

### Home, Hacked Home

Taken from: The Economist Magazine

12th July, 2014

http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home

### Prevention is better than cure

Taken from: The Economist Magazine

12th July, 2014

http://www.economist.com/news/special-report/21606424-more-vigilance-and-better-defences-can-make-cyberspace-lot-safer-prevention-better

By: Maria José Verdugo Vilches

Class: ED1106C Section 01

### *Home, hacked home*

# The perils of connected devices

Jul 12th 2014 | [From the print edition](http://www.economist.com/printedition/2014-07-12)



ONE NIGHT IN April a couple in Ohio was woken by the sound of a man shouting, “Wake up, baby!” When the husband went to investigate, he found the noise was coming from a web-connected camera they had set up to monitor their young daughter while she slept. As he entered her bedroom, the camera rotated to face him and a string of obscenities poured forth.

**Complex Sentence 1**

When the husband went to investigate, he found the noise was coming from a web-connected camera they had set up to monitor their young daughter while she slept

The webcam was made by a company called Foscam, and last year a family in Houston had a similar experience with one of their products. After that episode, Foscam urged users to upgrade the software on their devices and to make sure they had changed the factory-issued password. The couple in Ohio had not done so. The problem arose even though Foscam had taken all the right steps in response to the initial breach, which shows how hard it is to protect devices hooked up to the internet.

**Compound Sentence 1**

The webcam was made by a company called Foscam, and last year a family in Houston had a similar experience with one of their products

There will soon be a great many more of them. Cisco, a tech company, reckons that by the end of this decade there could be some 50 billion things with web connections (see chart 5). Among them will be lots of consumer gear, from cameras to cars, fridges and televisions.

**Smart or foolish?**

This new network is already turning out to be very useful. Smart cars are able to read e-mails and text messages to drivers on the move; smart fridges carefully manage the energy they use; smart medical devices allow doctors to monitor patients from afar; and smart screens in the home display all kinds of useful information. Entire cities in South Korea are already rushing to link their infrastructure to the web to make it more efficient and improve services.

**Simple Sentence 1**

This new network is already turning out to be very useful.

But security experts are sounding the alarm. “There is a big difference between the internet of things and other security issues,” says Joshua Corman of I Am The Cavalry, a group of security specialists trying to promote greater awareness of emerging risks to public safety. “If my PC is hit by a cyber-attack, it is a nuisance; if my car is attacked, it could kill me.”

**Complex Sentence 2**

“If my PC is hit by a cyber-attack, it is a nuisance; if my car is attacked, it could kill me.”

This may smack of scaremongering, but researchers have already demonstrated that some vehicles are vulnerable to cyber-attacks. Modern cars are essentially a collection of computers on wheels, packed with many microcontrollers that govern their engines, brakes and so forth. Researchers such as Chris Valasek and Mathew Solnik have shown that it is possible to hack into these systems and take over a vehicle.

**Compound Sentence 2**

This may smack of scaremongering, but researchers have already demonstrated that some vehicles are vulnerable to cyber-attacks

Their experiments, which include steering wheels suddenly being wrenched to one side and engines being switched off without warning, have caught the attention of carmakers. The techniques used to hack the vehicles’ controls are sophisticated, and many require physical access to the engine, so for the moment this is unlikely to happen to your car. But technology moves fast: at an event in Singapore earlier this year two researchers showed off a car-hacking tool the size of a smartphone that cost less than $25 to build.

Some medical devices, including several types of insulin pump, have also been hacked in public demonstrations. Jay Radcliffe, a security researcher who happens to be diabetic, made headlines a few years ago when he discovered that his computerised insulin pump could be attacked by remotely entering the wireless-communications system that controlled it. A malicious hacker could have changed the amount of insulin being administered. In a recent blog post, Mr Radcliffe gave warning that emerging medical technology is often ill-equipped to deal with threats arising in an interconnected world.

Other researchers agree. “There are just super simple flaws in some medical devices,” says Billy Rios of Qualys, a cyber-security firm. Last year he and a colleague found “back doors” into various bits of medical equipment. These are passwords used by technicians from firms that sell the devices to update the software that runs them. A hacker with a back door could use it to, say, adjust an X-ray machine so that it administers a far higher dosage than its display shows. Mr Rios took his findings to regulators and worked with them and with the companies involved to fix the flaws.

**Simple Sentence 2**

Other researchers agree

It all sounds rather worrying, but so far there has been no known case of a cyber-attack in which a car has been forced off the road or a medical device misappropriated. Mr Rios accepts that some people think his research is designed to drum up sales for the cyber-security industry, but he insists that the risks are real.

Many items, including mundane things like light bulbs and door locks, are being hooked up to the internet by putting tiny computers into them and adding wireless connectivity. The problem is that these computers do not have enough processing power to handle antivirus and other defences found on a PC. The margins on them are wafer-thin, so manufacturers have little scope for spending on security. And the systems are being produced in vast quantities, so hackers finding a flaw in one will be able to get into many others too.

This is already happening with some home wireless routers. Earlier this year Team Cymru, an American cyber-security firm, found a network of 300,000 compromised routers in various countries, including America, India, Italy and Vietnam. In 2012 crooks in Brazil took control of 4.5m routers, using the stolen information to plunder a large number of bank accounts.

**Simple Sentence 3**

This is already happening with some home wireless routers.

**Watch that fridge**

A lot more devices with little computers inside them will end up in people’s homes, often connected to one another via home-automation systems. That will make them tempting targets for cyber-attackers. In January Proofpoint, a security firm, claimed it had found evidence that a group of compromised devices, including home routers, televisions and a refrigerator, had been commandeered by hackers and were being used to pump out spam. That is annoying enough, but what if a tech-savvy arsonist were to find a way of, say, taking control of home boilers and turn them up so much that they burst into flames? Mr Rios has already found tens of thousands of corporate heating, air-conditioning and ventilation systems online, many with vulnerabilities in their software that a hacker could exploit.

Some companies are now trying to build security into their products from the start. Broadcom, a chipmaker, recently unveiled a microchip specially designed for web-connected devices that has encryption capabilities baked into it, and Cisco has launched a competition offering prizes for the best ideas for securing the internet of things. But many firms plunging into this market are small startups which may not have much experience of cyber-security.

Mr Corman worries that it may take a catastrophic event to get makers to focus on the need for better security in connected devices. But optimists believe that pressure from customers will be enough to force their hand.

**Parts of speech: summary**

**Content Words**

|  |  |  |  |
| --- | --- | --- | --- |
| **NOUNS** | **ADJECTIVES** | **ADVERBS** | **VERBS** |
| Couple | Stolen | Already | Promote |
| Information | Best | Now | Believe |

**Function Words**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRONOUNS** | **DETERMINERS** | **PREPOSITIONS** | **CONJUNCTIONS** |
| Them | Many |  With | So |
| One Another | Their | Among | And |

***Prevention is better than cure***

**More vigilance and better defences can make cyberspace a lot safer.**

Jul 12th 2014 | From the print edition

CYBERSPACE WILL NEVER be completely secure. The threats posed by what Sir David Omand, an academic and former head of Britain’s GCHQ intelligence agency, calls “the cesspit of modernity”—online crime, espionage, sabotage and subversion—are not going to disappear. Nor is the temptation for governments to treat the internet as a new combat zone, alongside land, sea, air and space.

In 1996 John Perry Barlow, a cyber-libertarian, issued a “Declaration of the Independence of Cyberspace” addressed to governments, insisting: “You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear.” He turned out to be wrong. Governments have shown in a variety of ways—from the theft of industrial secrets by Chinese spies to the mass surveillance conducted by Western ones—that they are determined to make cyberspace their own.

Political leaders are fond of saying that they want their citizens to benefit from the huge opportunities that a secure and reliable internet can offer, and that they are determined to protect them from crime and terrorism online. Yet they do not hesitate to use the web for their own purposes, be it by exploiting vulnerabilities in software or launching cyber-weapons such as Stuxnet, without worrying too much about the collateral damage done to companies and individuals. Some of the trends pinpointed in this special report, including the rise of organised crime on the internet and the imminent arrival of the internet of things, will only increase concerns about a widening security gap.

**A plain man’s guide**

So what can be done? The first thing is to change the tone of the debate about cyber-security, which is typically peppered with military metaphors. These tend to suggest that companies and individuals are powerless to help themselves, giving governments latitude to infringe their citizens’ privacy. “The internet is the most transformative innovation since Gutenberg and the printing press,” says Jason Healey of the Atlantic Council, an American think-tank. “Yet we’re treating it as a war zone.”

Bruce Schneier, a security expert, has suggested that crime-fighting is a better analogy than warfare. This is a useful idea. Police are needed to go after criminals, but people can help prevent crimes in the first place by taking sensible precautions. And although extraordinary powers of investigation and arrest are sometimes needed to apprehend wrongdoers, they are subject to robust legal protections for citizens.

Applied to cyberspace, this means that, far from being powerless against hackers, companies can do a lot to help themselves. Simply ensuring that only approved programs can run on their systems, regularly patching all software, educating employees about cyber-risks and constantly monitoring networks would help keep most intruders out. Yet too many companies fail to do these things, or do them consistently.

Tackling cybercrime often requires international co-operation. In recent years this has been getting better, partly thanks to agreements such as the Council of Europe’s Convention on Cybercrime, whose members assist each other in international investigations. More resources for crime-fighting outfits, including teams on secondment from the private sector, would clear out more crooks.

That still leaves the job of dealing with the most sophisticated hackers, whose motives often have nothing to do with money. Getting broader agreement on norms of behaviour in cyberspace is crucial, but it will not be easy. Forging a consensus on what bits of critical infrastructure should be off-limits to a cyber-attack would be an excellent start.

Making sure that fewer bugs crop up in software in the first place would also be helpful, particularly as the internet of things is about to take off and opportunities for breaches will multiply manifold. The best method would be for companies to come up with robust proposals of their own for securing the new connected devices. In March a group of firms including Cisco, IBM and GE set up the Industrial Internet Consortium, which among other things will look at innovative approaches to security in web-connected industrial gear. Something similar is needed in the consumer field.

**Simple Sentence 4**

Something similar is needed in the consumer field.

The internet has turned out to be one of the biggest forces for progress in the history of mankind. Having started life as a gathering place for a small bunch of geeks and academics in the early 1970s, it is now at the heart of the global economy. Mr Gibson’s “consensual hallucination” has become a worldwide success story. It must be kept in good working order.

**Simple Sentence 5**

It must be kept in good working order.