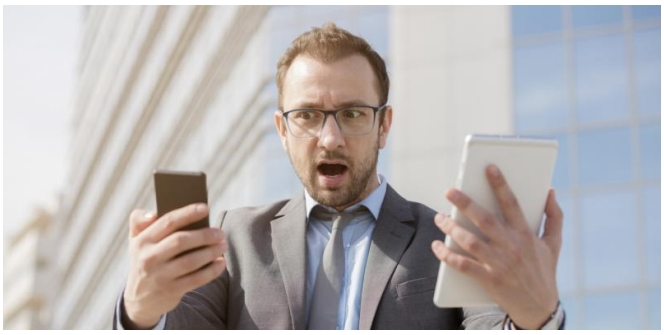
How to save the Internet of Things from cyber attacks – with psychology

15 November 2016, by John Blythe



Credit: Shutterstock

Two scientists were recently able to take over the lights of an office building using a drone and some clever computer hacking. They demonstrated how "smart" lightbulbs connected to the internet were vulnerable to a virus that could spread from one infected light to any bulb in range. The researchers flew a drone up to the building, transmitted a signal that hacked into one light and then took control of the whole floor. In theory, such an attack could be used to take out the lights of an entire city, if smartbulbs were to become commonplace.

These bulbs are just one example of devices that can be connected to the Internet of Things (IoT). The IoT refers to any everyday object with the ability to collect to and exchange data over the internet. The technology can allow you to remotely and automatically control the heating, lighting, sound-system and other devices in your home, based on your normal routine.

But these devices are also vulnerable to cyber attacks. The lightbulb example may have been a research experiment, but in a major attack recently, hundreds of thousands of IoT devices were captured by hackers and used to bring down many popular websites. So we need to make these objects more secure. One way to do this is to use psychology to understand users' capabilities and motivations and try to change people's behaviour.

Changing behaviour

Behaviour change when it comes to technology is an under-researched area. But recent work has started to take more of the theory into account, for example by focusing on "nudging" users towards better security and privacy. Nudge theory focuses on presenting choices to people in ways to steer them towards better decisions.

For example, one study explored Facebook privacy nudges by getting users to consider the content of what they are posting – and who will see the post. The researchers found that showing users pictures of their friends when posting a status prevented them from unintentionally disclosing things they would regret (such as a colleague seeing a nasty comment about their boss).

But we also need to think about longer-term behavioural change that focuses on people's capabilities and what motivates their behaviour when it comes to security. One route to doing this is by asking whether people don't know how to be secure or are just too lazy to do anything about it.

To answer this question, we need to understand behaviour in context using theory. For example, one model of behaviour, known as the "COM-B" model, says that to behave in a certain way, people need to have the capability and opportunity to do so – and be more motivated to do so than behave in any other way. They have to want to perform the behaviour and feel that they should.

By understanding what drives people's behaviour in this way, we can come up with ideas for how to change it. For example, the reason a person does not use a password on their device may be that they do not know the risk they are taking. In this case, we need to improve the user's capability

through teaching them about security risks.

By contrast, the reason could be that the device is hard to interact with and it takes up a lot of time to set up a password. Then we need to increase users' motivation perhaps by providing inbuilt incentives to having a password, such as offering additional services and features to users.

But looking at IoT security in this way also brings to how important it still for manufacturers to change their devices. Ultimately, most people don't have the ability to remember lots of complex passwords and may not even have the opportunity to create a password for their device. So we need to make sure security features are built into IoT devices and that they are simple and convenient enough for anyone to use, even if they have little or no technological skill. Only then can we start to make significant advancements towards making the IoT secure.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation