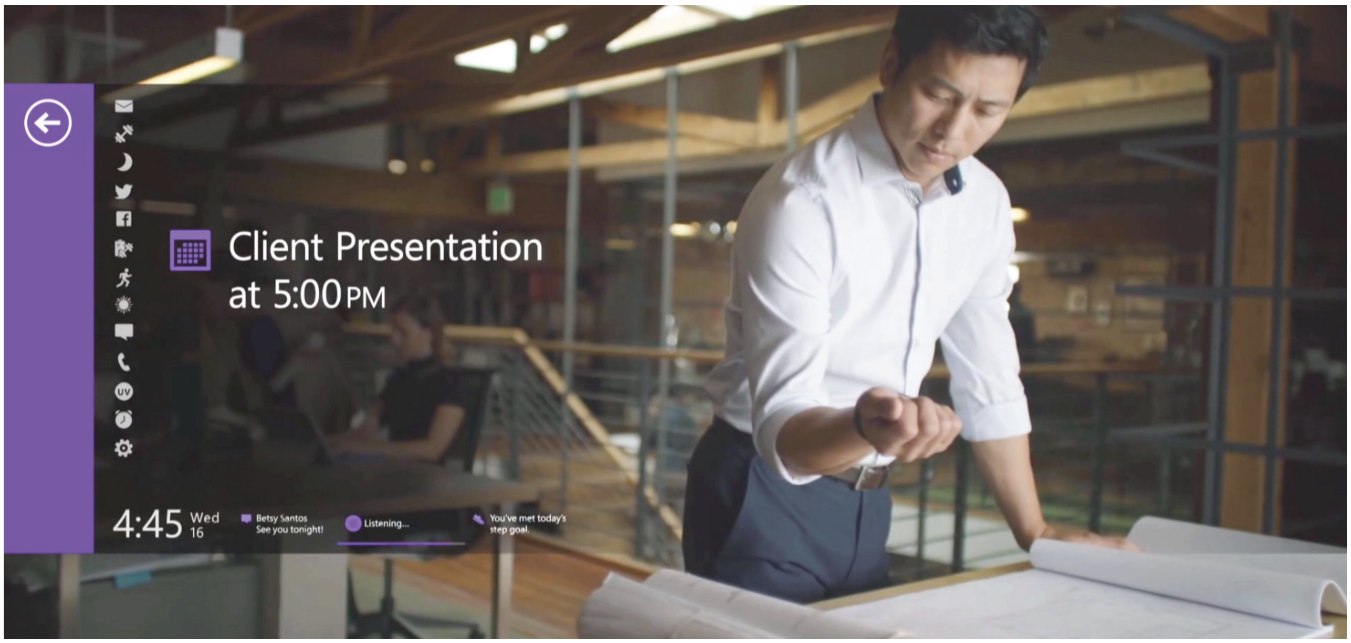


CAN WE TRUST THE INTERNET OF THINGS TO PROTECT US?

Within the next decade the internet could connect as many as 200 billion things—and not just machines such as cars or household appliances, but anything that you can fit a chip or sensor into—including humans. These devices, collectively known as the Internet of Things, should make life simpler, even healthier, but can we trust them to look after us?

It's 6am on Monday 1 October 2025. The device on your wrist has sensed that you're waking up so it sends a message to your coffee machine to start brewing. You delay the coffee and go for a run instead. While you're pounding the pavement, the sensors in your earphones detect an irregular heartbeat. The device sends an ECG readout to a cardiologist. He sees that the arrhythmias are just harmless ectopic beats and decides to take no further action.

Back home, you have your well-earned coffee and put the empty cup in the dishwasher. The dishwasher is full, so it starts running. A sensor detects that the appliance is due for a service. It makes the appointment with an engineer and books a date in your diary, which you later confirm.

A couple of decades ago, dishwashers were one of the biggest causes of house-fires, but not anymore. The internet of things (IoT)—devices connected to each other over the internet—has made the world infinitely safer.

From self-driving cars to smart pills that measure our health from the inside, the internet in 2025 has become a custodian of our health and safety.

But have we been wise to give the reigns of responsibility—that we once took hold of ourselves for things like driving or administering medicine—to a device?

JUST THE BEGINNING

This scenario may sound far-fetched, but the seeds of these developments have already been sown.

South Korean electronics company, LG, has developed earphones that double as a heart-rate monitor, and Israeli telemedicine firm, Aerotel Medical Systems, is one of a number of companies that provide technology that can remotely transmit real-time ECG results to medical centres for assessment.

Swiss drugmaker Novartis working with digital medicine company, Proteus Digital Health, to develop tablets containing embedded microchips that can tell if patients have taken their medication. There are also smart pills on the market that contain inbuilt cameras and various sensors to measure pH levels, blood pressure, and temperatures in the stomach.

And, although self-driving cars aren't yet publically available, most automobile makers are extensively testing their vehicles both on public roads and in fenced areas. Elon Musk, founder and CEO of Tesla, wants to make autonomous vehicles the standard by 2020, the same year Google expects that its own self-driving cars will be ready.

Over the past six years, Google's vehicles have been involved in "11 minor accidents (light damage, no injuries) during 1.7 million miles of driving", says the programme's director Chris Urmson, and "not once was the self-driving car the cause of the accident."

There are thousands more IoT devices, from crash helmets to implantable wireless microchips, that are designed, and are being designed, to make us safer. But are we naïve to assume that a device can be entrusted to watch out for us—better than ourselves, or someone else, could?

For Olivier Ribet, vice president of Dassault Systèmes High Tech Industry, the key question is: "How do you determine when you allow IoT devices to make decisions on your behalf and when you want to make the decision for yourself?"

"So far, all of these objects have explicitly asked you 'do you want me to do that for you?' Now, more and more, you start to see people saying we shouldn't even question devices taking decisions on our behalf," he adds.

If that's the case, we have to be certain that we trust the devices. This is where testing becomes paramount. Using Dassault Systèmes **3D**EXPERIENCE® platform, designers can simulate anything in a virtual environment, from a self-driving car on a motorway to smart pill in a body, in order to understand every possible and unprecedented scenario before we use the products in real life.

But even if an IoT device does prove to be failsafe, can we really be sure that there are no other risks?

THE DARK SIDE

A healthier, safer life might sound great but, as we know, computers can be hacked. When criminals manage to breach anti-virus software, they can wreak havoc with our computers and mobile devices—getting into bank accounts, stealing information and bribing people. Nobody intentionally dies, though. So what if, in the future, hackers could get into the drug delivery system embedded in your skin and give you a fatal dose of medicine? Or what if they took control of the steering wheel of your car as you sped down the motorway? What if they changed the radiation exposure limit on a CT scanner?

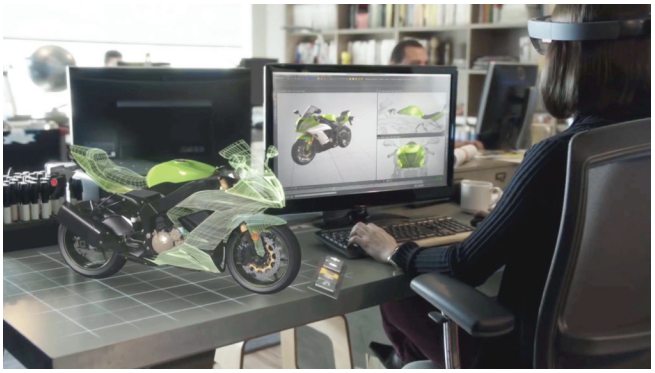
Pacemakers, computerised insulin pumps, defibrillators, baby monitors, webcams, fitness trackers and smart toilets have all already been hacked. Most of these have been public demonstrations of hackers' prowess rather than any real mischief. But it's proof that it can be done.

A study by HP found that three-quarters of IoT devices are vulnerable to being hacked. And when it comes to home IoT systems, where lots of devices are talking to each other and making decisions about how to manage the house, all you need is one weak link in the chain and the whole system can be compromised.

OVERBLOWN

"In theory, IoT devices are quite attackable because the security on them is often not very good," says Kris Flautner, general manager for IoT business at security firm, ARM. "But, at the same time, you also have to know a lot about those devices and how they're configured. To me, I'm not actually sure if the [hacking] threat goes up or down."

Rob Ragan, a senior security associate at Bishop Fox, a security consulting firm, agrees that the threat of hackers getting into IoT systems is overblown. "People have this fear that if they have an internet-enabled home security system, there's going to be some gang of cat burglar cyber-criminals who are going to sweep through their neighbourhood, disable everyone's security alarms and steal all their things," he says. "I don't think that's a real scenario because it's not happening very often now even though many homes are protected by high-tech devices."



As with all new technology, there's always a risk. But Ragan says he welcomes these devices even though, as a security consultant, he intimately knows their dangers and risks.

Ultimately, IoT's ability to protect us may lie with those that want to make the most of the devices. "As fast as we progress in technology, we need to make sure people progress alongside it, operating and interacting with it, and staying in control of it," says Ribet.

No doubt it will soon become easier to sleep soundly knowing that the internet is watching over us. Or we're watching over it.

NOTE: This article was first published as an Advertisement Feature on bbc.com and was created by the BBC Advertising Commercial Production team in partnership with Dassault Systèmes.