CONNECTED HOMES COULD POSE THREAT TO NEW OWNERS

Realtor aims to make transferring of smart devices run smoothly

USA TODAY Weekend Extra 19Feb 2017 Elizabeth Weise

SAN FRANCISCO Realtor Chad Curry recently talked to a homebuyer who worried there was something wrong with the furnace in her new house. Every time she set the thermostat to 70 degrees, it reset itself to 80.

Some sleuthing finally revealed the problem: The former owner's new house was cold, and he kept trying to get the heat to go on by turning up the temperature using the app on his phone. Unfortunately, **his phone was still connected to the thermostat in his old house**.

As the Internet of Things finds itself in houses via connected devices, more and more homes contain hot new tech gadgets that can all too easily become unlocked digital backdoors.

From thermostats to garage door openers to keyless locks, **"people can be vulnerable if they don't reset these,"** said Curry, managing director at the National Association of Realtors.

"It could be something as simple as turning lights on and off and make them think their house is haunted. Or it could be something creepier, like watching through their cameras or locking or unlocking doors," said Charles Henderson, global head of IBM X-Force Red. He spoke on the topic at the RSA computer security conference Friday in San Francisco.

As with many new technologies, companies have focused on getting their connected devices into stores and into customers' homes without thinking through the downstream consequences.

"There hasn't been much discussion of what happens when they sell that device or the house that contains that device," Henderson said.

That's how Curry came to work on a project with the Online Trust Alliance to create a Smart Home Checklist for real estate agents — not that the list is any more user-friendly than the items themselves. One suggestion is that homebuyers "review the configuration settings for remote access, encryption and update cycles and adjust where needed."

NOT JUST A BULB

It isn't always obvious what items within a home might have digital interfaces.

For example, **a house could be equipped with state-of-the-art light bulbs that link to a hub that allows the owner to use a phone app to control the lighting**.

But there's no way for a new homeowner to know that automatically. They might not realize the small box tucked away in a corner allows someone with the right app to control their lights — so they might not know to ask for information about how to disable it or take it over.

"As smart as the light switch is, it's not smart enough to know it's been sold," Henderson said. The issue hasn't really become part of the home-buying process. So far only **15% of clients ask their Realtor about smart home technology in a house they're considering** (2016 National Association of Realtors survey). While today even the most wired home seldom has more than a connected thermostat, lock and perhaps webcam, "at some point soon we'll have 30 to 40 devices in our homes," Curry said, "all of which will be vulnerable if people don't reset them." **If the new owner doesn't get the original documentation, they must find the name and version of each device and look online to find the relevant documentation** so they can know what's necessary to reset the devices.

CONNECTED HOMES COULD POSE THREAT TO NEW OWNERS

SEEKING SIMPLICITY

Realtors want to work with the burgeoning Internet of Things world to streamline and simplify this for customers.

“We would like to help the industry understand how to make it simpler to transfer ownership of these devices,” Curry said.

State laws differ on what is considered a part of the home and therefore what must stay in a house when it is sold.

In most jurisdictions, fixtures stay with the home, while nonfixtures don’t. A fixture is by definition anything that’s affixed to the house. So a Next thermometer that’s installed in the wall is a fixture and stays put, while a webcam on a shelf is not.

To be certain, **ownership of connected devices should be added to the contract** so that “what stays and what goes” is clearly laid out, Curry said.

Another issue is that **many connected home devices require WiFi**, which is **often one of the first things the original homeowner removes when a house is readied to be shown** and sold. So the new owner can’t actually get access to the devices until they move in and install their own WiFi network.

As smartphones became popular, cellphone manufacturers eventually adopted the idea of an easy-to-do “factory reset” because so many users sold or passed on their phones, making it crucial for phone owners to be able to start fresh and protect their privacy.

The connected home device world hasn’t yet gotten to that point, Henderson said.

Curry said his dream would be for each home device to come with a simple user interface and an easy-to-access method for resetting the user login ID and password that also completely wipes the device of all previously stored data.

Unfortunately, he said, “We’re not there yet.”

Online Trust Alliance

THE SMART HOME CHECKLIST

Maximizing security & privacy in your connected home

PRIOR TO OCCUPANCY / CLOSING	
❑	Obtain inventory and documentation of all connected devices including but not limited to manuals, vendor / manufacturer contacts and websites. Examples of connected devices include: ❑ Modems, gateways, hubs, access points ❑ Connected access for garage, locks, gates ❑ External keypads for garage, locks, gates ❑ Thermostats, HVAC, energy systems ❑ Smart lighting systems ❑ Smoke, carbon monoxide, etc. detectors ❑ Sprinkler / irrigation systems ❑ Appliances (TV, refrigerator, washer/dryer, etc.) ❑ Auto controls linked to home systems ❑ Security alarms, video monitoring systems
❑	Review privacy and data sharing policies of all devices and services.
❑	Obtain confirmation from previous occupants and vendors they no longer have administrative or user access.

ALL SMART HOME DEVICES & APPLICATIONS	
❑	Submit change of ownership and contact information to device manufacturers and service providers (email addresses, cell phone numbers, etc.) to ensure you receive security updates and related notifications to maximize your security and privacy.
❑	Review devices' warranty and support policies. Occupants should consider disabling devices or specific features that are no longer supported by a vendor.
❑	Review the configuration settings for remote access, encryption and update cycles and adjust where needed.
❑	Reset privacy and data sharing settings to reflect your preferences. For example – data collection and sharing, camera and microphone settings and other device functions.

MODEMS, GATEWAYS & HUBS	
❑	Review home Internet routers and devices to ensure they support the latest security protocols and standards and disable older insecure protocols.
❑	Update and modify all system passwords and user names upon taking possession of your new home or rental unit. Where possible create unique passwords and usernames for administrative accounts.
❑	Run updates and contact manufacturers to confirm devices are patched with the latest software and firmware.

SECURITY ALARMS, KEYLESS ENTRY, GATE SYSTEMS, ETC.	
❑	Reset access and guest codes for gates and garage door openers.

HOME THERMOSTATS, HVAC SYSTEMS, SMART TVS, LIGHTING & OTHER DEVICES	
❑	Disable connectivity for devices no longer supported by the manufacturer or replace these devices.
❑	Review the privacy practices of the connected devices including data collection and sharing with third parties and reset permissions as appropriate.