EXECUTIVE SUMMARY

Individual Differences in the Adoption, Secure Use, and Exploitation of Smart Home Technology

Emma Williams, Emma Slade, Duncan Hodges, Phil Morgan, Dylan Jones, Bill Macken, Emily Collins and Tasos Spiliotopoulos

INTRODUCTION

This report details the key findings of work conducted by the *Individual Differences in Adoption, Secure Use, and Exploitation of Smart Home Technology* project.

The project consisted of three primary work packages (WPs) using smart home-based IoT technology to explore the relationship between individual differences in the adoption and secure use of new technology, and the exploitation of such technologies for nefarious purposes.

The project was delivered by a multi-disciplinary team, which included experts in consumer behaviour and technology adoption, psychology and human factors in the cyber domain, and cyberspace operations.

- WP1 reviewed current literature to develop a framework for *modelling the cyber-enablement of traditional crimes through the introduction of pervasive smart home-based IoT technology*, using residential burglary as a case example.
- WP2 then deployed an online survey, collecting qualitative and quantitative data from 633 participants, to explore the relationship between *individual differences and consumer adoption, and secure use, of some of the different types of smart home technology* identified in WP1.
- Within WP3, an online experimental task was then designed and programmed to examine how *priming people regarding security and privacy may influence their decision-making in smart home contexts,* using trigger action rules as a way to explore this. Two online

experiments (n = 375) were conducted to measure security and privacy settings under a range of conditions, including when participants were explicitly primed (experiment 1) and when they were implicitly primed (experiment 2) to think and act either more securely or more privately.

The approach of the latter two work packages provided a means to further consider the potential exploitation of connected smart home devices via vulnerabilities that may emerge as a result of people's choices.

Recommendations arising from this work are provided, with a particular focus on how the secure adoption and use of products and services by all consumers can be facilitated, including potential integration into the product development lifecycle.

KEY RECOMMENDATIONS

Our work shows how the opinions that people hold about technology can carry over to the choices that they make when setting up that technology. Consumers may benefit from increased engagement and education in the early stage of product consideration and use (e.g. during marketing, sales, and initial set-up/registration stages) regarding the relevance and importance of security for different types of smart home devices, particularly those not traditionally viewed as relevant to security.

For current users of devices, engagement via existing customer relationship management channels may provide a useful route (e.g. Dewnarain, Ramkissoon & Mavondo, 2019). More generally, this research suggests the importance of stressing the dangers to security and privacy from being overly trusting of technology and its applications, as well as highlighting the risks of particular types of use.

As part of these communications, current adopters and non-adopters of smart home technology would benefit from targeted communications differentially focused on emphasising potential risks and benefits (e.g. Key & Czaplewski, 2017). This would enable current adopters to better understand (and mitigate) security risks and non-adopters to understand the potential benefits that smart home technology may bring to their lives.

A balanced view of security risks should be encouraged via end-to-end collaboration internally within organisations, with security, product development, and consumer behaviour and marketing professionals all actively engaged to consider the full product lifecycle – from product development to adoption and eventual discontinuance (e.g. Jugend, Ribeiro de Araujo, Pimenta, Gobbo & Hilletofth, 2017).

To ensure sufficient understanding and buy-in across these groups of the needs and priorities of the other, internal marketing mechanisms may provide a useful structure to communicate and develop a shared internal vision of secure, consumer-focused innovation in relation to smart home devices, which can then be effectively communicated to consumers (e.g. Ballantyne, 2003; Kadic-Maglajlic, Boso & Micevski, 2018).

Increasing consumers' perceived proficiency with technology, both directly related to security aspects and wider technology interactions, may facilitate greater confidence to both adopt such technologies and to use them securely. Our work also suggests that people could benefit from more support in understanding how their systems are configured and the likely knock-on effects of upgrades and additions.

The use of community-focused, grassroots networks and organisations to develop and support technology proficiency within the community may increase the likelihood that such approaches can target a diverse range of consumer groups (e.g. Nicholson, Coventry & Briggs, 2019). Explicitly linking such approaches with existing, trusted organisations (e.g. across NGOs, industry, and the public sector) via sponsorship or other activities, may provide further credibility to networks and community technology support spaces, both in offline and online environments. Such approaches should provide support across the product lifecycle.

Reducing perceived vulnerability arising from using technology may increase the adoption of smart home technology but may also contribute to more insecure behaviour as a result if not managed appropriately. An approach that focuses on helping consumers to feel able to effectively manage any potential vulnerabilities that emerge rather than simply influencing perceptions of threat is likely to be preferable, and will also assist in building consumer resilience to emerging security risks as technology develops (e.g. Brass & Sowell, 2020; van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). Such an approach will likely require flexible and adaptive engagement with the community, or other trusted and accessible, support mechanisms. Such approaches should provide support across the product lifecycle.

Although risk information may increase secure behaviour it may also reduce intentions to use such devices. Therefore, exposure to media information regarding the risks of smart home technologies should be accompanied

by protective information that educates consumers on how they can easily manage these to increase secure behaviour without reducing usage or adoption of devices. Such information would likely benefit from the responsive, coordinated, and adaptive approaches typically seen in effective online crisis communications (e.g. Roshan, Warren & Carr, 2016).

Privacy and security work in slightly different ways and this requires more investigation. In the current work, although explicitly priming people to focus on improved security behaviours, it appeared to have an adverse impact on privacy behaviours. On the other hand, implicitly priming people to focus on privacy behaviours was shown to improve both privacy and security behaviours. As such, interventions in the smart home context should be carefully considered regarding the particular behaviour that they are aiming to encourage and the wider impacts that they may have on related behaviours.

ABOUT THIS PROJECT

This Executive Summary comes from the Full Report from the project *Individual Differences In The Adoption, Secure Use, And Exploitation Of Smart Home Technology.* You can find the Full Report *here*.

©2021 CREST, Creative Commons 4.0 BY-NC-SA licence.