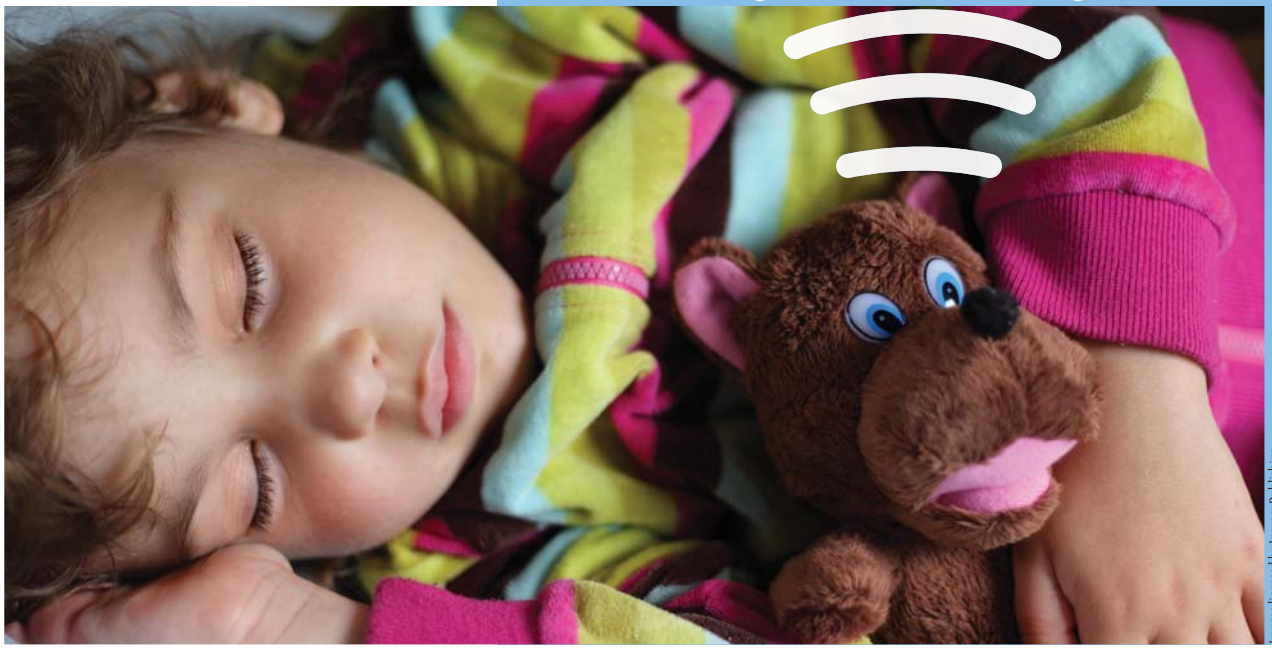
The Smart Parent's Guide to SMART TOYS

10 tips to help protect your family's online privacy and security.

BY PAULA KEHOE



Images licensed by Ingram Publishing

Considering buying a smart toy for your child this holiday season? These web-enabled toys offer fun features that promise to occupy little hands and minds and add a whole new dimension to play. There's a caterpillar that teaches kids how to code, a dinosaur that uses speech-recognition to answers kids' complicated questions, and a learning tablet that allows kids to play with interactive games, selected websites and even exchange messages with smart phones.

But this new generation of toys also comes with privacy and security risks that parents, and the toy companies themselves, are just starting to wake up to.

What are the risks?

Smart toys can capture video, pictures and even sounds and store that information on the Internet, along with the personal data you provide to get the toy working. Recent incidents suggest your child's and family's information may not be safe from hackers.

Last year, Mattel's Wi-Fi-enabled Hello Barbie was at the centre of a big smart toy uproar. Branded as the world's first "interactive doll," kids could talk to Barbie by holding down her belt buckle, their conversations recorded through the doll's microphone.

Privacy and security researchers discovered that the connected doll was vulnerable to hacking, allowing easy access to the doll's system information, account information, stored audio files and direct access to the microphone. Hackers could also access the owner's home Wi-Fi network and other Internet connected devices to steal personal information.

This past January, researchers at Rapid7, a Boston-based security company, found that the app connected to the Fisher-Price Smart Teddy Bear had several security flaws that would allow a hacker to steal a child's name, birthdate and gender, along with other data. Fisher-Price representatives said they had resolved the situation and had no reason to believe that customer information was accessed by any unauthorized person.

As if that isn't enough to startle you into getting your child a Rubik's Cube or a board game for the holidays, last year Hong Kong toy-maker VTech leaked not only the user-

names and passwords of its 6.4 million young users, but also photos, download histories and chat logs. Baby monitors have been hacked, too, allowing strangers to peek in at children in their beds and even talk to them.

While all three companies continue to work to correct identified security flaws, the fact remains that all devices connected to the Internet carry the possibility of being hacked.

"In the last few years, security and privacy have become a really big issue," says Luk Arbuckle, Director, Technology Analysis, Office of the Privacy Commissioner of Canada. "Manufacturers and service providers are asking about how they can secure their devices because it's become such as big issue and they recognize that if they don't do this, they will never gain the trust of the public. If they don't gain the trust of the public, they're never going to sell [products]," he says.

10 tips for parents

So what should you take away from all this? How can you help protect your family's online privacy from potential security threats all while enjoying the season's hottest smart toy?

1. **Buy from reputable brands.** Purchase smart toys from a strong, reliable brand that you trust, so that you can be assured that they're safe and appropriate for your children. "I want to know that if something [malicious] does occur that [the toy company] will get on top of it, secure it and make appropriate changes," says Arbuckle.

2. **Think about the scope of the information you're offering and determine if it's truly necessary.** "Know what personal information [the toy company] wants to collect and what information they need in order to make this device function... and for it to work the way it's intended. For example, it would make sense for them to have to collect an email address because they need some way to verify that it's my account when I go online to try and control that device. But there are other things that I may not be comfortable with. So you have to ask yourself 'do I feel comfortable sharing that information before I buy this device?'" says Arbuckle.

3. **Understand exactly how the smart toy works.** How does it connect to the Internet? What personal data can it access and where is that data stored? Do proper research on the new toy and weigh the risks and benefits – can this toy turn into a privacy hazard? Using data collected from the toy, could someone infiltrate the home Wi-Fi network to snoop on private conversations and steal other personal information?

4. **Read the privacy statement on the packaging.** Before activating the toy and connecting it to the web, carefully read the privacy statement on the box in detail, says Arbuckle. A privacy statement provides examples of data collected by companies, how they use it, and choices you can exercise as a consumer.

5. **Fake your personal information.** Think twice about whether you really need to disclose correct, yet sensitive information about your child to each service that asks for it. "They don't need to know my actual name and definitely don't need to know my child's name," says Arbuckle. He suggests that if you have to enter something, consider using an inaccurate or fake name, date of birth and location, if at all possible. "My kids use a pseudonym online; a fake name like a superhero name that they've made up. We have fun with it. If it's a device or toy that talks to a child and it uses that name, it's kind of funny."

Other tips: "If a device is collecting a date of birth, use a fake DOB. However, do keep it to the correct year for age appropriate controls just to be safe. If a location is required and the device wants to know where you live, you don't have to give the postal code of your home address. Just give it the postal code of your city or town so at least it knows what city or town you are in," says Arbuckle.

6. **Don't use your main email address.** Create separate email addresses and accounts just for this type of thing. "I have an email address I use just for Internet-connected devices," says Arbuckle.

7. **Set up a guest Wi-Fi network with password protection.** If your Wi-Fi router allows you to set up a "guest network," create one and connect the smart toy to it. That will isolate it from your other devices as well as giving you a kill-switch. "This keeps it separate from the rest of your house," says Arbuckle. "It just adds another layer of security."

8. **Create an unbreachable password.** Use complex and secure passwords and refrain from using default passwords. Be sure to change the toy manufacturer's pre-set passwords and make your new password something unbreachable – meaning it should be a completely random string of at least 8-12 letters and special characters.

9. **Install antivirus software and a firewall on all your computers.** "This can be basic, but it's good to have it," says Arbuckle. The more layers of defense, the harder for hackers to use your computer.

10. **Talk to your children about security.** Educate your kids on the risks they face when dealing with Internet-connected gadgets and toys, especially when they're first discovering the Internet. Walk them through the basics: what is the Internet? Why are there bad guys and who are they? How do they protect themselves? How can they set strong passwords?

Want more online privacy tips and information? Visit the Office of the Privacy Commissioner of Canada at www.priv.gc.ca.

Paula Kehoe is a Peterborough-based communications consultant & writer: www.redrockcommunications.ca