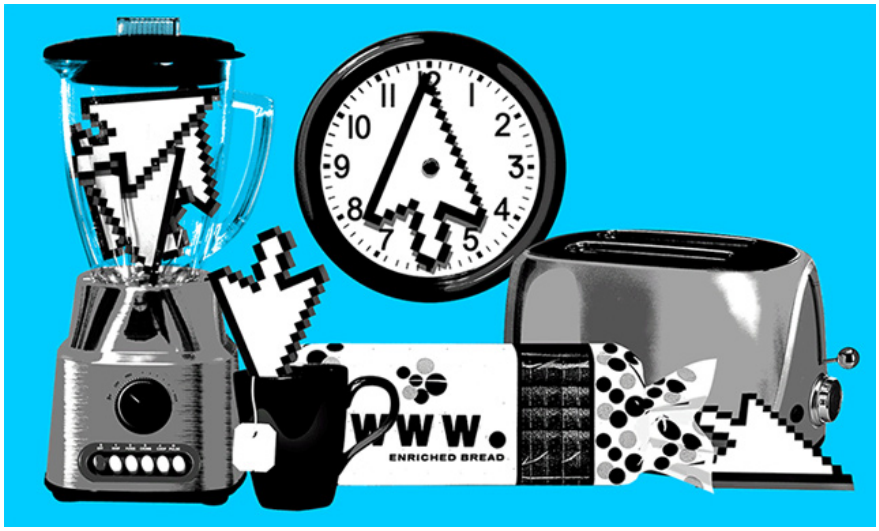
In the future, everything will become more scary than you think

More than 40 years ago, Bill Gates and Paul Allen founded Microsoft with the vision of putting personal computers on every desk. Nobody really believes them, many people even try to stop their crazy idea. And before anyone realized it, Microsoft realized its ambition. Everyone owns a Windows computer, and the governments of the country are eager to try to contain Microsoft's monopoly.

More than 40 years ago, Bill Gates and Paul Allen founded Microsoft with the vision of putting personal computers on every desk. Nobody really believes them, many people even try to stop their crazy idea. And before anyone realized it, Microsoft realized its ambition. Everyone owns a Windows computer, and the governments of the country are eager to try to contain Microsoft's monopoly.

This story is always repeated throughout the history of the technology industry. The daring founders have put their vision on something out of reach - like when Mark Zuckerberg wants to connect everyone - and the absurdity of their plan has made them escape from "tuberculosis." soi "of the community. By the time we keep up with their influence, that's when we can't do anything anymore.

And that is continuing to repeat. In recent years, the biggest forces of digital technology have placed their vision on a new goal for digital conquest. They promise fabulous conveniences for our health and happiness. But the problem is, if only one security hole is exposed, like the recent Facebook case, the world will be reversed, and people frantically try to fix it. "Loss of the new cow shed lo".

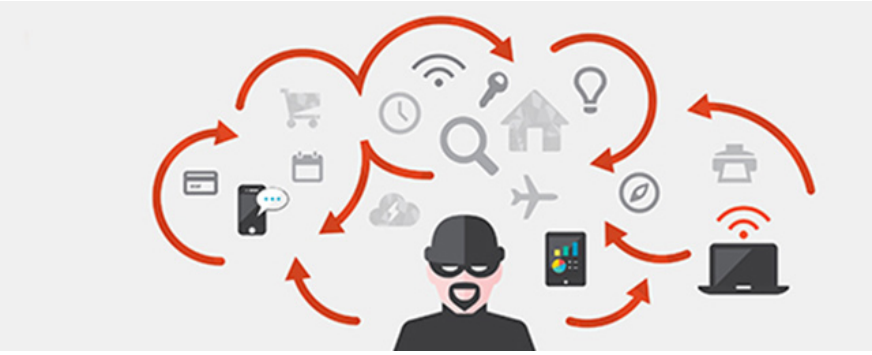


What is the industry's new goal? No longer is the computer on every desk or connecting people together but it will be something greater: a computer inside everything, connecting with people.

Cars, door locks, contact lenses, clothes, toasters, refrigerators, industrial robots, fish tanks, sex toys, light bulbs, toothbrushes and motorcycle helmets - items This daily is on the menu to become "smart". Hundreds of small start-ups are taking part in this trend - known by marketing terms as "universal internet" - but like everything else in the technology world, this movement is led by giants, including Amazon, Apple and Samsung.

For example, Amazon last month launched a microwave that integrates Alexa, its virtual assistant. Amazon will sell microwave ovens for $ 60, but it also sells chips - the core that makes devices smart for other manufacturers, making Alexa's connectivity reach far to many devices. More versatile appliances such as fans, toasters and coffee makers. And this week, both Facebook and Google announced their home-based "communication ports" that allow you to watch videos and perform other digital tricks by voice.

You can consider many things in this initiative to be foolish and certainly fail. But everything big in technology at the beginning looks silly, and statistics show that the internet of things is growing rapidly. Now is not the time to think whether IoT is successful - but to see how long it will take to take over the world.



Bruce Schneier, a security consultant, author of "Click Here to Kill Everybody" about IoT's threat to society shares: "I don't want to be pessimistic, but the current situation is hard not to. so".

Schneier argues that the economic and technical interests of the internet industry are incompatible with social security and privacy in general. Placing a computer in everything makes the world a threat to computer security. Errors and security holes discovered in the past few weeks at Facebook and Google show just how difficult digital security is, even for the largest technology companies. In a robotized world, data theft will not only affect your data but can also jeopardize your property, your life and even national security.

Schneier said that only government intervention could save us from the emerging disasters. He called for the re-emergence of digital security management the same way the US federal government changed its national security apparatus after the September 11, 2001 attack. Among other ideas, he outlines the need for a new federal agency - a National Cyber ??Office, to research, advise and coordinate anaphylaxis against the threats posed by the internet. .

"I think no industry in the last 100 years has improved its safety and security without relying on government coercion," he wrote. But he admits that government intervention does not seem to be the best. "In a society where the government is unable to do anything, I don't see any control of the development trend of businesses," he said.

These trends are now showing up. It was difficult to add internet connectivity to home appliances, but over the past few years the cost and complexity of this has plummeted. Today, unique mini computers like Arduino can be used to make every family object "smart". Systems such as Amazon are promising to accelerate the

development of Internet devices beyond that.

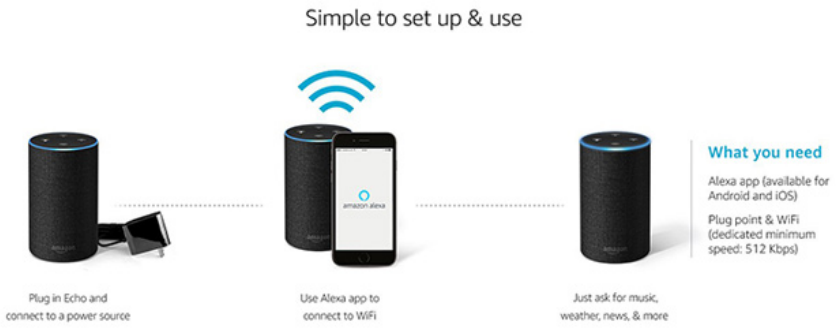
At a press event last month, an Amazon engineer showed that a home fan manufacturer could create a "smart" fan using Amazon's chip, called the Alexa Connect Kit. how. The toolkit that Amazon is testing with some manufacturers is easy to integrate, just plug in the fan controller during assembly. Manufacturers also have to write a few lines of code - in the fan manufacturer's example, Amazon engineers only need to write half the code page that the machine can run.

Just simple as that. The fan's digital bits (including security and cloud storage) are handled by Amazon. If you buy it from Amazon, the fan will automatically connect to your home network and start complying with the voice commands you tell Alexa. Just plug in the power.

This system is a reference to Schneier's larger argument, that the cost of adding computers to objects becomes so low that manufacturers have no reason not to connect all kinds of devices. suffer from internet.

Sometimes, intelligence will lead to convenience - you can shout at the microwave to heat up your lunch no matter where you stand in the room. Sometimes it will lead to a revenue opportunity for other products - Amazon's microwave oven will add popcorn to you when it is near (you will have to buy more corn seeds). Sometimes, intelligence is used for monitoring and marketing, as smart TV will track what you watch to allocate ads.

Even if the benefits are small, they will still create a certain market logic; At some point not long from now, devices that are not connected to the Internet will be rarer than devices with an Internet connection.



However, the problem is that business models for these devices often do not allow ongoing security maintenance that we are accustomed to using on more traditional computer devices. Apple has an incentive to continue writing security updates to keep your iPhone safe, because iPhone products are very expensive, and Apple's brand depends on keeping you safe from a crisis. number.

But low-profit home appliance manufacturers will have less expertise and motivation to think about security. That's why everything in the internet has so far been synonymous with the security crisis - why the FBI had to warn parents last year about the dangers of "smart toys", and why Dan Coats, US national intelligence director, has identified smart devices as a growing threat to national security.

An Amazon representative once said the company has built security features into the core of their smart technologies. Connect Kit allows Amazon to maintain the digital security of a smart device - and Amazon seems to have much better security than home appliance manufacturers. As part of its cloud computing business, Amazon also provides a service for manufacturing companies to check the security of their internet services.

According to Schneier, government intervention is not a "panacea", but a speed-reducing line, a way for us to keep up with technological advances. Government regulation and oversight slows innovation - that's one reason experts don't like it. But when global dangers come, slowing down one step is not a bad idea.

Connecting things can bring great benefits to society. But the threat may spread. Why not slow down before entering the uncertain future?

See more:

1. Things to know about a computer engineer
2. Reduce fatigue when sitting on a computer with a few simple movements
3. Things to know about a computer system administrator

According to VnReview