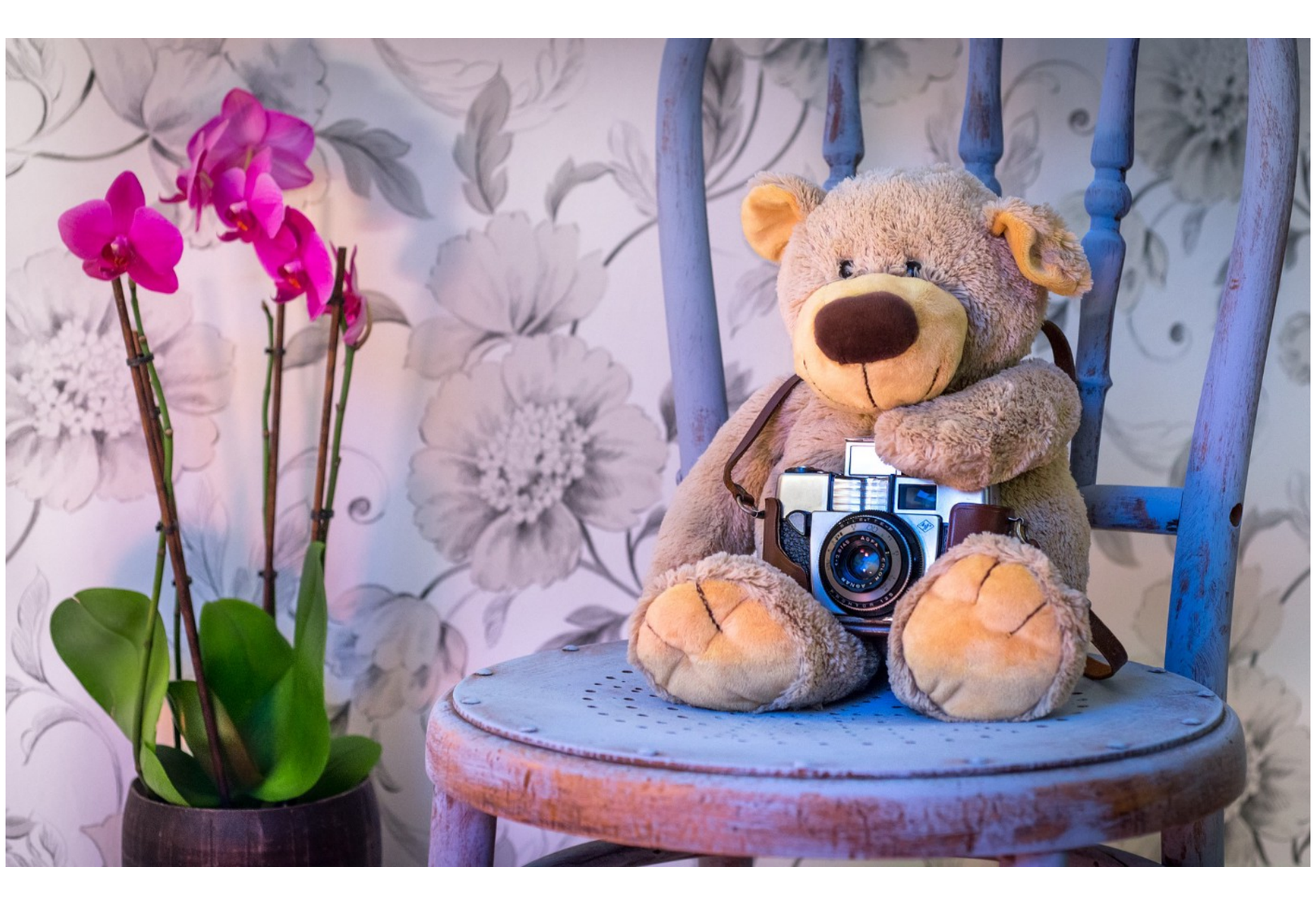
This Innocent Object You Bought Might Be Spying On Your Kids

AXEL Follow
Jan 16, 2018 · 7 min read



The world can be a scary place for parents. You know that not everyone has good intentions. So the more you can do to keep your kids safe the better you feel.

But what if you're doing the opposite? What if you've done something to compromise their security?

You'd want to know wouldn't you?

Of course you would.

You love your children. You want what's best for them. You'd do anything and everything to protect them.

So you go above and beyond to make sure they're protected. You're vigilant, you read the warning labels, you make sure they're wearing their gloves and scarves, and you have a security system at home.

All of that is great…but…something in your house is spying on your kids.

Worse of all, you brought that "something" into the house yourself.

As technology has become more advanced so have the toys for kids. Many parents love "smart toys" for kids. After all they're entertaining and complex and the kids love them…and it teaches them how to use technology. What's not to love?

Well, what you might not realize is these toys have terrible security features and they're easy for anyone to hack into. And when they hack into them they get access to, you guessed it, your kids.

VTech is one of the largest manufacturers of smart toys. They recently had to settle with the Federal Trade Commission (FTC) for a data breach that occurred two years ago.

The worst part? The data for 2.5 million kids was stolen.

An open window in your child's life

When we think about a data breach for adults we immediately think about credit cards, bank accounts, and identity theft. We don't worry about the "small stuff".

But when it comes to kids, even the small stuff can be harmful. The VTech data breach "gave hackers access to customer's names, addresses, encrypted passwords and even birthdays and genders for kids."

How comfortable do you feel about a stranger having this info on your child? What could they do with that information?

It's a scary thought but it's absolutely real.

Make no mistake, this isn't the ramblings of an overcautious alarmist and VTech isn't the only offender in this space. The issue is so serious that even the FBI has issued a warning to parents to be cautious of smart toys.

Some of these smart toys come with cameras, microphones, and GPS trackers. So, yes, there's the potential for someone to listen and watch your child while knowing their exact location.

There's even the potential for an outsider to talk to your child directly through the toys themselves. Can you imagine how harmful that could be in the wrong hands?

It gets worse when you consider the breadth of the reach of smart toys. In 2017 alone 224 million smart toys were shipped and nearly $5 billion in revenue was generated from these toys. Both numbers are expected to nearly double by 2020.

Simply put, these toys have the potential to be the biggest security risks for children worldwide. It will expose millions and millions of children to hackers everywhere.

Suddenly that boring box of crayons doesn't seem so bad anymore does it?

Smart toys, dumb manufacturers

It's not just the hackers either. Many smart toy manufacturers have come under fire for mining this data for their own benefit.

You know the practice by now. You buy a flight to Miami and for the next few days all the ads you see online are for hotels and restaurants in Miami. It's not a coincidence.

We also know that companies are not above collecting children's data. We've even given you pointers on what you can do to protect your kids online.

But when you combine the potential data collected by smart toys with these data mining practices you get an extra special layer of exposure.

Spiral Toys, the makers of the popular toy CloudPets, drew criticism when it was revealed that they stored voice recordings of kids and parents using the toy.

Yes, they saved your conversations with your child!

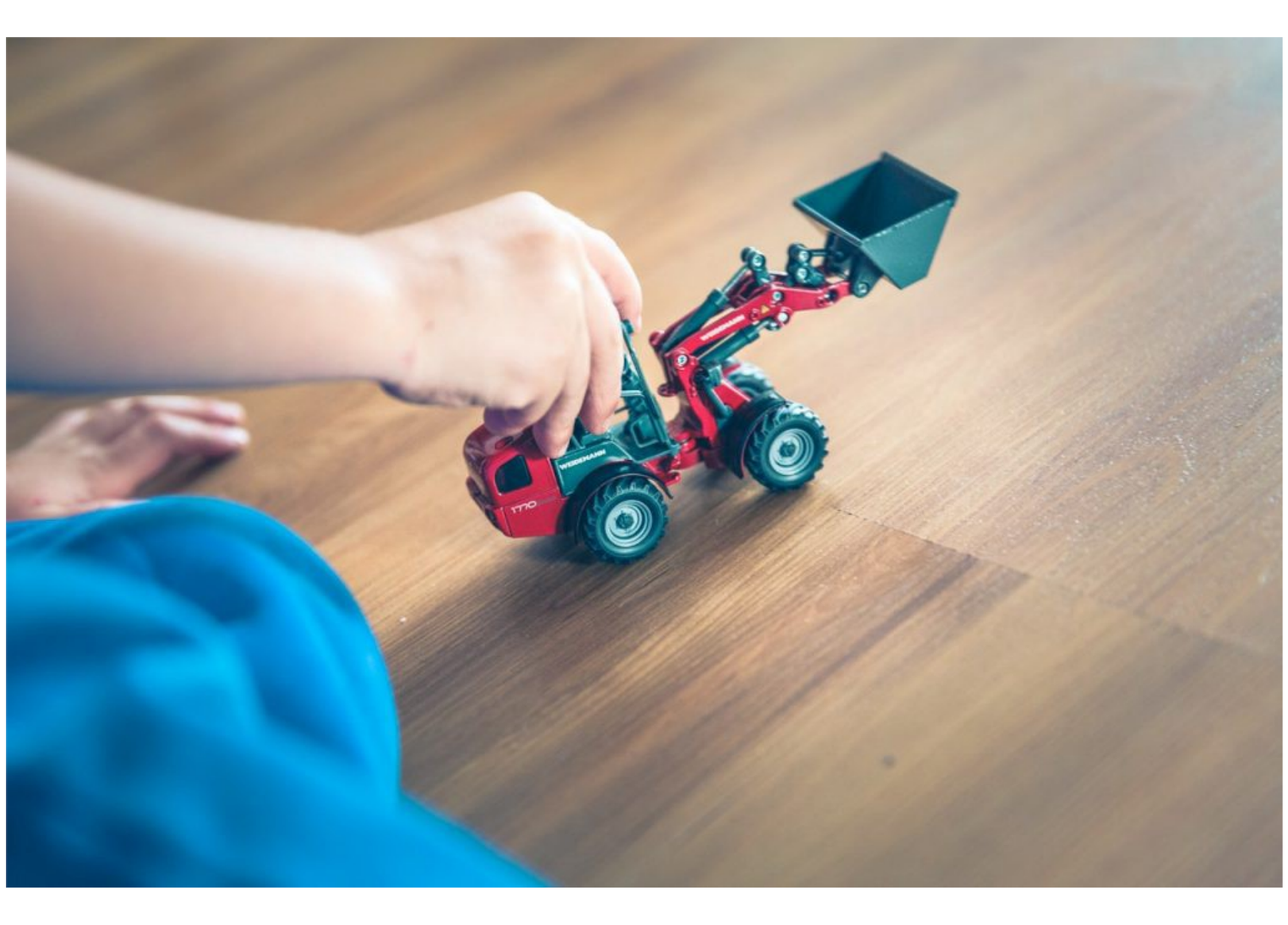
Oh and they left all the recordings on the web without even a password to protect them.

So of course they were stolen and eventually ransomed. Over 820,000 files just exposed and then ransomed to the highest bidder.

Some countries are already taking a stand against smart toys.

Germany banned a toy called Cayla from the market due to its ability to record and transmit conversations without the parents' knowledge. In the UK there is a movement to ban toys with known security flaws.

These are good policies to have in place. But we all know that we can't rely on the government to have our best interests at all times.



As always, we need to ask the question why do these companies collect this data to begin with? And, more importantly, why don't they have security protection on everything?

Then, of course, the question of what can we do to protect our children?

"Dumb" toys = safe toys

We have to make sure we're in control of our kids' safety.

Until we know more about smart toys and their security features (or lack thereof) it might be a good idea to hold off on giving them to your kids. Especially younger children that are more vulnerable.

If you've got some smart toys at home already, it's not too late to protect your kids. You can follow this advice from the FBI:

- Connect toys only to a secure WiFi access point.
- If the toy uses Bluetooth, make sure it requires PINs or passwords when pairing with Internet-connected devices.
- Make sure the toy uses encryption when transmitting data to the WiFi access point, the server or the cloud.
- See if the toy can receive software updates and security patches and, if so, keep it updated to the most recent version.
- Find out if the company will notify you if it suffers a data breach, discovers vulnerabilities in its toy or changes its disclosures.
- Provide as little personal information as possible when setting up user accounts for the toy.
- Choose strong, unique passwords when creating your account.
- Pay attention to what your children are doing with the toy, either by monitoring them in person or using the parent portal, if there is one.
- Turn the toy off when your children are not using it, especially if it contains cameras and/or microphones.

If you're still considering buying a smart toy, you should look out for some major red flags as pointed out by SecurityIntelligence.

- The toy is sold only through a ubiquitous, nameless, faceless retailer — in other words, it is available only online.
- The company manufacturing the toy does not have a physical address, return address or consumer complaint number.
- The mobile app provider requires the user to sign up for the cloud service using his or her real first and last name and physical address.
- The toy stays connected to the cloud even when it is off.
- The toy is programmed to receive automatic updates or downloads.
- The toy comes equipped with a long-range receiver and transmitter.
- The cloud provider storing the data is never identified in the end-user license agreement (EULA).
- Neither the toy nor the mobile app comes with an EULA.

Additionally you can look for toys that are certified for approval from COPPA. COPPA is a great organization that was created by the FTC to protect children's privacy.

Alternatively there are a lot of great toys out there that kids love that aren't "smart" but are equally entertaining. Kids love toys of every kind and many kids are just as happy with a regular toy as they would be with a smart toy.

As with anything when it comes to parenting, smart toys need to be researched and vetted so you know what you're putting in front of your kids.

Knowing what you're up against makes it easier to decide what you are and aren't comfortable with.

The whole thing might sound like a lot of work but it's the only way to make sure you can outsmart the smart toys and keep your kids safe!

Liked what you just read?

Do you share our vision of making life easier for people WITHOUT compromising their privacy?

→ Click the 👏 below to **CLAP** for this piece.

→ **SHARE** our story with people you think will benefit from it.

→ Get the latest updates — **FOLLOW** our blog, Reddit, Facebook, or Twitter.

We're working hard to bring you great content. If you have something you want us to write about, let us know in the comments below!

Written by: Vsem Yenovkian

Security Cybersecurity Privacy Hacking Hacker

WRITTEN BY
AXEL Follow
We're AXEL, asking the hard questions on who's doing what with YOUR data. www.axel.org