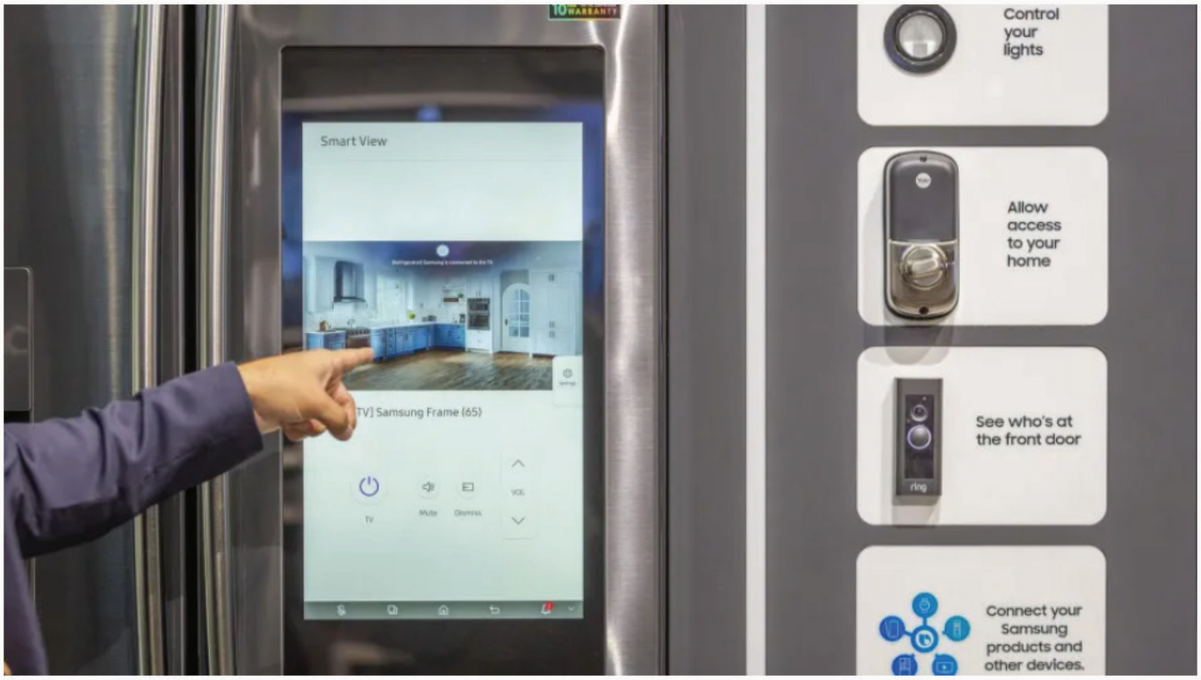
# Column: How to stay secure when all your devices rely on the Internet of Things


Smart View
[TV] Samsung Frame (65)
Control your lights
Allow access to your home
See who's at the front door
Connect your Samsung products and other devices.

Eric Kayne / AP

Earlier this summer, Samsung Electronics America Inc. showcased its different smart appliances for homes during a conference in California.

By CATHY CUNNINGHAM

PUBLISHED: August 9, 2018 at 4:15 p.m. | UPDATED: December 13, 2018 at 12:38 a.m.

Have you ever stopped to think about how many items in your home are connected to the internet?

If you have (or even if you are doing it just now), have you stopped to wonder why? The umbrella term for all these connected appliances, electronics and other devices is "smart."

We are living in the age of the smart home, smart car, smartphone, smart remote, smart thermostat, smart fridge … well, you get the idea.

So, what does all this "smartness" do for us?

Sure, it might allow us to adjust our thermostats when we are a thousand miles away on vacation or enable our microwave ovens to respond to voice commands.

But just how secure are all these internet-enabled devices?

Not very, according to two internet security experts with whom I spoke.

One of those experts is Bruce Schneier, fellow and lecturer at the Harvard Kennedy School of Government and author of the forthcoming book, "Click Here to Kill Everybody: Security and Survival in a Hyper-connected World."

“We prefer our software full of features and inexpensive — at the expense of security and reliability,” Schneier said.

And because our appliances, electronics, cars, medical equipment and other devices essentially have become general purpose computers, they are now at risk for the same hacks as any other computer that runs internet-based software.

“We now have millions of computers — in the form of devices — connected to the internet,” said Matthew Green, an associate professor of computer science at Johns Hopkins University.

This interconnectivity is known as the Internet of Things, he said.

“These computers are all vulnerable,” Green said. “They all have software running on them and unfortunately, not all of it was written by the best software developers. And to make matters worse, the software often doesn’t get updated.”

Both Schneier and Green pointed to the largest distributed denial-of-service attack (DDoS), which happened in October 2016 and infected computers with malware, known as botnets, to bombard servers with traffic until they collapsed.

Hackers took down Twitter, Netflix, Reddit, CNN and many other websites around the world for almost an entire day, both Schneier and Green said.

What was the innocuous conduit for accomplishing this majorly disruptive feat?

Webcams, DVRs and home internet routers with weak passwords and poorly written software — much like the ones you and I have in our homes today.

The problem, Schneier said, is that, “You have no way of knowing if your device is affected by this (or any other) botnet and you kind of don’t care. And there is no way to patch it. It will be a member of that botnet until you throw it away, which could be a decade from now.”

He added, “Once computers start affecting the world in a direct and physical manner, there are real risks to life and property. And the market won’t resolve this.”

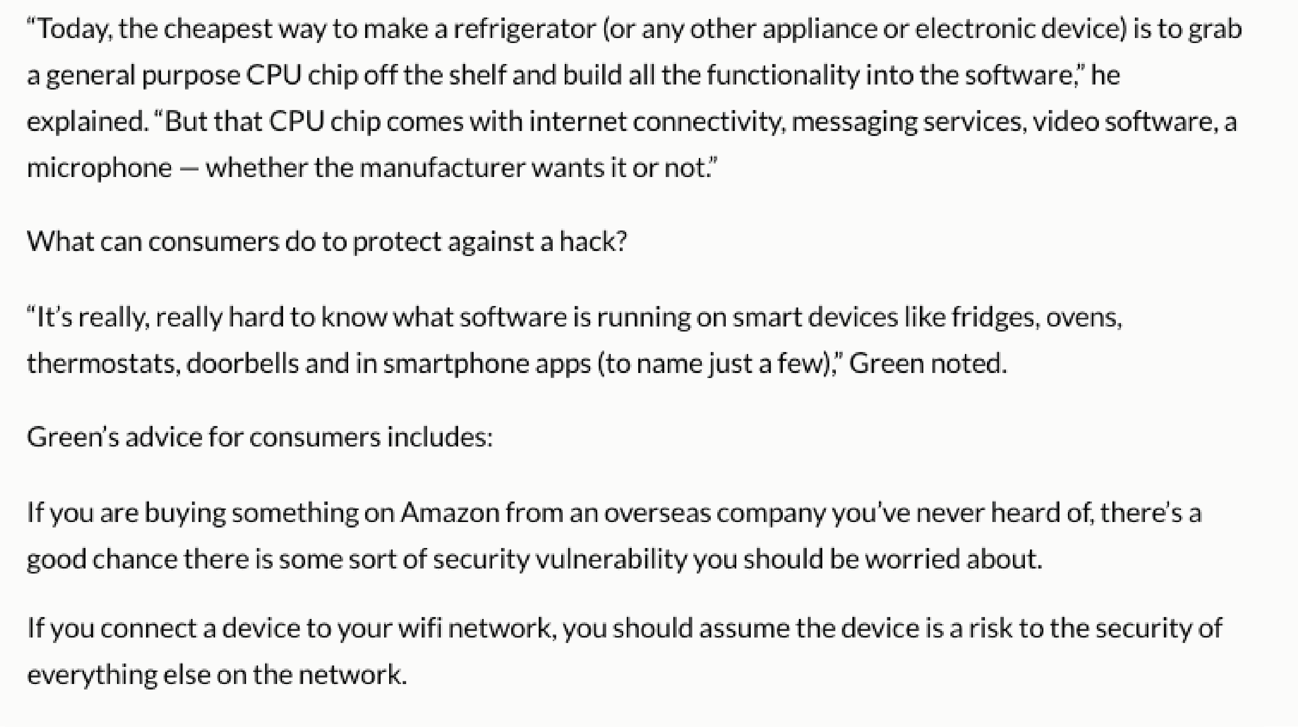
Think disabled cars, purposely interrupted pacemakers and the shutdown of electrical grids.

There are only two ways to fix the problem.

Customers must demand it, which, Schneier asserts, won’t happen because customers don’t really know what’s going on. Governments also should pass laws ensuring that device manufacturers build and update their products to reduce software vulnerabilities, he said.

So, why is it that everything seemingly is moving toward becoming a part of the Internet of Things?

Because it’s cheaper to make appliances and other devices with smart technology than not, Schneier said.



"Today, the cheapest way to make a refrigerator (or any other appliance or electronic device) is to grab a general purpose CPU chip off the shelf and build all the functionality into the software," he explained. "But that CPU chip comes with internet connectivity, messaging services, video software, a microphone — whether the manufacturer wants it or not."

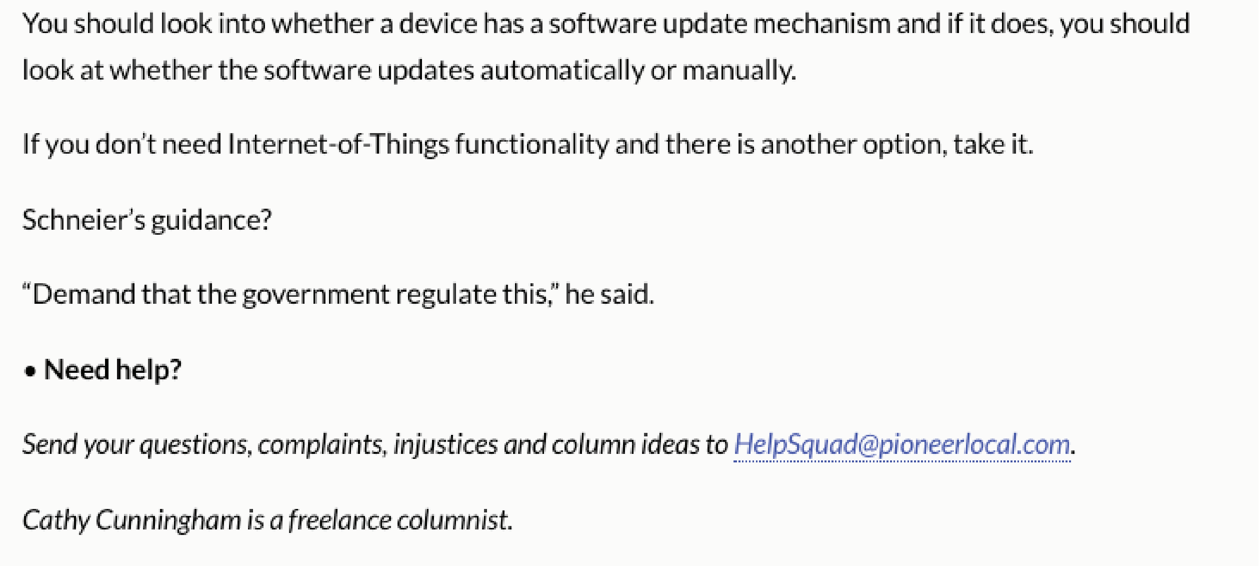
What can consumers do to protect against a hack?

"It's really, really hard to know what software is running on smart devices like fridges, ovens, thermostats, doorbells and in smartphone apps (to name just a few)," Green noted.

Green's advice for consumers includes:

If you are buying something on Amazon from an overseas company you've never heard of, there's a good chance there is some sort of security vulnerability you should be worried about.

If you connect a device to your wifi network, you should assume the device is a risk to the security of everything else on the network.



You should look into whether a device has a software update mechanism and if it does, you should look at whether the software updates automatically or manually.

If you don't need Internet-of-Things functionality and there is another option, take it.

Schneier's guidance?

"Demand that the government regulate this," he said.

• **Need help?**

*Send your questions, complaints, injustices and column ideas to HelpSquad@pioneerlocal.com.*

*Cathy Cunningham is a freelance columnist.*