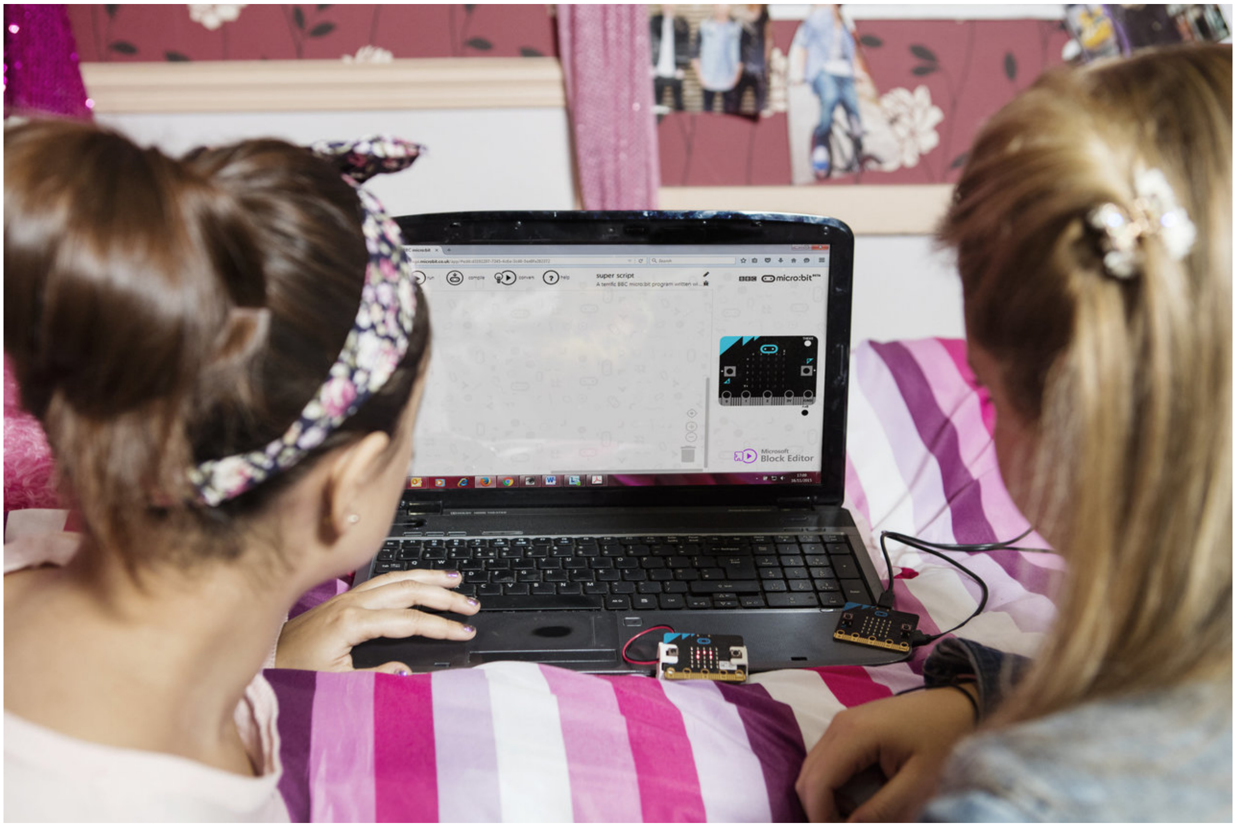
PHYS.ORG

Computer scientists are to explore how children can stay safe and retain their privacy as they engage with IoT

November 29 2017



Researchers are looking at how children can stay safe and retain their privacy as they engage with the Internet of Things. Credit: Micro:Bit Education Foundation

Computer scientists are to explore how children can stay safe and retain their privacy as they engage with the 'Internet of Things' (IoT).

Concerns about levels of computing literacy among young people, and the demands of future economies, has led to innovative programmes aimed at encouraging more children to explore and programme connected devices.

Schemes to help ensure future generations of digital innovators include the creation of the BBC Micro:Bit, a micro controller with in-built sensors, such as compass and accelerometer, Bluetooth connectivity and pins that enable it to be connected to external sensors and other devices.

The developers of the Micro:Bit took a very considered ethical approach to developing their device - purposefully restricting some functions, such as disabling Internet connectivity, restricting radio communication, and strengthening security around others, such as Bluetooth pairing, due to concerns around safety and privacy of children users.

However, as many other current, and potentially future, devices can connect to the Internet researchers are keen to learn more about how so called IoT devices could affect the privacy and security of young people.

Working alongside partners from the NSPCC, the Family Online Safety Institute, and the Micro:Bit Educational Foundation, researchers from Lancaster University, including computer scientists involved in the development of the operating software for the BBC Micro:Bit, will explore these issues as part of a one-year project 'Child Proofing the Internet of Things'. The project has been funded by the Engineering and Physical Sciences Research Council (EPSRC) via the PETRAS IoT Hub.

By working with groups of children to find out the ways they would use IoT devices, and then working with child protection experts, the research aims to:

- Discover the likely privacy and security challenges arising from children using IoT devices
- Find out what design and programming considerations are needed to provide greater protection
- What guidelines and advice is needed for children, their families and teachers for programming IoT devices

Dr Bran Knowles, Lancaster University Lecturer in Data Science and principal investigator, said: "Because we want future generations to be computer literate and to have a better range of core programming skills, children are encouraged to interact with programmable devices. Many of these devices have great functionality that requires them to be connected to the Internet. However this could potentially cause concerns around the privacy and security of the children using these devices.

"By working closely with child protection experts, this research will help provide a much richer understanding of the potential implications that may arise with children and IoT.

"In addition, we will also explore how the Micro:Bit, which was conceived as an educational tool, can be used to teach children how to engage safely with IoT devices."

Micro:Bit devices will be a key focus of the project, and the educational tool will help shed light on broader implications associated with children and all programmable IoT devices.

Gareth James, Chief of Education and Strategy at the Micro:Bit Foundation, said: "Students today need to prepare themselves for the huge variety of career options and challenges ahead. Connectivity means many people will be able to work from, or create business anywhere. Adaptability is vital - 65 per cent of today's reception children will need skills for jobs that don't exist yet and the average Briton will work in six different job roles spanning six different companies in their working life.

"There is a massive demand for digital competencies and skills, therefore it is vital that students are digitally adept otherwise they will miss out. We can support that by ensuring effective research is put in place now, in order to protect the privacy and security and safety of young people."

"By addressing concerns about children's safety and security with IoT devices as a primary step in their process, Micro:Bit is setting a positive example of building privacy by design into connected devices," said Stephen Balkam, Family Online Safety Institute (FOSI) CEO. "In our recent work and newest research study, FOSI has noted an increase in both awareness and concern from parents around their children's use of smart toys, devices, and wearables.

"This approach is directly in line with many of the recommendations being made by experts in this growing area of interest, and will allow parents to feel more comfortable letting their children take advantage of all the benefits this technology can offer."

Andy Burrows, NSPCC's Associate Head of Child Safety Online, said: "This innovative project will help shape our understanding of how internet devices will be used by young people; knowledge we greatly need in today's online world.

"As ever greater numbers of children start to use internet-connected toys and web-enabled household devices, it is crucial that we better understand the implications for child safety.

"This research will build our understanding of the privacy, security and safety implications for children, parents and policymakers, and we are pleased to be able to support it."

Provided by Lancaster University

Citation: Computer scientists are to explore how children can stay safe and retain their privacy as they engage with IoT (2017, November 29) retrieved 26 April 2024 from https://phys.org/news/2017-11-scientists-explore-children-safe-retain.html