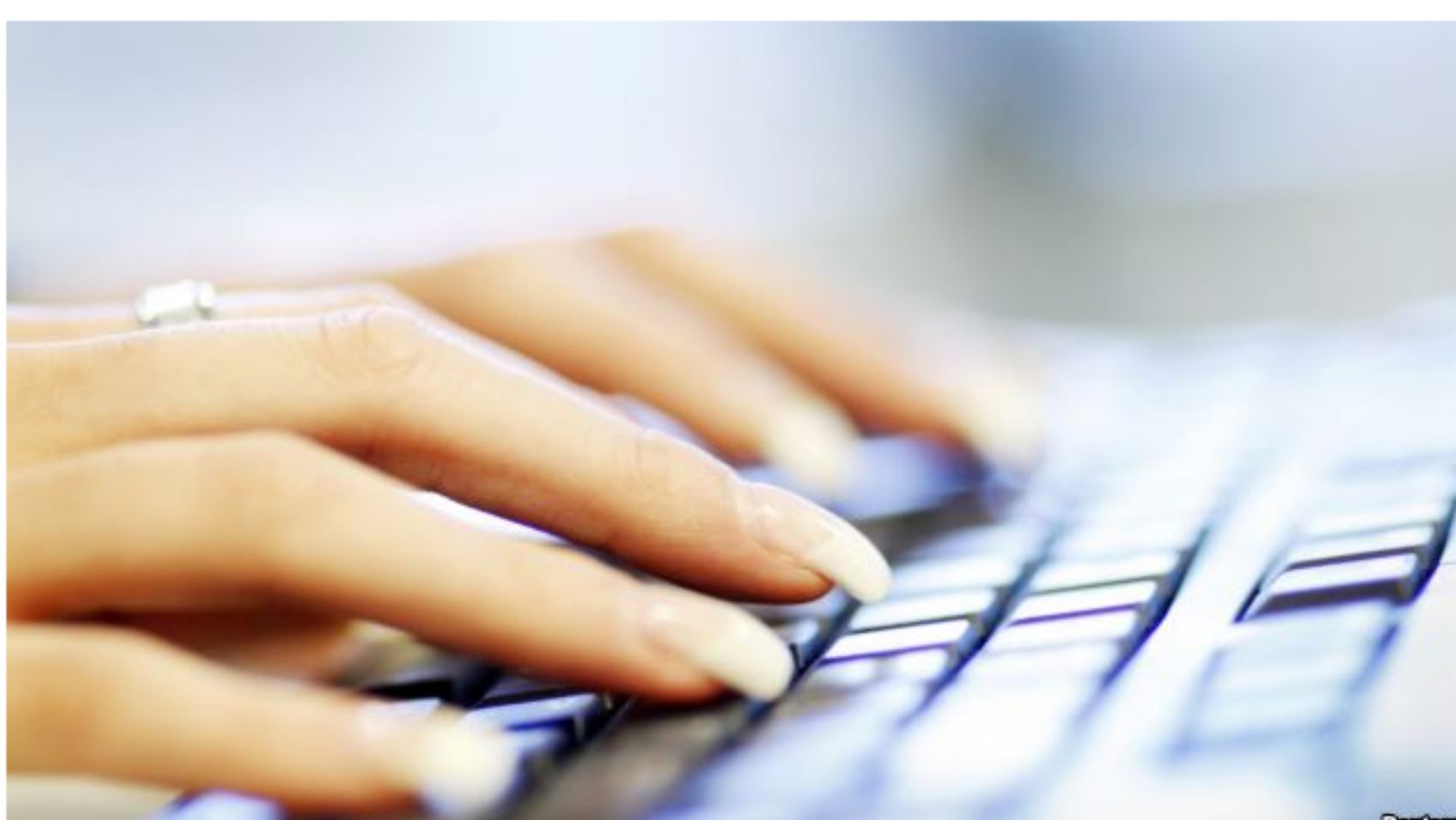


[News / Science & Technology](#)

'Internet of Things' Carries Privacy Risks

Print
 Comment
 Share:



FILE - A woman uses a computer keyboard.

Doug Bernard

March 23, 2015 6:28 AM

There's no need explaining to Adam and Heather Schreck how the Internet can threaten privacy in unexpected ways. They know firsthand.

Last spring, the Cincinnati-area couple was asleep one night when Heather awoke to what sounded like a man's voice coming from their infant's bedroom.

There, Heather found an unknown person was watching their daughter via the video monitor attached to the crib, again and again yelling, "Wake up, baby!"

When her husband entered moments later, the webcam swiveled up to look at the couple, with the user screaming obscenities at Adam until he yanked the camera's plugs.

"Someone had hacked in from outside," Heather told a local TV station.

Added her husband, "You kinda do feel violated."

The Schrecks are among many Americans who are learning how the "Internet of things" — the collection of everyday appliances that users increasingly can manipulate via the Web — can provide equal measures of convenience as well as privacy and security challenges.

While their case grabbed headlines, such stories are becoming more common.

And, according to a security report released earlier this month, the threats presented by the rapidly expanding Internet of Things, or IoT, are likely even larger than previously thought.

Insecurity of things

"Back in the day, it used to be mass-mailing email worms [that worried us], but obviously things have changed," said Candid Wueest, co-author of "Insecurity in the Internet of Things" and a principal threat researcher with the Internet security firm Symantec. "It's clear everything's connected now. Unfortunately, connected also means 'could be attacked.'"

The industry analyst firm Gartner estimates that 4.9 billion "things," or smart devices, will be in use this year, with that number skyrocketing to 25 billion in just five years.

These things increasingly touch on nearly every aspect of our personal and professional lives: smart TVs, closed-circuit cameras, heating and cooling systems, cars, refrigerators, ovens and door locks.

Chances are pretty good that if it can be built, someone will connect it to the Internet.

The IoT promises a world of enhanced convenience.

For example, you can turn up your air conditioning via your smartphone before you return from the beach or switch on and off your home lights and oven while still at work.

'How secure are they?'

But, Wueest said, every new device connected to a home network or Internet creates a new path for hackers to break in. And this, he said, is not an issue many manufacturers are addressing.

"We see people are buying these devices. The question is: How secure are they? Does your neighbor see what you're doing at home? Could he actually switch off your lights?" Wueest asked.

Previous studies have suggested the answer is a qualified yes.

A 2014 study by researchers at HP Fortify found the average IoT device — such as for home alarms, thermostats and garage door openers — has an average of 25 vulnerabilities, with 70 percent of devices vulnerable to attack.

Earlier this year, Wueest and his team at Symantec's Global Security Response Lab began looking more deeply into these connected devices. They analyzed 50 smart home devices, already on the market, for security or privacy exploits.

Nearly every device Wueest's team looked at had one or more security vulnerabilities: most of them basic, and some as fundamental as not having password-protecting devices or requiring user authentication.

"It's devastating and shocking to see that we still see so many devices with no proper authentication implemented," Wueest told VOA. "So for many of the devices we looked at, we actually saw that once you deployed them in your Wi-Fi at home, your network, they don't require any additional authentication. Anyone [accessing] that smart home Wi-Fi can send commands and do what they like."

For example, the Symantec team identified one vulnerability in a popular smart door lock that would have allowed a hacker, with one command, to unlock thousands of doors across the country.

Relearning from the past

The Symantec report details a variety of attack pathways and tactics hackers could use to gain control over a host of smart things.

While some of those include obvious holes, such as password protection, Wueest's team found a range of back-end vulnerabilities nearly identical to those that home computer manufacturers identified and fixed a decade ago.

"It's a beginner's mistake. ... It seems like history is repeating," he said. "We see the same mistakes, like website vulnerabilities or not using passwords being repeated again and again. The question for us: Are the manufacturers not doing it because users are requesting it?"

The report doesn't directly ascribe blame for the security lapses, but researcher Wueest said both users and manufacturers share in the problems and the solutions.

On the user end, he said that even if offered robust password security, most users still opt for all-too-hackable passcodes such as "1-2-3-4."

Additionally, he said, once people get a device up and working, they're often unlikely to adjust the security settings or download software updates to patch security holes — exactly what enabled hacking of the Schrecks' baby cam.

Such good "Web hygiene" habits, Wueest said, can go a long way to discouraging the bad guys.

And while Wueest believes manufacturers should take privacy and security more seriously, the only way that's likely to happen is if customers begin demanding it.

Research manufacturer

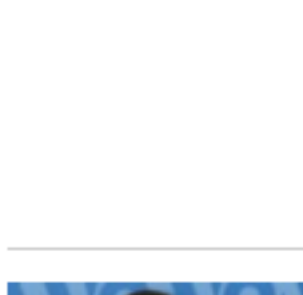
"If you're thinking about buying these devices — and by all means, I use a few of these at home so we're not saying don't use them — you should check out the manufacturer's website and see if they have a record of updating patches and fixes," he said.

"If you don't see anything like this, this might be a good indication that they don't really look into the security."

So, is the IoT something to be welcomed or feared? Should people begin worrying about their toasters or coffeemakers?

No, Wueest said, at least not yet.

But it is time for everyone connecting up those 5 billion smart things in their homes and offices to be aware that they can bring as much insecurity as they can convenience.





Doug Bernard
[@dbjohnson@voanews.com](mailto:dbjohnson@voanews.com)
 Doug Bernard covers cyber-issues for VOA, focusing on Internet privacy, security and censorship circumvention. Previously he edited VOA's "Digital Frontiers" blog, produced the "Daily Download" webcast and hosted "Talk to America", for which he won the International Presenter of the Year award from the Association for International Broadcasting. He began his career at Michigan Public Radio, and has contributed to "The New York Times," the "Christian Science Monitor," SPIN and NPR, among others. You can follow him @dfrontiers.

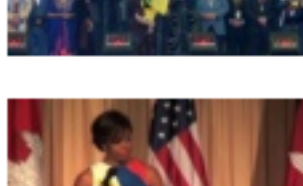
Print
 Comment
 Share:

Tweet (43)
 Recommend
 Share (7)
 +1 (4)
 Pin it

YOU MAY LIKE

- 

Ghani Heads to Washington for First Visit as President
 Visit comes at outset of spring fighting season, with Afghan security forces lacking active foreign military support [More](#)
- 

Turkey's Kurdish Leader Ocalan Calls on Rebels to End Fighting
 Call made in letter to Kurds celebrating Nowruz, or new year, in Turkey's predominantly Kurdish southeast [More](#)
- 

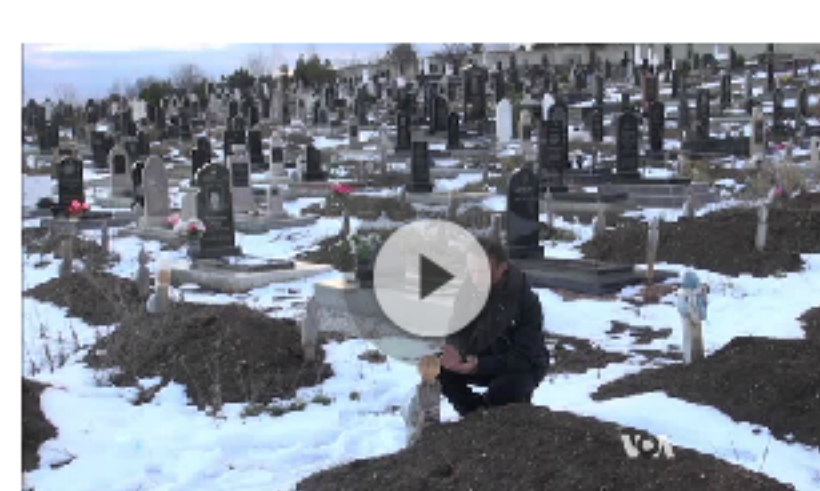
Michelle Obama: Education Gives Girls 'Tools to Speak Up'
 First lady visits Cambodia on trip highlighting global women's education initiative of Peace Corps [More](#)

[Comment on this forum](#)

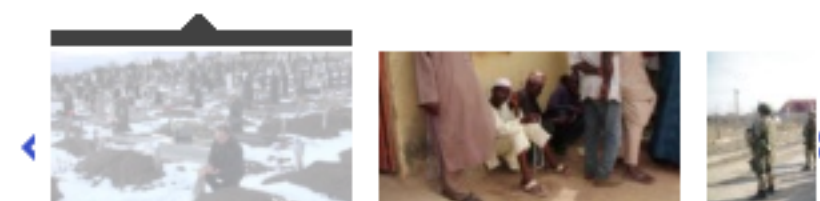
Comments

There are no comments in this forum. Be first and add one

FEATURED VIDEOS



Crimea's Tatars say Climate Worsening Under Russian Rule

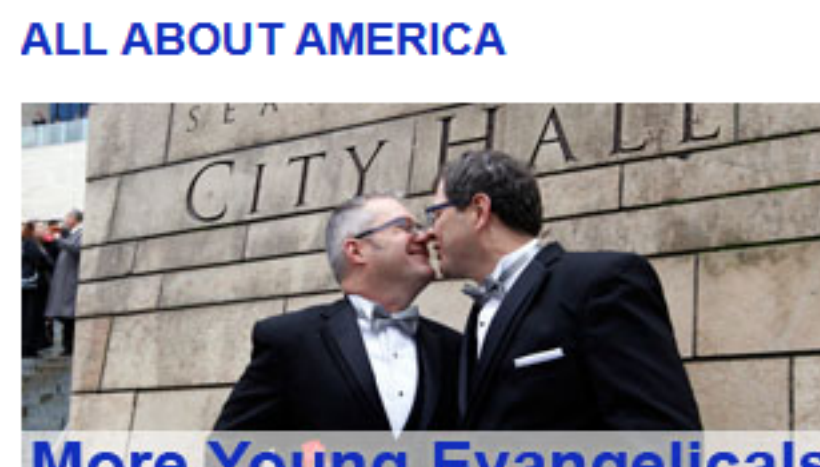


VOA SPECIAL REPORT



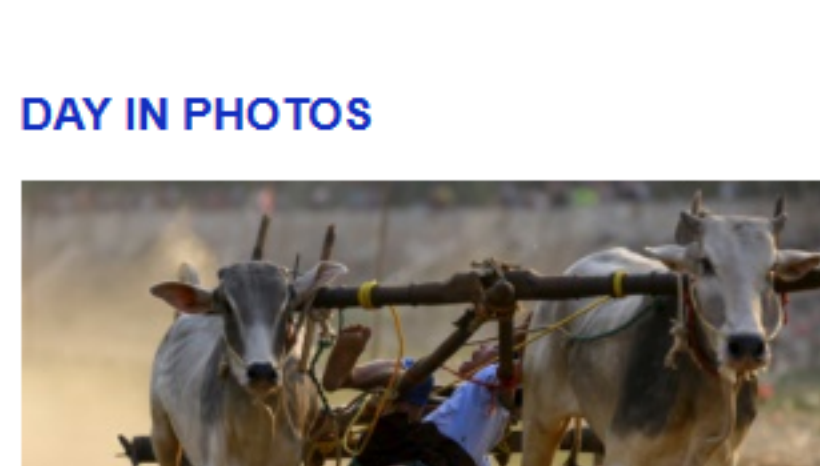
Download the VOA News Mobile App

ALL ABOUT AMERICA



[More](#)

DAY IN PHOTOS



CIRCUMVENTING CENSORSHIP

An Internet Primer for Healthy Web Habits

As surveillance and censoring technologies advance, so, too, do new tools for your computer or mobile device that help protect your privacy and break through Internet censorship.

[More](#)

MORE SCIENCE & HEALTH NEWS

Obama to Announce \$240M in Education Donations at Science Fair

'Internet of Things' Carries Privacy Risks

WHO Rolls Out New Strategy to Wipe Out TB

Liberia Investigates How Latest Ebola Patient Got Infected

UN Report: World Faces 40% Water Shortfall by 2030

[More Articles](#)

BLOGS

Science World

• Science Scanner: MAVEN Finds Surprises, Iron Rain, Exercise Boosts Cancer Treatment 4 days ago

• Science Scanner: Milky Way Bigger than Thought, Hydrothermal Activity on Saturn Moon, New Way to Fight Cavities & Gum Disease, Dwarf Galaxy Surprises Scientists 11 days ago

• Mars Once Abundant With Water 13 days ago

Tectonics

• Text Messaging Gives Malawi's Expectant Mothers a Head Start 3 days ago

• App for Ringing Ears; MusicGlove; Ethical Robots; Trust in Facebook? 4 days ago

• FREAK Bug, Smart Glasses Still Alive; Windows 10 Piracy; IoT Future 5 days ago

Most Viewed

1. Marines Urge Vigilance After IS Posts Threat

2. Obama: Delay on Lynch Nomination 'Purely About Politics'

3. Lee Kuan Yew, Founder of Modern Singapore, Dies at 91

4. NATO General: West Should Consider Arming Ukraine

5. Hundreds Arrested in Indian Academic Cheating Scandal

Most Emailed

Most Discussed