# Why I won't Connect My Refrigerator to the Internet

February 11, 2019 - It has been almost exactly nine years ago that we first warned our readers about the dangers of smart home technology. Smart home devices include everything from thermostats to digital assistants like Google Home and Amazon's Echo with Alexa. There are cameras, speakers, appliances, baby monitors and even light switches in the smart home category, and all of them need to be connected to your home network if you want to be able to use them when you are away from home. Therein lies the problem. Anything you connect to the internet is vulnerable to hacking, and the number of these devices being hacked is growing.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
  (function() {
    var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
    po.src = 'https://apis.google.com/js/plusone.js';
    var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
  })();
```

Most people don't realize that the push for smart home technology didn't really come from industry. It came as a mandate from the White House Science and Technology Policy Office in 2009 under the guise of giving consumers more control over their electrical usage. It turned out that the government's motivations were a lot different than that - you can read about that here. Regardless of that, marketing professionals around the country also saw an opportunity to market the new technology as a convenience to consumers. And consumers have bought in hook, line and sinker.

There aren't a lot of statistics on the hacking of smart home devices. No agency or organization tracks this and so far regulatory agencies haven't been compelled to monitor statistics. But there are more and more individual reports from people who have been hacked. In a recent widely reported  incident, an Illinois family found out they had been hacked when a voice started talking to them via their smart home speakers. If you go to YouTube and do a search on smart home hacks, you'll get a variety of returns; some showing how to avoid being hacked and others showing footage and interviews of people who have actually been hacked.

There is an irony in some of these reports. Many of these smart home devices are sold as a means to protect your home and your family. But when not property installed, they do just the opposite.

Once your home network becomes compromised, a hacker can gain access to a lot of information about you just by looking at the way your smart home devices are used. If you set your smart thermostat to 60 degrees every day before you leave for work and then turn it up via your cell phone every day before you come home, a pattern of your comings and goings is easy to come up with. That means that a burglar can case your home from the privacy of his own living room without risk of being reported to the police by the neighbors.  And that's just one example.

But maybe the hacker just doesn't like you for some reason. Or perhaps he just likes being a mischief. So he hacks into your thermostat on a particularly cold day and turns your heat off. You're pipes then freeze, your dog gets frozen to death and you have an expensive problem on your hands. At the same time, he turns on your oven and turns off your fridge. And just for grins, he turns on your clothes dryer just because he can. You get the idea.

Is all of this so-called convenience really worth it? Is it so difficult to manually change your thermostat? And why in the world does anyone need to have their laundry equipment connected to their home network? I frankly can't think of single instance in which I've ever thrown the clothes in the dryer, somehow or another forgotten to turn it on and then suddenly remembered that horrible error a few hours later when I was at work. If that ever does happen, I guess I'll just have to deal with it after much gnashing of teeth and be forced to wait until I get home and have to turn on the dryer manually. Oh, the horror!

But since more and more appliances now come with internet connectivity, consumers seem to feel compelled to connect them to their network without thinking through the potential downsides. I know my refrigerator can be connected to my home network even through there is no easy way to setup a secure password for it. Since the only thing I can do with a network connection is change the temp - something I can do manually too - I fail to see the point. Again, in my entire life I've never had he need to change the temperature on my fridge from a remote location.

The point here is that by connecting everything we own to a network, at the very least you are risking your privacy. And you may be creating a safety risk for yourself and your family. So think about what you are doing ,and about how you are doing it.

Before you purchase a smart device, do a little homework. Can that device be protected by a strong password? Figure out if you can install it yourself of if you need professional installation. Are there competitive devices that have a better record for security and privacy? And perhaps more important than any of these questions is this: Do you really need to connect that new device to a network at all? If the answer is "no", then don't.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS