CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The Nation / CBSN   Log In   Search

⬤CBSNEWS   Video | US | World | Politics | Entertainment | Health | MoneyWatch | SciTech | Crime | Sports | Photos | More

Trending Videos   CBSN LIVE »

CBS This Morning
Teen trapped in rubble for five days after Nepal e...

CBS This Morning
Over 100 arrested in New York City during Freddie ...

CBS This Morning
Baltimore Mayor: Pain in city about larger issues ...

CBSN
Baltimore protester

By **MICHAEL ROPPOLO AND ELIENE AUGENBRAUN** / CBS NEWS / *September 9, 2014, 5:00 AM*

Keeping "smart homes" safe from hackers

6 Comments / f **19** Shares / 🐦 **73** Tweets / 🔴 Stumble / @ Email   More +

Science fiction has long promised us a future with flying cars, jetpacks, and robotic home appliances that are smart enough to run themselves. Flying cars and jetpacks are still a long way off, but smart home technology is here and becoming more sophisticated every day. What will it take to get these high-tech devices adopted in homes across America -- and to keep them safe and secure?

The Internet of Things

As tech giants enter the race to empower your home -- with Apple's recent launch of HomeKit and Google's acquisitions of Nest Labs and Dropcam -- the so-called "Internet of Things" seems poised to move into the home appliance market in a big way.

Never heard of the Internet of Things, or IoT, as it's commonly known in tech circles? You are not alone. A recent Harris poll for SOASTA, a cloud and mobile testing service, showed that 73 percent of those surveyed were unfamiliar with the term for Internet-enabled devices, sensors and appliances that are envisioned to connect and communicate seamlessly. However, once the concept was explained, a majority said they were excited about the possibility, according to the report.

A true smart home could integrate this technology everywhere from the front door, which you lock and unlock from your phone; to the air conditioning, which turns

⬤CBSN CBS News. Always On.   **Watch Now ›**

Most Popular

01 / Baltimore mom who smacked son during riots: "I don't want him to be a Freddie Gray"
631698 *views*

02 / Baltimore mom: To see my son at riots with rock in hand, "I just lost it"
391499 *views*

03 / Baltimore mom: "I just lost it" seeing son at riots with rock in hand
274085 *views*

04 / Angry mom grabs son off street amid Baltimore riot
75821 *views*

05 / Baltimore mom: "I don't want him to be a Freddie Gray"
61030 *views*

Watch CBSN Live

itself on as you head home from work; to the music system, which knows which tunes you like to sing in the shower and what sets the mood for a Saturday night date; to the light bulbs, which turn off automatically when you go to bed.

For example, Savant Systems has an Apple-based product that knits together smart plugs, appliances, climate control, entertainment, alarm and security systems into one intelligent unit. Their system combines multiple tasks into modes like "waking up," to seamlessly coordinate all the devices you use in the morning, or "away on vacation," with energy-saving features and a lighting patterns to fool a would-be robber.

It can also alert homeowners to the unexpected.

One of Savant's cofounders, Jim Carroll, says his smart home lets him know if his daughters are playing hooky: "When my teenage girls come home from school, if it's outside of the parameters that I'd normally expect them to come home, meaning it's before 3 o'clock Monday through Friday from September to May, I'll get a text saying, 'Shannon's home from school.' I could look at my cameras and see if she came home alone to understand 'Why are you home at one o'clock on a school day?'"

Compatibility and ease of use

Consumers today are constantly "inundated with better, cheaper products," says Virginia Moon, the managing editor of special projects at HGTV, including the HGTV Smart Home 2014 giveaway. "But which investments are going to be reliable and make their life better?"

Do-it-yourself versions of smart home technology will be more approachable to the average homeowner, and easier to install, Moon told CBS News in an email. After all, plugging an IoT device into the wall to control your lamps is much simpler and less expensive than installing a whole new high-tech lighting system.

But that raises issues of compatibility, notes Jeremy Tilley, the director of trade relations and professional experiences at Scripps Network Interactive. With so many IoT devices running mostly on proprietary systems and interfaces, one device is not necessarily compatible with others.

"Consumers...want a single interface that's simple to use, and they just want it to work," Tilley told CBS News in an email.

That's the idea behind Apple's HomeKit, to get everything into the home on one system. A number of startups are also attempting to solve these problems by designing a system around an item that a homeowner will most likely already own: the smartphone. oort, a company based in San Francisco, is in the process of designing a highly customizable system that uses Bluetooth to connect all devices, such as the oort powerstrip and wall socket, to the homeowners' smartphone, regardless of its operating system.

"Even Apple's recent smart home announcement misses the mark as they are focused on only on iOS," oort's founder and CEO, Radek Tadajewski told CBS News in an email. "Families are not all on a single smartphone platform and they don't want to be locked into one, just because it's the only one that runs their house."

The other challenge, he notes, is that with multiple devices and multiple apps, consumers can't create a seamless custom ecosystem, which he says is "the true

Watch CBS News Live

Watch CBS News anytime, anywhere with the new 24/7 digital news network. Stream CBSN live or on demand for FREE on your TV, computer, tablet, or smartphone.

Watch Now

play **VIDEO**

Teen trapped in rubble for five days after Nepal earthquake rescued

Most Shared

Baltimore mom who smacked son during riots: "I don't want him to be a Freddie Gray"

Baltimore mom: "I just lost it" seeing son at riots with rock in hand

promise of a smart home."

"For example, what if you want your blinds to open, your coffee to brew and your thermostat to turn up the heat the moment you wake up," Tadajewski explained. If they're not fully integrated into one system, "you'd have to set each of those individually...which means if you hit snooze on your smartphone alarm, you'd have to go through each app to hit snooze for individual devices or end up with burned coffee."

The effort to standardize the IoT appears to be at a crossroads, with tech giants dividing into three separate camps. A consortium called the AllSeen Alliance, established last December, includes Microsoft, LG and Qualcomm, while a rival group called the Open Interconnect Consortium, announced in July, includes Intel and Samsung. A third, called Thread Group, launched just a week later, also with the backing of Samsung and Google's Nest.

Security concerns

Before consumers start integrating smart devices into their homes en masse, they'll need to feel confident that such technology is secure.

Like any computer that is connected to the Internet, the IoT may never be fully impervious to hackers and viruses. Scott Morrison, senior VP and distinguished engineer at CA Layer 7 Technologies, says that future and current technologists will have to design devices that are resilient on their own, rather than assuming that the home network is already secure.

"Security techniques are always evolving. New attacks appear, and new defenses are concocted in response. No system is ever perfect and no system is completely impervious unless it is completely isolated and unreachable, which is clearly an untenable approach," Morrision told CBS News in an email.

Gary Davis, Chief Consumer Security Evangelist for McAfee, warns that the most vulnerable link in any smart home system is the mobile device that controls it. Now, in addition to being the key to your social media life, your cellphone could be the key to your house and every system in it. He urges consumers to use security features, at very least a pass code and theft recovery program on their phones. According to a survey conducted by Consumer Reports in 2013: "Almost 40 percent in our survey didn't take even minimal security measures, such as using a screen lock, backing up data, or installing an app to locate a missing phone or remotely erase data from it."

"Hackers who could get access to something as simple as your historical thermostat records could predict when you are in [or] out of the house (giving clues when to rob it)," Morrison explains. "We need to take control over the emerging consumer surveillance society before it becomes so entrenched it is too difficult to manage."

Tadajewski recommends that consumers should look for devices that feature 128-bit encryption or higher. Consumers should also enable encryption on all their devices, including communication between devices.

"In other words, users can choose to restrict access to the device and secure data with impenetrable encryption (AES 128-bit)," Tadajewski explained. "To provide some perspective, via brute force methods, it would take hackers with supercomputers longer than the current age of the universe to crack a device's encryption."

Girl who battled cancer is dismissed for missing school

Armenians worldwide mark 1915 genocide of 1.5 million people

Baltimore PD: "Credible" gang threat against cops

80 **PHOTOS**
Earthquake rocks Nepal

Most Discussed

Chaos spreads in Baltimore as police try to restore order
2483 **COMMENTS**

Hillary Clinton: Time to "end the era of mass incarceration"
1805 **COMMENTS**

George W. Bush knocks Obama on foreign policy
1628 **COMMENTS**

National Guardsmen descend on Baltimore after riots, fires paralyze city
1527 **COMMENTS**

Should the Supreme Court decide same-sex marriage?
*1387* **COMMENTS**

Though any WiFi or bluetooth enabled device could have security vulnerabilities, Davis thinks that security monitors need special attention: "If I had to choose a single system that I think would be the most at risk, would probably be the home monitoring system, both your baby monitors as well as home monitors."

Davis says that to McAfee and Intel, "what is top of mind for us is managing your identity." Replacing hackable passwords with biometric technology to confirm the homeowner's identity could help. "If you could sit down at your device and your device knows who you are and what you have the means to go do ... that is going to go a long ways toward enabling the Internet of Things."

6 Comments / f **19** Shares / 🐦 **73** Tweets / ⓢ Stumble / @ Email   More +

Recommended

Missing Maryland woman Nicole Marie Torain found dead in Baltimore trash…

Suspect on house arrest uses cat to trick police

Watch this language video (it's mind-blowing)
Pimsleur Approach   Sponsored

4 Billionaires Say: Big Change Coming in U.S.A
Stansberry Research   Sponsored

Learn more   Powered by YAHOO! for you

Featured in SciTech

Popular

25 years of breathtaking Hubble Telescope images

Since it was launched in 1990, the Hubble Space Telescope has sent us breathtaking images back from the deepest corners of space

11 species threatened by

New Android App

CBS News App for Android®

For your Android phone and tablet, download the FREE redesigned app, featuring CBSN, live 24/7 news.

Download

climate change

As the world warms, many plants and
animals are struggling to adapt

Los Angeles Police
Department looking for graffiti
artist who tagged cop's horse

Gay businessman: Hosting
dinner for Ted Cruz a "terrible
mistake"

"Saturday Night Live" star
Cecily Strong's best political
zingers at nerd prom

Catching a wave with Helen
Hunt

Baltimore mom Toya
Graham: "I just lost it" seeing
son at riots with rock in hand

Good news for older workers
seeking new careers

6 Comments

6 Comments / *12 people listening*   **SIGN IN**

| | **+ FOLLOW** | | Share ▾ | **POST COMMENT AS...** |

COMMENTING FAQS / GUIDELINES

NEWEST | OLDEST | TOP COMMENTS

BC_PROGRAMMING *September 13, 2014 10:10PM*

The only thing The Matrix got wrong was what was in control of network - instead of
being controlled by robots most people are slaves to their damned iCrap.

👍 **LIKE** / ↩ **REPLY**

COLT4542 *September 9, 2014 4:4PM*

How about a private home network NOT connected to the internet and controlled by a

device similar to a pager (NOT a phone) that is not connected to anything but the private network. Allows complete control when you are at home. Anything that needs to be done while you are away could be programmed into the network/non-connected computer.

Or, just flip the dang switch on/off yourself!

👍 **LIKE** / ↩ **REPLY**

STEFF CLARKE *September 9, 2014 1:1PM*

Today, people use their smartphones for everything from storing passwords to managing finances, even to controlling their home security systems.
http://goo.gl/tGs42e

👍 **1 LIKE** / ↩ **REPLY**

PAYASYOUGO *September 9, 2014 11:11AM*

My flip phone has never been hacked.

👍 **1 LIKE** / ↩ **REPLY**

ROBERT_HOLT *September 9, 2014 9:9AM*

So lets see, thanks to modern technology, all these things in my home can happen automatically or I can do them remotely because I'm incapable of doing them manually before I leave home or after I come home. The problem is, some hacker can do the same thing with my home and this "security" system that is supposed to protect me and my home, has left me wide open and a sitting duck. No thanks. I think I'll just use my brain more and rely on all these machines less. We didn't have these problems twenty years ago.

👍 **1 LIKE** / ↩ **REPLY**

PARISDAKAR *September 9, 2014 8:8AM*

Jeez, this smartphone crap is out of control.

👍 **1 LIKE** / ↩ **REPLY**

CBSNews.com
Site Map
Help
Contact Us
CBS Bios
Careers
Internships
Development Programs

CBS Interactive
Privacy Policy
Terms of Use
Mobile User Agreement
About CBS
Advertise
Closed Captioning

Follow Us
Facebook
Twitter
RSS
Email Newsletters
YouTube
CBS Radio News
CBS Local

◎CBSNEWS
Copyright © 2015 CBS Interactive Inc.
All rights reserved.

Search... 🔍