Is the IoT worth it? The real price of intelligent homes

Do you envision coming to a home that anticipates your needs and effortlessly creates the perfect environment for your maximum comfort? Then you'd better be ready to pay, because IoT gadgets are not cheap.

For instance, smart lighting costs between $20 for a single bulb and $160 for a 3-bulb starter kit that lets you adjust intensity, set custom colors, color combinations and schedule lighting to welcome you home or fend off intruders while you're on vacation.

A smart socket can cost up to $50. It gives you the nifty power to turn off any plugged-in device from a mobile application on the smartphone. Comes in handy when you worry you've forgotten your TV or your iron on, right?

A portable Wi-Fi video camera will set you back around $200. It's a device that you should spend an extra dollar on. After all, you need to make sure it functions properly and watches over your home 24/7.

To control every connected device, you might also like a home automation system. That adds another $200 to your expenses list. It will let you manage all your connected devices and appliances to adjust the temperature to match the climate and give you the music and lighting to match your preferences.

Add the smart watch, laptop and smart TV you already own and the investment totals several thousand dollars. And these devices represent a very small fraction of the smart gadgets now available on the ever-expanding IoT market.

The stakes are higher

If someone breaks into your home by taking advantage of one of the new handy, yet security-faulty devices, he can cause real, physical damage.

Your digital identity can also be exposed if your smart socket is unsecured and leaks your Wi-Fi password during setup, for instance. Once inside the home network, someone can intercept unencrypted traffic including online account credentials, images and sensitive banking data you would want private. He can also install malware on connected computers or mobile devices.

Luckily, so, far, attacks have mainly been the work of researchers and have proven to be limited by proximity (the attacker needs to be in the same Wi-Fi network) and the attacker's tech skills. However, it's only a matter of time before more ill-intentioned people see the opportunities and attacks will be performed at a larger scale.

Who would be spying on you?

You may be convinced that no one is interested in the temperature in your home, but be sure that turning your surveillance camera off is something a thief would do.

More importantly, the Internet of Things can become a tool of a mass-surveillance in the hands of governments.

"Security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services," said James R. Clapper, Director of National Intelligence. "In the future, intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

So, investing in your home is a great idea, as long as you insure it.

Bitdefender BOX is an all-inclusive cybersecurity hardware design to protect the entire network and any device connected to it: from phones, coffee makers, washing machines, headphones, lamps, and wearable devices to almost anything else you can think of.

This means your iPhone, iWatch and other Apple devices are also safe against malware, viruses, hacks, phishing, online fraud, spying and data theft. And with the embedded Private Line feature, it secures the connected devices even when outside the home perimeter.

http://www.macworld.com/article/3055513/internet-of-things/is-the-iot-worth-it-the-real-price-of-intelligent-homes.html