Got a toy that can spy? Here's how to know and what to do

December 21 2017, by Joseph Pisani

In this Friday, Nov. 25, 2016, file photo, shoppers browse at a Toys R Us store in Miami. The toys your kids unwrap this Christmas could invite hackers into your home. That Grinch-like warning comes from the FBI, which said this summer that toys connected to the internet could be a target for crooks who may listen in on conversations or use them to steal a child's personal information. (AP Photo/Alan Diaz, File)

The toys your kids unwrap this Christmas could invite hackers into your

home.

That Grinch-like warning comes from the FBI, which said earlier this year that toys connected to the internet could be a target for crooks who may listen in on conversations or use them to steal a child's personal information.

The bureau did not name any specific toys or brands, but it said any internet-connected toys with microphones, cameras or location tracking may put a child's privacy or safety at risk. That could be a talking doll or a tablet designed for kids. And because some of the toys are being rushed to be made and sold, the FBI said security safeguards might be overlooked.

Security experts said the only way to prevent a hack is to not keep the toy. But if you decide to let a kid play with it, there are ways to reduce the risks. Below, some tips:

RESEARCH, RESEARCH, RESEARCH

Before opening a toy, search for it online and read reviews to see if there are any complaints or past security problems. If there have been previous issues, you may want to rethink keeping it.

Reputable companies will also explain how information is collected from the toy or device, how that data is stored and who has access to it. Usually that type of information is found on the company's website, typically under its privacy policy. If you can't find it, call the company. If there isn't a policy, that's a bad sign.

"You shouldn't use it," said Behnam Dayanim, a partner at Paul Hastings in Washington, and co-chair of the law firm's privacy and cybersecurity practice.

Companies can change their privacy policies, so read them again if you're notified of a change.

USE SECURE WI-FI

Make sure the Wi-Fi the toy will be connected to is secure and has a hard-to-guess password. Weak passwords make it easier for hackers to access devices that use the Wi-Fi. Network. Never connect the toy to free Wi-Fi that's open to the public. And if the toy itself allows you to create a password, do it.

POWER IT OFF

When the toy is not being used, shut it off or unplug it so it stops collecting data.

"They become less of an attractive target," said Alan Brill, who is a cybersecurity and investigations managing director at consulting firm Kroll in Secaucus, New Jersey.

And if the item has a camera, face it toward a wall or cover it with a piece of tape when it's not being used. Toys with microphones can be thrown in a chest or drawer where it's harder to hear conversations, Brill said.

REGISTER, BUT DON'T GIVE AWAY INFO

A software update may fix security holes, and you don't want to miss that fix, says Brill.

But when registering, be stingy with the information you hand over; all they need is contact information to let you know about the update. If they require other information, such as a child's birthday, make one up.

"You're not under oath," said Brill. "You can lie."

BE VIGILANT

If the toy or device allows kids to chat with other people playing with the same toy or game, explain to children that they can't give out personal information, said Liz Brown, a business law professor at Bentley University in Waltham, Massachusetts, who focuses on technology and privacy law.

Discussions are not enough: Check the chat section to make sure children aren't sending things they shouldn't be, Brown said. People could be pretending to be kids to get personal information. "It can get creepy pretty fast," said Brown.

Reputable companies that make toys with microphones will offer ways for parents to review and delete stored information. Take advantage of that.

REPORT BREACHES

If a toy was compromised by a hacker, the FBI recommends reporting it online through its internet crime complaint center at IC3.gov.