healthline

Parental Warning: Baby Monitors Can Be Hacked

Written by Jenna Flannigan | Published on August 18, 2016



Many modern baby monitors come with a long list of high-tech features, from wireless connectivity to motion sensors.

But when Vikas Bhatia was shopping for a baby monitor for his little one, he didn't want any of those extra capabilities — and especially not Wi-Fi.

"I don't trust it," he told Healthline.

Bhatia, who is chief executive officer of the cybersecurity firm Kalki Consulting, understands the real risk is that baby monitors with Wi-Fi can be hacked from virtually anywhere in the world.

He won't take the chance that hackers could try to peep at his 3-month-old infant.

Read more: Videos show kids sleeping in unsafe environments »

Parents may not be aware

Most new parents, however, aren't aware of that risk — and some have found out the hard and terrifying way.

For a Washington family, the wake-up call came quite literally when a hacker spoke to their 3-year-old son through his baby monitor, saying, "Wake up little boy, daddy's looking for you."

The parents, Sarah and Jay, asked journalists not to reveal their last name to protect their privacy.

Their son had told them he was afraid because someone was talking to him at night, Sarah told Kiro 7 News.

Then they heard the hacker's voice and noticed the baby monitor's camera following their movements.

It's only one case in a growing list of baby monitor hacking incidents.

In another incident in Texas, parents of a 2-year-old girl heard a hacker's voice through her baby monitor, calling their daughter "a moron" and other disturbing insults.

And in an Indiana case, a mother heard the Police song "Every Breath You Take" playing from her daughter's baby monitor, followed by "sexual noises."

Hackers tend to be opportunistic, explained Bhatia, who has more than 16 years of experience in the cybersecurity field.

Online predators know that people have baby monitors that can be connected to home Wi-Fi networks and accessed through web portals.

"All they're doing is looking for a vulnerability to exploit," Bhatia said.

Read more: Back-to-school healthy habits for children »

The "internet of things"

Baby monitor hacking isn't a rare problem — and it isn't going away.

In 2014, the United Kingdom's Information Commissioner's Office (ICO) warned of a Russian website that was live-streaming footage from thousands of webcams, including baby monitors and other Wi-Fi enabled cameras.

The video feeds came from all over the world and were easily searchable through Google, without the knowledge of the people who own the cameras.

And when it comes to everyday items that families use, baby monitors aren't the only things that can be hacked.

Baby monitors are just one category of devices in a huge spectrum of household products that make up the internet of things (IoT).

"The internet of things is basically the extension of network-capable devices beyond traditional computing devices," Bhatia told Healthline, "Everything from a TV to a fridge to weighing scales in the bathroom."

One of the risks of these devices is that people don't tend to think of them as computers — but they are.

Although people often understand the importance of updating security software on their home or work computer, they may not recognize that network-connected household items can be a security risk, too.

In actuality, Bhatia thinks IoT devices may be even more vulnerable to hackers than traditional computers.

"When it comes to the internet of things, there are fewer people using the devices, both as consumers and on the engineering side, which means it's going to take longer for vulnerabilities to (a) be detected, and (b) when they are detected, to be remediated," Bhatia said.

The problem isn't much closer to being solved than it was two years ago.

Last month, the ICO issued another warning that people are not taking sufficient steps to secure their connected devices, citing baby monitors and music systems as examples.

"A lack of security when it comes to devices could mean that a search engine is used by criminals to locate vulnerable devices and then gain access to them or others on your home network. An attacker could then use your equipment to mount attacks on others or take your personal data to commit identity fraud," the ICO warned.

Read more: Nearly a third of medical studies involving children never published »

Baby monitor challenges

When it comes to protecting yourself and your family from cyberattacks, there are two main issues.

First, the security of the device itself, and second, the actions of a user to keep it secure.

For baby monitors, the challenges are steep.

A 2015 study conducted by Rapid7, an internet security company, tested nine internet-connected baby monitors for security issues.

They gave all but one a failing grade, finding numerous vulnerabilities that could allow a device to be "maliciously abused by an attacker."

To make matters worse, research suggests that the average person who uses the internet is not particularly careful about cybersecurity.

Researchers at Brigham Young University conducted a series of studies that revealed people tend to ignore online security warnings.

In one study, even people who claimed to care about internet security ignored the warnings.

In another study released this week, researchers found people are especially likely to disregard warnings that come at inconvenient times.

Bonnie Anderson, Ph.D., an associate professor of information systems at Brigham Young University, and co-author of the studies, noted that computing devices are less secure than many people assume, and that's especially true when it comes to the IoT.

She stressed that keeping your software updated is one of the best things you can do to keep your devices secure.

"As soon as those updates are out, then malevolent folks can see exactly what's been fixed, and then they know what to target," Anderson told Healthline. "People who are not up-to-date on their updates and patches are then at big risk."

Read more: Digital detox to cleanse yourself of the internet »

Making smart choices

If you're in the market for a baby monitor, Bhatia has some advice.

“The first question I would ask anyone who is buying a Wi-Fi enabled baby monitor is, ‘Do you specifically want to be able to access this monitor from outside the house?’… Most of the time, I hear, ‘No,’” he said.

In that case, you can opt for a monitor that doesn’t connect to the internet. If you’ve already purchased a Wi-Fi enabled monitor, you can turn off that function.

If you do want remote access to the baby monitor, there are steps you can take to make an internet-connected device as secure as possible:

- Before you buy a monitor, do some research to see if the manufacturer is proactive about addressing security issues, such as by releasing security patches and updates.
- Change the default username and password on the device right away. Most IoT products are preset with usernames and passwords that can be found with a simple Google search.
- Choose a password that is long and complex, not a simple word. You can use a password manager to help you keep track of your passwords for different accounts.
- Ensure your home Wi-Fi network is password-protected. To be extra safe, you can set up a separate network for your baby monitor and control which devices are authorized to access that network. Check that your router has logging enabled so that you have a record of any IP address that accesses it.
- If you are fairly tech savvy, you can also change the monitor’s default communications port in its network configurations setting.
- Register your product with the manufacturer so that you receive software updates to fix security issues. Even if you register, it’s a good idea to set a regular reminder for yourself to double check for any updates you might have missed.

For Bhatia and his wife, choosing a baby monitor meant considering the absolutely minimum requirements they needed to keep tabs on their new arrival.

Ultimately, they selected separate video and audio monitors, neither of which is Wi-Fi enabled.

Copyright © 2005 - 2018 Healthline Networks, Inc. All rights reserved. Healthline is for informational purposes and should not be considered medical advice, diagnosis or treatment recommendations.