By Emma Williams and Emma Slade

What Influences Consumer Adoption And Secure Use Of Smart Home Technology?

THE INCREASING USE OF SMART DEVICES IS MAKING OUR HOMES MORE CONNECTED BUT OUR CHOICES AS CONSUMERS ARE VITAL TO ENSURE THEY ALSO STAY SECURE.

The increasing use of smart devices is making our homes more connected but our choices as consumers are vital to ensure they also stay secure.

The opportunity to fill our domestic spaces with smart speakers, smart thermostats, smart lights, smart locks, and an array of other connected appliances *can save us both time and money*. However, this increased connectivity is also accompanied by *security and privacy risks* associated with their use.

Unauthorised access to internal camera feeds and personal data, unlocking doors, and manipulating the activity of devices can all present security and privacy threats.

Although a greater emphasis is now being placed on making products as *secure as possible by design*, the behaviour of consumers who choose to use these products is a key element in *making sure that our homes continue to be safe*.

At the University of Bristol, we have been exploring *what influences people to use smart home technologies and how they choose to interact with them*. How do different people consider and respond to security risks related to smart devices, from when they choose a product and set it up in their home through to its longer-term maintenance and eventual discontinuance?

Consumer behaviour at all of these touchpoints has the potential to either mitigate or exacerbate security vulnerabilities in the smart home. In this way, understanding the influence of different factors on consumer choices and actions throughout the product lifecycle is vital to effectively mitigate security threats and to maximise the potential benefits that the digital economy has to offer.

As part of our research, we undertook an online survey capturing data from 633 people across a range of ages (18–79 years) and backgrounds in the UK. We developed four scenarios for use in this survey that considered security behaviours at different product touchpoints, based on the classification of smart devices (e.g. more 'simple' devices such as smart lights compared to more 'complex' devices such as smart locks) and vulnerabilities identified by our colleagues at Cranfield University.

Participants were asked to evaluate these scenarios and consider the extent to which they would behave in the same way and why. We explored how different people responded to these scenarios. Specifically, whether people who scored higher in characteristics such as risk-taking, impulsivity, and general technology adoption propensity would interact with smart home devices more or less securely.

We were also interested in what might influence people to adopt devices and the various factors that may influence their security-related behaviour. To help us understand this, the questionnaire included open-ended and closed questions, enabling us to collect and analyse both qualitative and quantitative data.
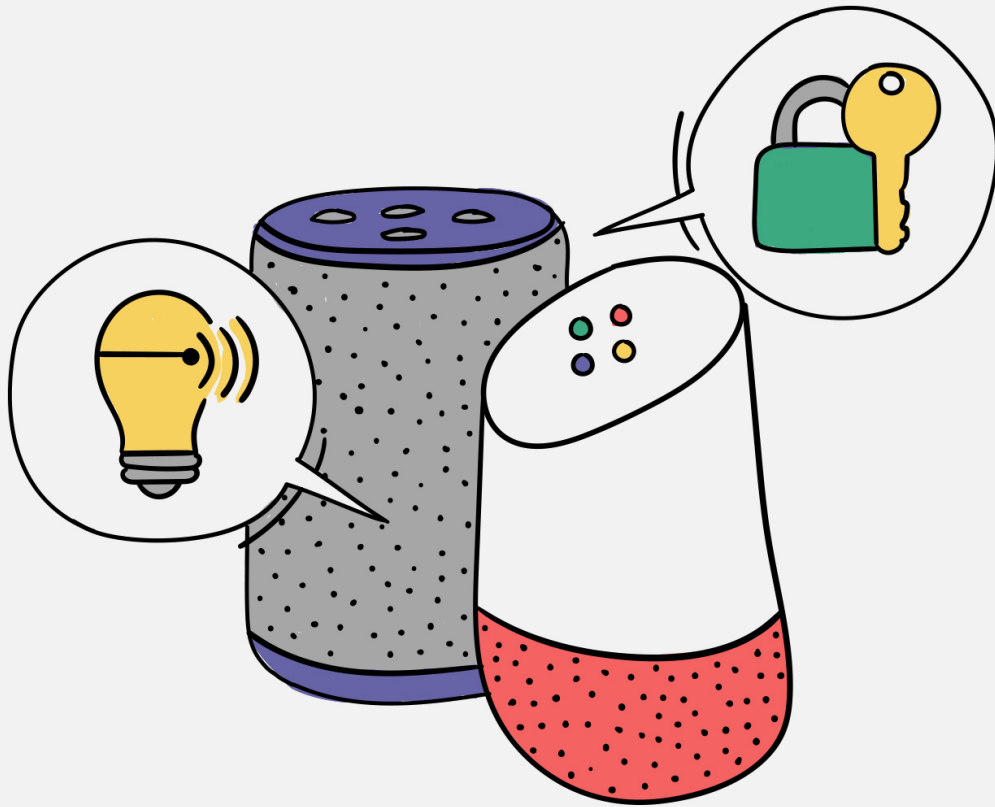
Initial findings suggest some key differences between current adopters of smart home technology and those who have yet to make the leap.

Being more optimistic about technology, considering oneself more proficient in using technology, and feeling less vulnerable from technology use was associated with adoption. Feeling more vulnerable from technology use, but also considering oneself more proficient in using technology, was related to more secure behaviour.

These findings highlight the potentially complex role of perceived ability to manage technology and perceived vulnerability to security threats in the adoption and secure use of smart home devices. The role of risk-taking and impulsivity was less clear.

We also identified a range of aspects that people consider influences their adoption of smart home devices and their secure use of these devices across the product lifecycle.

Participants consistently showed heightened secure behaviour for scenarios involving the 'complex' device (smart locks) compared to the 'simple' device (smart lights). The products were also viewed differently, both in terms of how important people consider security to be in relation to their operation and to the various factors that may influence their wider adoption, set-up, use, and discontinuance.

Importantly, although many people raised potential security concerns related to the use of such technology, the key question was whether the potential benefits were considered to outweigh the potential risks. Overall, results showed that greater perceived benefits and lower perceived security risks are likely to contribute to more insecure behaviour with regards to smart home technology.

We hope that our initial findings will help practitioners to consider consumer differences when developing smart products and designing marketing materials, and in planning interventions that will enable all sectors of society to safely and securely benefit from the opportunities provided by the digital economy.

READ MORE

This article is part of a series exploring the security of smart home technology. See all outputs from the project here: *www.crestresearch.ac.uk/projects/adoption-and-exploitation-of-smart-home-technology/*