SECURING THE CONNECTED HOME

Smart but vulnerable IoT devices present an opportunity for home broadband providers

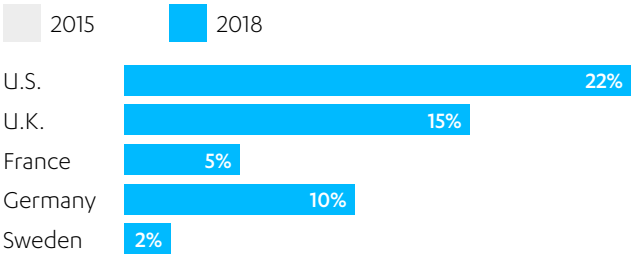
F-Secure

Internet-connected "things" are lacking in basic security protections, putting consumers at risk. Home broadband providers are in a unique position to protect their customers' connected devices through value-added security solutions.

As the Internet of Things continues its advancement, our world is becoming smarter and smarter. Consumer televisions and security cameras are already connected to the internet. Adoption of connected thermostats, lights, security systems and voice assistants is growing fast, particularly in North America. Soon homes will have connected washing machines and toasters as well.

According to a 2018 PwC survey, ownership of smart devices in UK homes more than doubled in the previous two years. And according to a study from Parks Associates, more than 50% of US households with broadband plan to buy a smart home device in the coming year. A survey from Metova revealed that 74% of respondents think connected home devices are the wave of the future.

Digital assistant, 12% adoption in all 5 countries



No one is more aware of this trend than Mikko Hyppönen, Chief Research Officer at leading cyber security provider F-Secure. Hyppönen has been fighting computer viruses and defending cyber space since his tenure at F-Secure began in 1991, before most people even knew about the internet. The advent of connected "things" has opened up a new frontier of cyberspace in need of guardians like him to protect it.

> "If it's smart, it's vulnerable."
>
> Mikko Hyppönen

"Everything is becoming a computer," says Hyppönen. This matters because, as he says in an apt aphorism that he's self-coined as Hyppönen's Law, "If it's smart, it's vulnerable."

"So here's a smart phone—vulnerable phone," Hyppönen says. "Here's a smart watch—vulnerable watch. Smart car, smart city, smart grid...You get my point."
The essence of Hyppönen's Law is that anything that can be programmed can also be hacked. When we add connectivity to the appliances and gadgets around us, we open ourselves and our homes up to potential compromise by malicious actors from afar. Almost all these connected devices use the home gateway Wi-Fi password, yet all are lacking in basic security protections.

Home broadband providers are in the unique position of managing these gateways. Given the relationship of trust already established with customers, broadband providers are well positioned to help consumers deal with the growing complexities of the connected world. By partnering with a cyber security provider like F-Secure, home broadband providers can help consumers keep their living spaces secure, even as homes become smarter.

CONNECTED AND COMPROMISED

That the IoT has security challenges is being acknowledged by no less than the FBI and Interpol. Both agencies have issued statements in the past year warning about the dangers of connected things.

"Cyber actors actively search for and compromise vulnerable Internet of Things devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and computer network exploitation," the FBI warned. "Cyber actors typically compromise devices with weak authentication, unpatched firmware or other software vulnerabilities, or employ brute force attacks on devices with default usernames and passwords."

The warning echoes a similar finding in a 2018 F-Secure report, Pinning Down the IoT: "In its current form the Internet of Things represents a considerable threat to consumers, due to inadequate regulations regarding its security and use."

According to the FBI, cyber criminals are leveraging compromised IoT devices for various nefarious activities, such as sending spam emails; generating click fraud activities; buying, selling and trading illegal images and goods; and conducting credential stuffing attacks, which involves testing stolen passwords on website login pages using an automated script.

In the wider context, they can also be used in distributed denial of service (DDoS) attacks on organizations to shut down servers or services. One of the most powerful DDoS attacks ever seen took place in October 2016 when a botnet targeted the systems of a major DNS provider, rendering the internet unavailable to users in many areas of Europe and North America. The ensuing investigation revealed that the botnet had been made up not of conventional computers, but of connected gadgets like IP cameras and baby monitors. The devices were infected with a special type of malware that targets IoT devices, exploiting devices on which the factory default login credentials had not been changed.

Closer to home, what impact can a compromised IoT device have on the average consumer? Device owners may notice spikes in internet usage and increased monthly bills or slow performance of a device or connection. There can potentially be even deeper, more personal effects. In recent years, stories have emerged of vulnerable webcams leaving consumers open to peeping tom hackers and vulnerabilities in critical technology like implantable cardiac devices and baby heart monitors.

INHERENTLY INSECURE?

Compared with conventional computers, laptops and smartphones, connected "things" present their own unique challenges to security, an issue that begins with the very design of a product. Real world product companies, although they manufacture useful home appliances, toys and everything else you can touch and feel, often know little about information security. It's no surprise that in their smart products, security is not given the priority it deserves.

These companies focus on how desirable and useful their product is, not on how secure it is. They worry about whether their product is easy to use, not about whether it can be remotely hacked. And to keep costs down and move products out the door, they often sell products built with chips that use outdated software. Such devices may have grave security flaws from the beginning.

Even if these companies were concerned about security, the miniature size of many IoT devices creates challenges. Limited size and processing power narrow the options for security measures. A given computer, smartphone or tablet can have third party security software installed to protect it; this is not the case with connected things. There is no way to install security onto a smart surveillance camera or a smart fitness tracker.

Limited size and processing power narrow the options for security measures.

Compounding the problem is the difficulty with updating vulnerable software in IoT devices. Many smaller devices are low cost, and if a vulnerability is discovered on such a device it may be difficult to update the software and then to let customers know about a fix. Even if customers were notified, they would have to have the know-how to download and install the patch.

HOW SMART IS SMART?

For consumers, there are already "smart" hairbrushes, luggage, even condoms. Almost half the homes in America have a smart TV. New F-Secure research confirms that the only thing preventing even faster adoption of smart devices that connect to the internet is the privacy and security concerns of the people who are most excited about this technology. While 89% of early tech adopters in the UK said they are excited about IoT, 66% also reported being concerned about malware and hacking.

For businesses, the move to connecting almost everything has been happening since before this decade began. To get a sense of how far along we are in the computerization of the world, Hyppönen advises visiting a factory, where companies rely on industrial control systems for billions if not trillions of dollars of commerce.

"When everything is becoming a computer, companies get hacked in surprising ways," he says. For an example, he points to one of the largest credit card breaches in history—the 2014 hack of US department store retailer Target, which exposed the data of up to 70 million customers.

"In this case, the actual credit numbers were lost as customers were paying at the cashier desks...The shop's own credit card terminals were stealing the credit card numbers." The attackers had found a way in through the computers that controlled the ventilation systems, and had worked their way over to infiltrating the POS systems.

WHEN EVERYTHING IS CONNECTED, EVERYTHING MUST BE PROTECTED

Anything that can be programmed can be hacked, and like the Target case, it may be hacked to get to something else that's far more interesting than just the ventilation system.

"They are not hacking your washing machine or your fridges to gain access to your washing machine or to your fridge," Hyppönen told Nasdaq's Tomorrow's Capital. "They are hacking those devices to gain access to your home network...The weakest link in the home network is an IoT device, and we have seen this multiple times. Company networks get breached because of ventilation-automation systems which have nothing to do with your laptops or your servers, but they are computers because everything is becoming a computer." In the same way, home networks can get compromised through the most innocuous smart device...smart, remember, meaning vulnerable.

The weakest link in the home network is an IoT device, and we have seen this multiple times.

There's no easy solution for securing the Internet of Things. In order to experience all the benefits of the IoT without scary scenarios of cyber criminals accessing our data and controlling us via our Things, we have to begin by coming to grips with what it's going to be like to live in a future governed by Hyppönen's Law.

HOME WI-FI SECURITY

The good news is the problem is recognized, and bold new solutions are available – and it's up to home broadband providers to bring these solutions to their customers. According to an F-Secure survey*, 60% of consumers said they would purchase their security and privacy services from their internet service provider. Partnering with a cyber security partner to offer value-added IoT security solutions on top of broadband services is one way a broadband provider can secure their customers' connected lives, and in doing so, enhance their own brand loyalty and trust.

Home Wi-Fi security from F-Secure gives broadband customers protection for every internet-connected device in their home – from smart TVs to gaming consoles, thermostats, wireless printers and baby monitors, to traditional computers and mobile devices. IoT devices are protected against malicious websites and other online threats with breakthrough SENSE technology from F-Secure. Consumers also receive notifications if their devices begin to exhibit odd behaviour. Home broadband providers can enhance their proposition and increase their addressable market with leading-edge, worry-free security for consumers and small businesses.

Everything is becoming a computer, so everything is vulnerable. This is already true for our businesses and it's becoming truer and truer for our homes. Our personal sanctuaries where we live, work, and play need to be shielded from the dark underbelly of the internet. Home broadband providers are already providing the bandwidth that powers our connected home and all its devices; it just makes sense to also be part of the solution for protecting these devices, their owners, and the connected home.

ABOUT F-SECURE

Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of office, homes, and millions of people. F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure's AI-driven solutions also help to protect the connected devices and homes of your customers. The unique combination of technology and world-class Business Services supporting the entire customer lifecycle is what makes F-Secure an excellent fit for the service provider channel. F-Secure's products are sold globally by more than 200 service providers and thousands of resellers.

www.f-secure.com/connected-home-security

F-Secure®