Despite Fast Adoption of Internet of Things, A Shocking 72 Per Cent Of Consumers Don’t Know How To Secure Their Connected Devices

Submitted by: The PR Room
Thursday, 17 March 2016

New research from BullGuard reveals that 66 per cent of consumers are very worried about hacks and breaches against their IoT devices, and 72 per cent don’t know how to protect themselves from these risks

London, 17 March 2016: A survey of over 6,000 UK residents by BullGuard (http://www.bullguard.com/), an industry-leading provider of mobile and internet security, illustrates just how widespread the Internet of Things (IoT) has already become while also highlighting serious security concerns among consumers.

The Internet of Things (IoT) has already arrived and is set to become even larger and more pervasive in the near future as more devices are connected to the internet. Over a quarter of consumers are planning to buy IoT devices in the next 12 months alone.

Deep security concerns

An IoT device is an appliance or similar device that connects to the internet. This ranges from automobiles and smart TVs to heating thermostats, security systems, baby monitors, surveillance cameras, dishwashers and garage doors. Additionally, connected smart coffee makers, batteries, light bulbs and even toothbrushes are also available.

BullGuard found that 66 per cent of consumers are ‘very concerned’ or ‘highly concerned’ about potential hacking and data theft carried out against their connected devices, with a worryingly large 34 per cent having already experienced a security incident or privacy problem in the past. A large 78 per cent of consumers express concern about security risks such as viruses, malware and hackers, while 66 per cent of consumers express concern over data collected by device manufacturers being inappropriately used or stolen. 57 per cent of consumers are also anxious about privacy breaches.

The IoT industry has yet to establish common security standards among devices. Smart device manufacturers tend to adopt their own approach to security while updates to ensure device security are often too technical and complex for consumers to carry out, even those who are technically literate. BullGuard’s research revealed that 22 per cent of consumers with advanced technical skills are not confident in their ability to keep their connected devices secure.

IoT used for state spying

These vulnerabilities have even been acknowledged by intelligence agencies across the world. In a recent testimony to the US senate James Clapper, the US director of national intelligence, said “In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking…or to gain access to networks or user credentials.”

Paul Lipman, CEO of BullGuard said: “Most of us have been working with internet connected devices such

as computers, smartphones and tablets for some time, but the Internet of Things is changing our perception of personal security, for both ourselves and our data. It's not just those who consider themselves 'technophobes' that have these concerns – tech savvy users are saying the same."

Education is essential

Clearly there are still issues to address when it comes to reassuring and educating consumers, even those who consider themselves technically literate.

When asked how they would rate their computer skills, the majority of respondents – 63 per cent – described themselves as 'intermediate or advanced'. 81 per cent said they are capable of setting up their own router, yet when asked if they have changed their router's password, 63 per cent said 'no.' 49 per cent also admitted that they don't know how, and a substantial 72 per cent do not know how to configure a router to keep a home network secure.
Router security is essential in the realm of IoT. An IoT device provides a gateway to a home network via a router, allowing cyber criminals the ability to essentially 'scope out' home networks and remain undetected.

"Consumers are clearly not equipped to handle the myriad of security risks presented by connected devices," said Paul Lipman, CEO of BullGuard. "With devices such as security cameras, alarm systems and door locks now being connected to the internet, physical security is becoming as much of a consideration for consumers as data security. Keeping these devices secure is absolutely imperative."

Consumers are clearly looking to antivirus vendors to help them solve this problem; 44 per cent of consumers believe antivirus vendors are responsible for securing their connected devices. The antivirus vendor was selected as the primary choice, even ahead of the device manufacturer and the ISP.

About BullGuard

BullGuard is a fast growing antimalware and mobile security brand. Its award-winning product portfolio includes internet security solutions, mobile security, 24/7 identity protection, and social media protection for both home and small business users, including BullGuard Premium Protection - a unique suite that goes beyond the PC to safeguard personal and financial information by continually monitoring the web, social networks, as well as the dark web for stolen and compromised data sources.
For more information visit BullGuard (http://www.bullguard.com/).

-Ends-

More information:

Press Contact
Paul Lester
The PR Room Ltd
Tel: +44 (0) 845 094 2902
Mobile: +44 (0) 7977 429 741

Email: paul.lester@theprroom.co.uk

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of The PR Room

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com