need to be aware of what they are buying and bringing home to their children," said Javvad Malik, a researcher with cybersecurity company AlienVault. "Many of these internet-connected devices have trivial ways to bypass security, so people have to be aware of what they're buying and how secure it is."

The problem isn't new, but it's growing as manufacturers introduce a wider range of toys that can connect online, part of an overall trend of "smart" electronics. About 8.4 billion "connected things" will be in use worldwide this year, according to estimates from research firm Gartner, up 31 percent from 2016, with the number projected to rise to 20.4 billion by 2020.

Sarah Jamie Lewis, an independent cybersecurity researcher who tested toys

ahead of the holiday season, said many of the products did not take basic steps to ensure their communications were secure and that a child's information would be protected. She said the toys acted as "uncontrolled spy devices" because manufacturers failed to include a process that would allow the gadget to connect to the internet only through certain trusted devices.

Consider the Furby Connect doll made by Hasbro, a furry egg-shaped gadget that comes in teal, pink and purple. Researchers from Which?, a British charity, and the German consumer group Stiftung Warentest recently found that the Bluetooth feature of the Furby Connect could enable anyone within 100 feet of the doll to hijack the connection and use it to turn on the microphone and speak to children.

Earlier this year, Germany's Federal Network Agency, the country's regulatory office, said the My Friend Cayla doll was "an illegal espionage apparatus." Tony Cenicola/The New York Times

Then there's the Q50, a smart watch for children. Marketed as a way to help parents easily communicate with and keep track of their kids, bugs in the

watch would allow hackers to “intercept all communications, remotely listen to the child’s surroundings and spoof the child’s location,” according to a report by Top10VPN, a consumer research company this month.

And the BB-8 droid, which was released with “The Last Jedi” this month, also had an insecure Bluetooth connection, according to Ms. Lewis’s tests.

SinoPro, the Chinese manufacturer of the Q50 watch, and Genesis, the maker of the Cayla doll, did not respond to requests for comment. Sphero, the maker of the BB-8 connected droid, said the toy is “adequately secure.” Hasbro said the Furby Connect complies with the United States Children’s Online Privacy Protection Act, and that it hired third-party testers to perform security testing on the toy and app.

Toy manufacturers have long searched for ways to bring toys alive for children. While microphones and cameras introduced some level of responsiveness, those interactions were generally limited to a canned response preset by a manufacturer. Internet connections opened up a new wealth of possibilities; now the toys can be paired with a computer or cellphone to allow children to constantly update their toys with new features.

The My Friend Cayla doll, for example, uses speech recognition software coupled with Google Translate. The doll’s microphone records speech and then transmits it over the internet, a function that leaves it open to hackers, according to cybersecurity researchers. If the doll’s owner does not designate a specific cellphone or tablet with which the doll should have an internet connection, anyone within 50 feet of the toy can use the Bluetooth connection to gain access to it. Security researchers have also raised concerns over what type of data the doll collects, and how the data is used.

#toyfail - English Video by Forbrukerrådet Norge

In 2015, a cyberattack on VTech Holdings, a digital toymaker, exposed the data of over 6.4 million people, including names, date of birth and gender, in what experts said was the largest known breach to date that targeted children.

For parents looking to fulfill their holiday wish-lists, the first step is knowing about the risks involved with internet-connected toys. Earlier this year, the F.B.I. issued a broad warning about such toys, advising parents to pay particular attention to how a toy connected to the internet. If a toy connects wirelessly through Bluetooth, it should require some type of unique pin or password, to make sure that connection is secure.

The F.B.I. also recommended that connected toys be able to receive updates

from the manufacturers so they are kept up-to-date. And if the toy stores data, parents should investigate where that data is stored and how securely the company guards the data of its customers.

At a Target store this month in Emeryville, Calif., Sarah Lee, a 37-year-old mother of three, said she was rethinking her choices of presents for her children after hearing about the risks of connected toys.

“That’s so scary, I had no idea that was possible,” she said. “What’s the worst hackers can do? Wait, no, don’t tell me. I’d just rather get my kids an old-fashioned doll.”

Correction: December 22, 2017

Because of an editing error, an earlier version of this article misstated the year when a cyberattack at VTech Holdings exposed the data of over 6.4 million people. The attack occurred in 2015, not last year.