After the VTech hack, some tips on keeping your kids safe

December 8 2015, byBree Fowler

In this Tuesday, Sept. 28, 2010, file photo, a boy looks at VTech's V.Reader, an interactive e-reader for children ages 3 and older, in New York. Parents around the world have been understandably shaken by the hacking of a VTech database containing information on the more than 6 million children who use the company's toys. (AP Photo/Mark Lennihan, File)

Parents around the world have been understandably shaken by the hacking of a VTech database containing information on the more than 6

million children who use the company's toys.

But what's a parent to do? Internet-connected toys such as VTech's tablets, which ask parents to create personalized profiles for their children, continue to grow in popularity and are expected on many holiday gift lifts this season.

Meanwhile, children have larger digital footprints than ever before, often starting at birth with an announcement on Facebook or other social media.

Here are some answers to common questions about VTech's breach and how to protect your kids' information online:

———

WHAT KIND OF INFORMATION DID HACKERS ACCESS IN THE VTECH BREACH?

The attack compromised the profiles of 6.4 million kids around the world, along with the 4.9 million parent accounts that they were connected to.

The parental accounts included names, email addresses, secret questions and answers for password retrieval, numeric Internet Protocol addresses, mailing addresses, download histories and encrypted passwords. But information in the children's accounts was restricted to names, ages and genders, the Hong Kong-based company says.

The breach didn't expose any credit-card or other financial account information, as payments are handled by an outside company on a separate website.

Some reports suggested that photos of children and chats between kids and their parents might also have been accessed, but VTech Holdings Ltd. says it's still investigating and can't confirm that yet.

___

WHY IS THIS A BIG DEAL?

The worry is that even basic pieces of information could allow nefarious people to start building profiles of children, potentially setting them up for identity theft or worse down the road.

David Dewey, director of research for Pindrop Security, says kids have no credit history and their parents generally aren't checking their credit reports, making them easy targets.

"Fraud could go undetected for years, till they try to open what they think is their first credit card account," says Dewey, also a father to a pair of elementary school-aged girls.

While the worst case scenario would be for the information to be used to kidnap a child, the scenario of a "virtual kidnapping" is more likely, he says.

In that kind of situation, a person would call a parent and use the information they had about their child to convince them that they had kidnapped the child and demand a ransom. A voice recording would make such a scam much more convincing, Dewey says. Voice is something that some VTech devices collect, but it's unclear if any got stolen in the breach.

___

IS IT SAFE TO ENTER INFORMATION ABOUT MY KIDS INTO TOYS LIKE THESE?

Parents have become very accustomed to handing over personal information to companies in order to get a more personalized experience, whether they're setting up a kid's toy or signing up for Netflix. But there's always a chance that the database where it's stored could be hacked.

Parents have to weigh the importance of the information they're giving up against the benefits of having it collected.

Mark Nunnikhoven, vice president of cloud research for the IT security company Trend Micro, notes that when it comes to toys like VTech's, there's nothing stopping you from setting up your child's account with a different name, fake picture and other false information. And most of the time, you can refuse to provide it all together.

———

WHAT ABOUT SOCIAL MEDIA?

It's not realistic to expect most parents to stop posting childhood milestones of Facebook. Social media is often the most efficient way to share pictures and videos with friends and family who live far away.

But Nunnikhoven, also a father to two young kids, says it's important that parents monitor their privacy settings and make sure that what their posting is only going to friends and family. Parents also should think twice before posting pictures of events like school outings and concerts where there are other children involved.

And it's generally a good idea to stay away from Twitter, which basically

broadcasts your information to the entire world, he says.

———

WHAT ABOUT TWEENS AND TEENS WITH THEIR OWN ACCOUNTS? IS IT EVEN POSSIBLE TO CONTROL THEM?

Add this to the long list of things that make parenting hard.

Dewey, who doesn't have a Facebook account because of security worries, tells his daughters to question whether the world really needs to know what they're about to say online before they say it.

Nunnikhoven says that like any other tough issue you talk about with your kids, the important thing is to keep talking about it.

"Not only are the children changing faster than we would like, so is the technology," he says. "As a parent, you need to stay on top of those things."